UNIVERSITÉ DE GENÈVE

Archive ouverte UNIGE
https://archive-ouverte.unige.ch

Ouvrage collectif 2019

Published version Open Access

This is the published version of the publication, made available in accordance with the publisher's policy.

Responsabilité civile et nouvelles technologies : Journée de la responsabilité civile 2018

Chappuis, Christine (ed.); Winiger, Bénédict (ed.)

Collaborators: Campi, Arnaud; Vajzovic, Dino

How to cite

CHAPPUIS, Christine, WINIGER, Bénédict, (eds.). Responsabilité civile et nouvelles technologies : Journée de la responsabilité civile 2018. Genève : Schulthess éditions romandes, 2019. (Collection genevoise. Droit de la responsabilité)

This publication URL: https://archive-ouverte.unige.ch/unige:145437

© This document is protected by copyright. Please refer to copyright holder(s) for terms of use.

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

Collection Genevoise

Schulthess
ÉDITIONS ROMANDES

Journée de la responsabilité civile 2018

Collection Genevoise

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 § 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
© Schulthess Médias Juridiques SA, Genève · Zurich · Bâle 2019
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

Tous droits réservés. Toute traduction, reproduction, représentation ou adaptation intégrale ou partielle de cette publication, par quelque procédé que ce soit (graphique, électronique ou mécanique, y compris photocopie et microfilm), et toutes formes d'enregistrement sont strictement interdites sans l'autorisation expresse et écrite de l'éditeur.

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.

Avant-propos

À mesure que progressent les nouvelles technologies rendues possibles par l'intelligence artificielle (IA), on assiste à une dématérialisation des comportements, voire des effets de ceux-ci sur les sujets de droit. L'on songe par exemple aux véhicules automobiles sans conducteurs, à la résolution des litiges sans avocats ou sans juges, au diagnostic ou aux soins sans médecin, ni infirmière. Ces bouleversements mettent au défi les principes de base de la responsabilité civile : qui peut être rendu responsable de quel préjudice ? Est-on arrivé aux frontières du droit de la responsabilité civile ? Le moment était clairement venu de faire le point. *Nouvelles technologies et responsabilité* est ainsi le thème de la Xe Journée de la responsabilité civile de Genève, pour laquelle nous avons réuni différents spécialistes autour de sujets essentiels pour les juristes. Le présent volume contient la version écrite de la plupart des conférences prononcées lors de cette journée.

En ouverture, Marcel Salathé[1], professeur à l'EPFL, a présenté un exposé expliquant la technologie sous-jacente, intitulé *Artificial Intelligence : The basics behind the technology*. Il a montré les domaines dans lesquels l'IA moderne fondée sur l'apprentissage profond (*deep learning*) a fait des progrès substantiels : la reconnaissance d'images (*image recognition*), le traitement du langage naturel (*natural language processing*) et la prise de décision dans des situations complexes (*decision making in complex environments*). Ces avancées comportent leurs dangers, en particulier si les algorithmes sont fondés sur des données biaisées. En conclusion, il a attiré l'attention du public sur l'importance de comprendre ces technologies[2].

Les questions de responsabilité liées à l'utilisation de véhicules autonomes sont traitées par Vincent Brulhart, professeur et avocat, avec le concours de Dimitri Gaulis, avocat et doctorant. Après avoir examiné l'admissibilité des véhicules autonomes au regard des règles nationales et internationales applicables, ils se penchent sur la responsabilité *de lege lata*, compte tenu des nouvelles tendances de type *car sharing*, et *de lege ferenda*, en se demandant si la disparition de la responsabilité du détenteur n'est pas programmée à terme.

La profession d'avocat, elle aussi, peut profiter des – ou doit subir les – nouvelles technologies. Jérôme Gurtner, docteur en droit, approfondit les questions (souvent négligées) de responsabilité en relation avec la cyber

---

1 Cet exposé ne fait pas l'objet d'une contribution écrite.

2 Le prof. Salathé a signalé que l'École Polytechnique Fédérale de Lausanne (EPFL) propose des cours en ligne gratuits, par exemple, https://exts.epfl.ch/courses-programs/50-things-you-need-to-know-about-data (12.8.19).

sécurité, et montre les applications possibles de l'IA pour l'exercice du métier, non sans aborder les problèmes d'indépendance que posent des algorithmes opaques.

L'actualité fourmille de *fake news*, ces informations volontairement et facilement manipulées du fait de l'utilisation généralisée des médias sociaux et de l'internet. Traitant de la responsabilité des hébergeurs pour ces *fake news*, Michel Reymond, avocat stagiaire et docteur en droit, commence par décrire le phénomène, puis expose l'état actuel du droit suisse avant de montrer l'importance de l'autorégulation.

La professeure Valérie Junod aborde, en anglais, la responsabilité pour les préjudices causés par l'IA dans le domaine médical, par exemple en cas de diagnostic erroné. Elle examine, en particulier, la loi sur la responsabilité du fait des produits et l'art. 55 CO, puis énonce une série de recommandations destinées à améliorer le régime actuel de responsabilité.

L'ouvrage se termine sur deux questions d'actualité traitées par la prof. Christine Chappuis. La révision du droit de la prescription, enfin aboutie, modifiera substantiellement la pratique de la responsabilité civile. S'agissant des moyens dont bénéficie la victime d'une atteinte à la personnalité par voie de presse, une décision de 2017[3] met la remise du gain – un moyen à ne plus ignorer désormais – au centre du débat. Cette décision clarifie les exigences de preuve auxquelles le moyen est soumis, qui ne doivent pas être sévères au point de le rendre inopérant.

Ce dixième volume représente notre contribution aux missions de recherche et de service à la Cité incombant à l'Université dans le domaine de la responsabilité civile. Il repose sur le travail et le temps qu'ont offerts les conférencières et conférenciers pour faire progresser ce domaine du droit. Nous les en remercions chaleureusement. Nos remerciements vont aussi à Arnaud Campi, docteur en droit, qui nous a suggéré le thème, puis nous a assistés dans la conception et la mise sur pied de la journée, et à Dino Vajzovic, assistant doctorant, qui s'est chargé de la relecture des contributions et a assuré la coordination des travaux d'édition. Merci aussi à Francine Pinget, secrétaire, qui a mis ces textes en page avec le plus grand soin en vue de la publication.

Août 2019

Christine Chappuis Bénédict Winiger

[3] ATF 143 (2017) III 297.

Sommaire

Avant-propos 5
Sommaire 7
Liste des auteurs 9

VINCENT BRULHART ET DIMITRI GAULIS

La responsabilité liée à l'utilisation de véhicules autonomes 11

JÉRÔME GURNER

Les nouvelles technologies et la responsabilité des avocats
La cybersécurité et l'intelligence artificielle 45

MICHEL JOSÉ REYMOND

La responsabilité des hébergeurs pour *fake news* 105

VALÉRIE JUNOD

Liability for damages caused by ai in medicine: progress needed 119

CHRISTINE CHAPPUIS

***Hot topics* en matière de responsabilité civile : prescription et**
remise de gain 151

Liste des auteurs

VINCENT BRULHART	Professeur aux Universités de Genève et de Lausanne, docteur en droit, avocat
CHRISTINE CHAPPUIS	Professeure à l'Université de Genève
DIMITRI GAULIS	Avocat à Lausanne, doctorant à la Faculté de droit de l'Université de Genève
JÉRÔME GURTNER	Docteur en droit
MICHEL JOSÉ REYMOND	Docteur en droit, avocat-stagiaire
VALÉRIE JUNOD	Professeure aux Universités de Genève et de Lausanne, docteure en droit, avocate

La responsabilité liée à l'utilisation de véhicules autonomes

Vincent Brulhart et Dimitri Gaulis[1]

Table des matières

I. Remarques préliminaires 12
II. Véhicules autonomes : Notions et admissibilité 13
A. Notions 13
B. Admissibilité 15
1. Voitures autonomes – K2020 ? 15
2. Drones – Y-a-t-il un (télé)pilote de l'aéronef ? 17
3. Navires autonomes – Master and (Remote)Commander 20
4. Essai de synthèse – Rise of the machines ? 22
III. La responsabilité liée à l'utilisation de véhicules autonomes 23
A. De lege lata 23
1. La responsabilité du détenteur selon l'art. 58 LCR 23
2. L'auxiliaire au service du véhicule (art. 58 al. 4 LCR) 24
2. Le partage de véhicule (Car sharing) 24
4. Le recours de l'assureur RC 25
5. Conclusion intermédiaire 29
B. Responsabilité *de lege ferenda* 29
1. Généralités 29
2. Le constructeur peut-il écarter la responsabilité du détenteur ? 30
3. Fonction préventive du droit de la RC 36

---

[1] VINCENT BRULHART, Professeur aux Facultés de droit des Universités de Lausanne et de Genève, avocat à Lausanne ; DIMITRI GAULIS, avocat à Lausanne, doctorant à la Faculté de droit de l'Université de Genève. Les auteurs remercient JÉRÔME LORENZ, assistant-diplômé et doctorant à la Faculté de droit de l'Université de Lausanne, pour son soutien efficace dans la mise au point de ce texte.

4. Harmonisation internationale des solutions 38
5. Lex Robotica ? 39
IV. Bibliographie 40

I. Remarques préliminaires

La notion de « véhicules autonomes » recouvre une réalité complexe, une complexité que l'on peut aborder et sous l'aspect du *véhicule* et sous celui de son *autonomie*. S'agissant du véhicule tout d'abord : si la notion appelle certes en premier lieu l'image d'automobiles sur roues, le véhicule autonome peut prendre d'autres formes encore. L'autonomie, quant à elle, fait référence aux diverses technologies qui permettent aujourd'hui l'assistance et, demain, le pilotage du véhicule à distance ou sa mise en œuvre par des systèmes susceptibles de remplacer l'intervention de l'homme[2].

Le phénomène des véhicules autonomes peut se traduire en effet de diverses manières. D'aucuns tendent à considérer des assistances variables selon les routes empruntées et les conditions de circulation. Les systèmes d'assistance utilisables sur les tronçons autoroutiers et les zones urbaines paraissent aujourd'hui constituer un aspect prioritaire. Pour le reste du réseau, les incertitudes demeurent à ce jour trop importantes pour permettre une prévision sérieuse ; c'est en tout cas l'avis de la Commission européenne[3]. Mais il demeure, ainsi que l'exprime cette même Commission, que le revenu de la mobilité routière ira pour l'essentiel à ceux qui auront mis au point les systèmes d'intelligence artificielle améliorant les conditions de sécurité des voyageurs et des piétons, qui auront pu imposer leurs protocoles de communication entre véhicules et infrastructure, et qui disposeront des meilleurs outils permettant d'organiser les flux de circulation afin d'éviter les ralentissements, en particulier en zone urbaine[4].

Pour notre part, nous nous proposons de faire un point sur la notion de véhicule autonome, dans une perspective à moyen terme, et la responsabilité qui en découle, en droit positif et en droit désirable. Nous aurons en vue prioritairement les véhicules automobiles sur roues dans la mesure où c'est bien cette forme de mobilité avant tout qui attise aujourd'hui l'intérêt des constructeurs et des usagers, mais nous verrons que certaines réflexions

---

2 Cf. PETER-MARTIN MEIER, *Bringt automatisierte Fahrt auch Wohlfahrt ?*, Circulation routière 1/2018, pp. 49 ss (50).

3 Cf. p. ex. RENÉ DANESI *et al.*, Rapport d'information du Sénat sur la stratégie de l'Union européenne pour le véhicule autonome N 117 du 27 novembre 2017, p. 9.

4 Cf. DANESI *et al.*, p. 5.

s'inscrivent dans une perspective plus large, englobant d'autres formes de véhicules pilotés à distance.

Le plan de notre contribution en découle. Dans une première partie, nous verrons les différentes formes que peuvent prendre aujourd'hui les véhicules autonomes, ainsi que les questions juridiques d'admissibilité à la circulation. Dans une seconde partie, il sera question de la responsabilité liée à l'utilisation de ces modes de transport et ce, *de lege lata*. Dans une troisième et dernière partie, nous verrons dans quelle mesure il pourrait être envisageable, voire souhaitable, de reconsidérer les règles du droit de la responsabilité pour tenir compte des possibles évolutions techniques liées à l'utilisation des véhicules autonomes (responsabilité *de lege ferenda*).

II. Véhicules autonomes : Notions et admissibilité

A. Notions

La définition du véhicule est plus ou moins étroite selon que l'on qualifie ce dernier uniquement par ses caractéristiques intrinsèques –un engin à propulsion autonome se déplaçant d'un lieu à un autre– ou également par sa fonction, à savoir le transport de personnes et de marchandises. Nous aborderons ci-après le véhicule dans son acception *lato sensu* afin d'englober tant les voitures que les camions, les drones et les bateaux.

Les développements récents de ces différents types de véhicules ont pour dénominateur commun de bénéficier des technologies de l'information et de la communication les plus avancées[5]. Ces technologies permettent d'augmenter de plus en plus le niveau d'automatisation des véhicules pour tendre vers une automatisation complète. En effet, la conjugaison de capteurs hyperperformants avec des plateformes d'intelligence artificielle permet désormais de voir émerger des véhicules entièrement autonomes.

En général, on décline l'automatisation des véhicules en six niveaux allant d'une absence d'automatisation (niveau 0) à une automatisation complète (niveau 5). Trois niveaux consacrent un transfert de responsabilité de la personne aux commandes[6] à une machine, c'est-à-dire un logiciel d'intelligence artificielle. Il s'agit des :

---

[5] Cf. ALEXANDRE CASSART, *Aéronefs sans pilote, voitures sans conducteur : la destination plus importante que le voyage*, in : H. Jacquemin/A. de Streel (édit.), *L'intelligence artificielle et le droit*, Bruxelles 2017, pp. 319 ss N 2 ; SÉBASTIEN FANTI/CÉDRIC MIZEL, *L'homologation de nouveaux systèmes techniques routiers et la problématique des voitures intelligentes*, Circulation routière 2/2015, pp. 10 ss (14).

[6] C'est-à-dire le conducteur pour les voitures et les camions, le pilote aux commandes pour les avions, le télépilote pour les drones, le capitaine pour les bateaux.

- Niveau 3 – automatisation conditionnelle : le système assure le guidage du véhicule pendant un certain temps ou dans des situations spécifiques, mais la personne aux commandes n'a plus à surveiller le système en permanence. Elle doit toutefois être à même de reprendre le contrôle du véhicule lorsque le système le lui demande, toujours avec une anticipation suffisante ;
- Niveau 4 – automatisation élevée : le véhicule est capable de maîtriser automatiquement toutes les situations dans des conditions d'utilisation définies (par exemple la conduite sur l'autoroute). La personne aux commandes est priée de reprendre les commandes avant que les conditions en question ne changent. Si elle ne s'exécute pas, le véhicule se met dans un état de risque minimal (en se rendant par exemple sur la bande d'arrêt d'urgence) ;
- Niveau 5 – automatisation complète : le véhicule n'a plus besoin d'une personne aux commandes, du départ à l'arrivée. Le système assume toutes les tâches de conduite, indépendamment du type de route, de la vitesse admise et des conditions de circulation[7].

Il est intéressant de noter qu'au sein des instances internationales (notamment l'Organisation de l'aviation civile internationale et de l'Organisation maritime internationale) la question s'est posée de savoir si cette automatisation (avec pour corollaire la disparition progressive de la personne aux commandes) remettait en cause la nature de ces véhicules au plan juridique. L'enjeu de cette question étant l'application des Conventions internationales aux véhicules autonomes (en l'espèce aéronefs et navires). Une réponse pragmatique a été apportée dans le sens que ces équipements ne modifient pas la nature du véhicule, ce qui assure l'application des Conventions aux véhicules autonomes[8].

Il convient d'examiner dans quelle mesure ces véhicules autonomes sont admis à la circulation.

---

[7] Cf. site de l'Office fédérale des routes (OFROU), p. « https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/stufen-der-automatisierung.html » (consulté le 22 juillet 2019). À noter qu'il existe une classification quasi-similaire pour ce qui est des navires autonomes, cf. COMITÉ MARITIME INTERNATIONAL, *CMI International working group position paper on unmanned ships and the international regulatory framework*, p. « https://comitemaritime.org/wp-content/uploads/2018/05/CMI-Position-Paper-on-Unmanned-Ships.pdf » (consulté le 22 juillet 2019), p. 1 note 1, qui décrit ces niveaux comme : (3) *Delegated* ; (4) *Monitored and* (5) *Autonomous* ; LLOYDS REGISTER, *Code for Unmanned Marine systems*, art. 4.1.2, p. « https://www.lr.org/en/unmanned-code/ » (consulté le 22 juillet 2019).

[8] Cf. COMITÉ MARITIME INTERNATIONAL, p. 3 ; CHRISTIAN BJORTUFT ELLINGSEN/ESPEN TONDEL, *Maritime law in the wake of unmanned Vessel*, p. « https://svw.no/en/news/news/2017/august/maritime-law-in-the-wake-of-the-unmanned-vessel/ » (consulté le 22 juillet 2019), p. 3 ; SARAH JANE FOX, *The Rise of the Drones: Framework and Governance-Why risk it?*, The Journal of Air Law and Commerce vol. 82, 2017, pp. 683 ss (687) ; MIKKO HUTTUNEN, *Unmanned, Remotey Piloted, or Something Else ? Analysing the Terminological Dogfight*, Air & Space Law 42, 2017, pp. 349 ss (354 ss).

B. Admissibilité

Bien que la problématique de l'automatisation soit commune aux différents modes de transport, chaque type de véhicule obéit à un régime juridique propre. C'est la raison pour laquelle nous aborderons séparément la question de l'admissibilité des voitures autonomes (*cf. infra*1), des drones (*cf. infra* 2), et des navires autonomes (*cf. infra* 3), pour conclure avec un essai de synthèse (*cf. infra* 4).

1. Voitures autonomes – K2020 ?

La Convention sur la circulation routière conclue à Vienne constitue le siège de la matière[9]. D'après son préambule, cette Convention a pour but de « faciliter la circulation routière internationale et d'accroître la sécurité sur les routes grâce à l'adoption de règles uniformes de circulation ». La Convention prévoit que « Tout véhicule en mouvement ou tout ensemble de véhicules en mouvement doit avoir un conducteur » (*cf.* art. 8 al. 1 Conv. Vienne), et que « Tout conducteur doit constamment avoir le contrôle de son véhicule […] » (*cf.* art. 8 al. 5 Conv. Vienne). Elle précise que « Le conducteur doit éviter toute autre activité que la conduite […] » (*cf.* art. 8 al. 6 Conv. Vienne) et que « Tout conducteur de véhicule doit rester, en toutes circonstances, maître de son véhicule, de façon à pouvoir se conformer aux exigences de la prudence et être constamment en mesure d'effectuer toutes les mesures qui lui incombent […] » (*cf.* art. 13 al. 1 Conv. Vienne)[10]. Il est à noter que la Convention de Vienne définit le conducteur comme « toute personne qui assume la direction d'un véhicule, automobile ou autre […] » (*cf.* art. 1 al. 1 let. v Conv. Vienne)[11]. Ceci implique que le conducteur est un être humain et non un système d'intelligence artificielle[12].

Le texte de la Convention a été amendé en 2016 et un alinéa 5*bis* complète désormais l'article 8 de la Convention de Vienne[13]. Il dispose que le véhicule est toujours réputé maîtrisé :

---

9 Convention sur la circulation routière conclue à Vienne le 8 novembre 1968 et entrée en vigueur pour la Suisse le 11 décembre 1992 (= Conv. Vienne ; RS 0.741.10).

10 L'art. 3 al. 1 et 3 de l'Ordonnance sur les règles de la circulation routière du 13 novembre 1962 (= OCR ; RS 741.11) concrétise ces obligations en prévoyant que « Le conducteur vouera son attention à la route et à la circulation […] » et que « les conducteurs de véhicules automobiles […] ne lâcheront pas l'appareil de direction […] ».

11 Cf. le texte anglais de la Convention où le terme *driver* est défini comme « *any person who drives a motor vehicle* ».

12 Cf. ALAIN BENSOUSSAN/JÉRÉMY BENSOUSSAN, *Le droit des robots*, Paris 2015, p. 84 N 383 ss ; FANTI/MIZEL, p. 15 ; NADINE ZURKINDEN, *AI and driverless cars : from international law to tests runs in Switzerland to criminal liability risks*, in : H. Jacquemin/A. de Streel (édit.), *L'intelligence artificielle et le droit*, Bruxelles 2017, pp. 341 ss, (343).

13 RO 2016 1019.

- en cas de manœuvre assurée par un système automatisé d'assistance à la conduite si le conducteur peut reprendre le contrôle total du véhicule en désactivant le système ;
- si le système automatisé est conforme aux règles fixées dans les prescriptions internationales en matière d'admission[14].

Compte tenu de la prolifération des systèmes automatisés d'assistance à la conduite (dits ADAS, *Advanced driver assistance* systems, dont le but est de contribuer à la sécurité active) dans les voitures intelligentes et connectées, l'art. 8 al. 5*bis* Conv. Vienne apporte une précision bienvenue qui était d'ailleurs préconisée par la doctrine[15].

Néanmoins, pour ce qui est des voitures véritablement autonomes – c'est-à-dire sans conducteur (niveau 5 – automatisation complète, dite également voitures-robot) – la Convention de Vienne constitue, en l'état, un écueil insurmontable à leur admissibilité (immatriculation). En effet, tant l'interprétation littérale qu'historique des articles 8 et 13 de la Convention conduisent à refuser la mise en circulation sur la voie publique de voitures autonomes[16]. Seules des autorisations *ad hoc* délivrées par le Conseil fédéral sur la base de l'art. 106 al. 5 de la Loi fédérale sur la circulation routière (ci-après LCR)[17] permettent de conduire des essais dans des conditions strictes[18]. C'est sur cette base qu'ont été effectués les essais de la voiture autonome Swisscom à Zurich, des navettes de Carpostal autonomes à Sion et des robots de livraison de colis (robots-facteurs) à Berne[19]. Notons que pour l'Office fédéral des routes (OFROU), les tests avec des véhicules de niveaux 3 à 5 nécessitent systématiquement une autorisation *ad hoc*[20].

Pour la mise en circulation de voitures autonomes, une rapide adaptation du cadre légal paraît donc indispensable. Cette adaptation passera inévitablement par une modification de la Convention de Vienne[21]. D'un point

---

14 Les Règlements de l'ONU annexés à l'Accord concernant l'adoption de prescriptions techniques uniformes applicables aux véhicules à roues, aux équipements et aux pièces susceptibles d'être montés et/ou utilisés sur un véhicule à roues et les conditions de reconnaissance réciproque des homologations délivrées conformément à ces prescriptions conclus à Genève le 20 mars 1958 (RS 0.741.411). Les Règlements techniques mondiaux de l'ONU élaborés dans le cadre de l'Accord concernant l'établissement de règlements techniques mondiaux applicables aux véhicules à roues, ainsi qu'aux équipements et pièces qui peuvent être montés et/ou utilisés sur les véhicules à roues, fait à Genève, le 25 juin 1998.

15 Cf. notamment A. BENSOUSSAN/J. BENSOUSSAN, p. 84 N 386 ; FANTI/MIZEL, p. 14.

16 Cf. A. BENSOUSSAN/J. BENSOUSSAN, p. 84 N 385 ; FANTI/MIZEL, p. 16 ; ZURKINDEN, p. 346.

17 RS 741.01.

18 Cf. OFROU, *Aide-mémoire concernant la réalisation de projets pilotes en Suisse du 05.12.2017*, p. « https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/pilotversuche.html » (consulté le 22 juillet 2019), notamment le ch. 2.

19 Cf. « https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/aktivitaeten-des-bundes-.html » (consulté le 22 juillet 2019) ; FANTI/MIZEL, pp. 21 ss ; ZURKINDEN, pp. 346 ss.

20 Cf. OFROU, notamment le ch. 2. ch. 1.

21 Cf. A. BENSOUSSAN/J. BENSOUSSAN, p. 84 N 387 ; FANTI/MIZEL, p. 16 ; ZURKINDEN, p 343.

de vue pratique, cela signifie que l'essor des voitures autonomes risque d'être beaucoup plus long pour les États membres de ladite Convention que pour les États non-membres (notamment les États-Unis et le Royaume-Uni) compte tenu du temps nécessaire à la révision de tels instruments internationaux. Les premiers États peuvent donc perdre en compétitivité au profit des seconds faute d'une évolution rapide du cadre réglementaire et d'une action concertée entre les États concernés[22].

2. *Drones – Y-a-t-il un (télé)pilote de l'aéronef ?*

Par nature, un drone n'emporte pas de pilote à son bord, mais il est dirigé par un télépilote au sol grâce à un poste de contrôle et un système de transmission de données[23]. Il faut donc considérer le système comme un tout et non pas uniquement l'engin volant. Désormais, on parle d'ailleurs plus de système d'aéronef télépiloté (*Remotely Piloted Aircraft Sytems*, RPAS) que de véhicule aérien sans pilote (*Unmanned Aerial Vehicle*, UAV).

Le télépilotage de ces véhicules peut se faire dans le champ de visibilité directe du pilote (*Visual line of sight*, VLOS) ou au-delà de son champ de visibilité directe (*Beyond line of sight*, BLOS). Les systèmes les plus évolués permettent de diriger les drones par ordinateur selon un itinéraire programmé, l'intervention du pilote se limitant aux cas d'urgence (niveaux 3 et 4 d'automatisation). En revanche, si techniquement les drones sont munis de systèmes permettant de détecter d'autres appareils (comme des transpondeurs) et de transmettre au télépilote les instructions nécessaires afin qu'il évite une collision, ils ne sont pas capables d'identifier avec certitude d'autres aéronefs ou des obstacles soudains (détection) et de rectifier automatiquement leur trajectoire de vol programmée en conséquence pour éviter une collision (évitement, ce qui correspond au niveau 5 dit d'automatisation complète)[24].

---

22 Cf. Déclaration d'Amsterdam du 14 avril 2016 sur la Coopération en matière de conduite connectée et autonome signée par les ministres européens des transports met d'ailleurs l'accent sur ces aspects. Cf. également, FANTI/MIZEL, p. 16.

23 Cf. la définition de l'Organisation de l'aviation civile internationale : « une série d'éléments configurables comprenant un aéronef télépiloté, ses postes de télépilotage, les liaisons nécessaires de commandes et de contrôle et tous autres éléments de système éventuellement nécessaires à tous points durant le vol », cf. OACI-Comité Juridique, *Questionnaire sur les aspects juridiques des systèmes d'aéronefs télépilotés*, p. « https://www.icao.int/Meetings/LC37/Documents/LC37%20WP%202-1%20FR%20Remotely%20Piloted%20Aircraft.pdf » (consulté le 22 juillet 2019), p. 3 N 3.

24 Cf. RPAS Working group de l'OFAC, *Les drones en Suisse – Un nouveau défi*, rapport du 7 février 2016, p. « https://www.bazl.admin.ch/bazl/fr/home/bonasavoir/drones-et-modeles-reduits.html » (consulté le 22 juillet 2019), p. 9 N 3.2.1.

Sur le plan international, l'art. 8 de la Convention relative à l'aviation civile internationale de Chicago[25], dispose qu'« Aucun aéronef pouvant voler sans pilote ne peut survoler sans pilote le territoire d'un État contractant, sauf autorisation spéciale dudit État et conformément aux conditions de celle-ci.[…] ». Il revient donc en premier lieu aux législateurs nationaux de réglementer l'utilisation des drones.

En Suisse, les drones sont considérés comme des « *aéronefs de catégories spéciales* » (*cf.* art. 108 al. 1er let c LA[26])[27]. Bien que les drones se différencient des modèles réduits[28], le même régime juridique leur est applicable, en particulier l'ordonnance du DETEC sur les aéronefs de catégories spéciales (OACS)[29]. Celle-ci encadre de manière sommaire l'utilisation d'aéronefs sans occupant. Elle prévoit que les aéronefs sans occupant, quel que soit leur poids, sont dispensés d'inscription au registre des matricules (art. 2 al. 1 OACS) et qu'ils n'ont pas l'obligation d'utiliser un aérodrome pour décoller et atterrir (art. 3 OACS). Enfin, une autorisation particulière n'est pas requise pour les vols commerciaux (art. 5 OACS). En revanche, l'exploitant de l'aéronef a l'obligation de conclure une assurance responsabilité civile couvrant les prétentions des tiers au sol d'un montant minimal d'un million de francs (art. 14 al. 2 et art. 20 al. 1er OACS)[30].

De plus, l'OACS opère une *summa divisio* entre les aéronefs sans occupant dont le poids au décollage est inférieur à 30 kg et ceux dont le poids au décollage est supérieur à 30 kg. Les premiers n'ont pas besoin d'autorisation pour être exploités (*cf.* art. 14*b* ss OACS et art. 14 al. 1er *a contrario* OACS)[31], ils ne sont pas non plus soumis à un examen de leur navigabilité (art. 2 al. 2 OACS). À noter également que, sur la base de l'art. 19 OACS, les Cantons de Genève et de Vaud ont adopté des règlements applicables à ces aéronefs[32].

À l'inverse, l'exploitation d'aéronefs de plus de 30 kg est soumise à l'autorisation de l'Office fédéral de l'aviation civile (OFAC ; art. 14 OACS). L'Office fixe dans chaque cas les conditions d'admission et d'utilisation de ces

---

25 Convention relative à l'aviation civile internationale conclue à Chicago le 7 décembre 1944 et entrée en vigueur pour la Suisse le 4 avril 1947 (RS 0.748.0).

26 Loi fédérale sur l'aviation du 21 décembre 1948 (= LA ; RS 748.0).

27 Cf. RPAS Working group de l'OFAC, p. 12 N 4.1.

28 *Ibid.*, pp. 7 ss N 2.4 ss. L'art. 17 OACS désigne d'ailleurs les aéronefs sans occupants en tant que « *modèles réduits d'aéronefs* », le terme drone n'existant pas dans la législation helvétique en vigueur.

29 Ordonnance du DETEC sur les aéronefs de catégories spéciales du 24 novembre 1994 (= OACS ; RS 748.941).

30 À noter que les aéronefs d'un poids inférieur à 0.5 kg ne sont pas soumis à cette obligation, cf. art. 20 al. 2 let. d OACS.

31 Cf. RPAS Working group de l'OFAC, pp. 12 ss N 4.3.

32 Cf. Règlement concernant l'exécution de la Loi fédérale sur l'aviation (RS GE H 3 05.02) ; Règlement concernant l'interdiction de survol de périmètres déterminés par des aéronefs sans occupants d'un poids inférieur à 30 kg (RS VD 720.24).

aéronefs. Dans ce cadre, l'OFAC examine la construction, la conception, la solidité et les aspects liés à la sécurité de l'exploitation de ces appareils. En ce qui concerne ces autorisations *ad hoc*, l'OFAC impose de manière standard d'exploiter ces aéronefs en visibilité directe (VLOS), excluant par-là les autres types de vols (BLOS/vols autonomes). Il est également intéressant de souligner que la pratique de l'OFAC en matière d'autorisation pour les drones de plus de 30 kg est plus restrictive que pour les modèles réduits d'aéronefs classiques. Cela s'explique par le fait qu'en dépit de l'équivalence d'un point de vue juridique entre ces types d'appareils, l'OFAC considère que l'usage des drones –particulièrement à des fins commerciales – est plus long, plus fréquent, et comprend un nombre plus grand de vols, ce qui accroît le facteur risque[33].

L'art. 17 OACS dispose que l'utilisateur d'un modèle réduit d'aéronef « doit avoir constamment un contact visuel direct avec celui-ci et pouvoir en assurer la conduite en tout temps »[34]. À la suite d'une procédure dite de Specific Operations Risk Assessment (SORA), une dérogation est possible à cette règle sur autorisation spéciale de l'OFAC pour autant qu'il n'y ait pas mise en danger des autres utilisateurs de l'espace aérien et des tiers au sol (art. 18 al. 2 OACS)[35]. L'autorisation peut être assortie de conditions (art. 18 al. 3 OACS).

En ce qui concerne les systèmes entièrement autonomes sans intervention de télépilote, ils ne sont pas autorisés pour l'heure[36]. Cela s'explique d'un point de vue technique par une capacité de détection et d'évitement des obstacles qui n'est pas encore aboutie, et juridiquement par le fait que la législation impose au télépilote de pouvoir assurer la conduite de l'appareil en tout temps et de garder un contact visuel direct avec celui-ci (*cf.* art. 17 al. 1er OACS). Si la première exigence peut faire l'objet de dérogation (autorisation *ad hoc* des vols BLOS)[37], il n'en va pas de même pour la seconde en l'état actuel.

Quoi qu'il en soit ce régime devrait connaître des modifications suite à l'adoption de règles –largement inspirées de la pratique helvétique – à l'échelon européen. Dans la mesure où la Suisse participe à l'Agence européenne de la sécurité aérienne, ces nouvelles normes ne manqueront pas d'influencer le cadre législatif helvétique compte tenu de l'objectif d'harmonisation poursuivi par cette Agence. Le Règlement (UE) 2018 11/39 concernant les règles communes dans le domaine de l'aviation civile et

---

33 *Ibid.*, pp. 16 ss N 4.5.2.

34 *Ibid.*, p. 13 N 4.3.1.1.

35 Cf. OFAC, *Fiche d'information Régime d'autorisation suisse en matière de drone*, p. « https://www.bazl.admin.ch/bazl/fr/home/bonasavoir/drones-et-modeles-reduits/autorisations-d_exploiter-des-drones-au-dessus-dun-rassemblement.html » (consulté le 22 juillet 2019) ; « http://jarus-rpas.org/content/jar-doc-06-sora-package » (consulté le 22 juillet 2019).

36 *Ibid.,* p. 7 N 2.2.

37 *Ibid.*, p. 15 N 4.3.4.

instituant une Agence européenne pour la sécurité aérienne du 4 juillet 2018 adopte une approche fondée sur les performances et les objectifs à atteindre (art. 4 al. 1 let. e Règlement). Il prévoit à ses articles 55 à 59 les exigences auxquelles les drones doivent répondre en termes de conception de production, de maintenance et d'exploitation. Le Règlement d'exécution (UE) 2019/947 du 24 mai 2019 concernant les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord concrétise ces exigences. Il classe lesdits aéronefs en trois catégories en fonction de la gradation des risques liés à leur exploitation : catégorie « ouverte », catégorie « spécifique » et catégorie « certifiée » (*cf.* art. 3). Les drones de la catégorie « ouverte » (*cf.* art. 4) doivent avoir un poids inférieur à 25 kg et leur pilote doit conserver à tout moment une vue directe sur l'aéronef sauf lorsqu'il vole en mode suivez-moi ou lorsqu'il utilise un observateur (*cf.* art. 4 al. 1 let. d). Les aéronefs ne remplissant pas ces conditions tombent dans la catégorie « spécifique », ils sont soumis à autorisation après une procédure de *risk assessment* (*cf.* art. 5). L'exploitation d'appareils de la catégorie certifiée (*cf.* art. 6) implique – quant à elle – le survol de rassemblements de personnes, le transport de personnes et de marchandises dangereuses ; ces véhicules doivent obtenir une certification et les exigences relatives à leur exploitation s'apparentent à celles applicables aux aéronefs avec pilote à bord. Enfin, les conditions de navigabilité que doivent remplir les véhicules de ces différentes catégories sont précisées dans le Règlement délégué (UE) 2019/945 relatif aux systèmes d'aéronefs sans équipage à bord et aux exploitants, issus de pays tiers, de systèmes d'aéronefs sans équipage à bord du 12 mars 2019 (*cf.* art. 4 ss pour les aéronefs de la catégorie ouverte et art. 40 pour ceux des catégories certifiée et spécifique). Néanmoins, bien qu'entrés en vigueur, ces Règlements ne commenceront à déployer leurs effets qu'à partir de juin 2020.

3. Navires autonomes – Master and (Remote)Commander

La navigation maritime est un terrain particulièrement propice à l'autonomisation, notamment en raison de la vitesse des navires[38], de l'espacement entre ces derniers et du faible nombre d'obstacles imprévus (en comparaison des autres modes de transport). Toutefois, le développement de navires autonomes remet en cause une composante fondamentale du transport maritime, celle du rôle du capitaine et de l'équipage. Cette remise en cause touche l'ensemble du droit maritime. Nous nous concentrerons ici sur les Conventions internationales.

[38] Ce d'autant plus que les bateaux ne croisent souvent plus à leur vitesse maximale de croisière afin d'économiser du carburant, pratique dite du *slow steaming*.

La Convention des Nations Unies sur le droit de la mer[39] définit les droits et obligations des États sur les mers et les océans. Elle contient en particulier des règles définissant dans quelle mesure un navire peut naviguer dans les différentes zones de la mer, quelles sont les obligations de l'État sur les navires battant son pavillon, et quels sont les droits des autres États sur les navires étrangers dans les différentes zones de la mer.

Si la législation de l'État du pavillon est la pierre angulaire du cadre juridique applicable aux navires (art. 90 et 91 al. 1er CNUDM), la Convention de Montego Bay prévoit un certain nombre d'obligations de l'État du pavillon. L'article 94 al. 3 b) et 4 let. b) CNUDM dispose en particulier que :

« Tout État prend à l'égard des navires battant son pavillon les mesures nécessaires pour assurer la sécurité en mer, notamment en ce qui concerne : […] *la composition, les conditions de travail et la formation des équipages*, en tenant compte des instruments internationaux applicables. Ces mesures comprennent celles qui sont nécessaires pour *s'assurer que : […] tout navire est confié à un capitaine et à des officiers possédant les qualifications voulues*, en particulier en ce qui concerne la manœuvre, la navigation, les communications et la conduite des machines, et que *l'équipage possède les qualifications voulues et est suffisamment nombreux eu égard au type, à la dimension, à la machinerie et à l'équipement du navire* ».

De plus, l'art. 98 CNUDM prévoit que le capitaine a une obligation de prêter assistance « pour autant que cela lui est possible sans faire courir de risques graves au navire, à l'équipage ou aux passagers ».

L'un des autres textes majeurs entrant en ligne de compte est la Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer[40]. L'annexe V de la Convention[41] prévoit que l'État du pavillon s'assure que tous navires sont « *sufficently and efficiently manned* » (règle 14 intitulée « *Ship's manning* ») et que « *in hazardous navigational situations where heading and/or track control systems are in use, it shall be possible to establish manual control of the ship's steering immediately* » (règle 24).

Dans la mesure où ces règles n'imposent pas la présence d'un équipage à bord, on peut considérer qu'un navire télépiloté remplit les conditions exposées ci-dessus[42]. En effet, le rôle du télépilote s'apparente à celui du capitaine dans la mesure où tous deux assument la conduite du navire. En

---

39 Convention des Nations Unies sur le droit de la mer conclue à Montego Bay le 10 décembre 1982 et entrée en vigueur pour la Suisse le 31 mai 2009 (= CNUDM ; RS 0.747.305.15).

40 Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer conclue à Londres le 1er novembre 1974 et entrée en vigueur pour la Suisse le 1er janvier 1982 (RS 0.747.363.33).

41 Non publiée au RS mais, p. « http://www.imo.org/en/OurWork/facilitation/documents/solas%20v%20on%20safety%20of%20navigation.pdf » (consulté le 22 juillet 2019).

42 Cf. COMITE MARITIME INTERNATIONAL, pp. 6 N 3.4 et 10 N 4.2.

revanche, les navires autonomes ne remplissent pas ces conditions. En effet, le système d'intelligence artificielle ne s'apparente pas à un équipage et la capacité de reprendre le contrôle du navire manuellement (même à distance) en cas de danger fait défaut.

L'implication humaine dans le processus de décision a donc un rôle central dans tous les instruments internationaux en matière maritime[43]. Par conséquent, une adaptation des Conventions en vigueur est nécessaire afin d'autoriser les navires autonomes[44].

Toutefois, les États disposent d'une large marge de manœuvre en ce qui concerne leurs eaux intérieures et la mer territoriale sur lesquelles ils sont souverains (*cf.* art. 2 CNUDM). Il s'agit là d'un cadre propice à l'expérimentation et au développement de navires autonomes puisque les Conventions internationales n'y trouvent qu'une application limitée[45].

4. Essai de synthèse – Rise of the machines ?

L'étude des Conventions internationales démontre que les véhicules automobiles avec automatisation de niveaux 3 et 4 sont admissibles tout comme les drones et les bateaux télépilotés. En revanche, les véhicules entièrement autonomes (niveau d'automatisation 5) restent interdits. L'admission de ces véhicules devra passer par la révision des textes internationaux. Or, l'issue de ce processus –à la fois long et laborieux– est incertaine puisque cette démarche n'a véritablement de sens que si un grand nombre d'États ratifie les Conventions amendées.

Au plan national, les règles internationales sont largement reprises avec toutefois une marge de manœuvre plus importante des États grâce notamment aux autorisations *ad hoc*. Si ce régime permet d'éprouver les systèmes et favorise l'innovation, il n'est cependant pas pérenne puisqu'il conduit à une fragmentation du régime juridique applicable aux véhicules alors que ces derniers ont pour vocation de se déplacer par-delà les frontières.

Ce tour d'horizon des règles relatives à l'admissibilité des véhicules autonomes a permis de mettre en lumière le fait que les problématiques rencontrées sont, pour une large part, communes aux différents types de

---

43 *Ibid.* pp. 20 ss N 6.

44 Le *Maritime Safety Committee* de l'Organisation Maritime internationale étudie désormais les amendements qui seront nécessaires au regard des Conventions existantes. Ce comité devrait poursuivre ses travaux jusqu'au milieu de l'année 2020, cf. p. « http://www.imo.org/en/mediacentre/meetingsummaries/msc/pages/msc-98th-session.aspx » (consulté le 22 juillet 2019).

45 Cf. le projet norvégien de navire autonome Yara Birkeland, p. « https://www.yara.com/news-and-media/press-kits/yara-birkeland-press-kit/ » (consulté le 22 juillet 2019) ; ELLINGSEN/TONDEL, pp. 1ss.

véhicules. Aussi pouvons-nous aborder la question de la responsabilité sous l'angle de l'automatisation des véhicules automobiles.

III. La responsabilité liée à l'utilisation de véhicules autonomes

Plusieurs contributions ont pu montrer que les dispositions en vigueur du droit de la responsabilité civile permettent de garantir une protection suffisante à la victime d'un dommage causé par la mise en œuvre d'un véhicule autonome, en tout cas s'agissant d'un véhicule sur roues. Nous le rappellerons très brièvement (A). En revanche, est moins considérée la question de savoir si le droit désirable doit proposer des solutions différentes (B). Est-il toujours justifié de faire supporter le poids principal de la réparation à un « détenteur », ou ne devrait-on songer désormais à mettre davantage de poids sur la responsabilité d'autres protagonistes, tels que le constructeur ou le concepteur des logiciels de pilotage ? Une telle réflexion ne devrait-elle pas être approfondie également pour des motifs qui portent sur la prévention du potentiel dommageable à sa source, sachant le rôle que peut jouer le droit de la responsabilité civile à cet égard ? Enfin, que dire de l'harmonie internationale des solutions ?

A. De lege lata

1. La responsabilité du détenteur selon l'art. 58 LCR[46]

L'art. 58 LCR est habité par la conception selon laquelle le risque d'accident résulte, d'une part, de facteurs physiques tels que vitesse, poids, énergie cinétique et, d'autre part, de la conduite humaine, l'homme étant susceptible de commettre des erreurs. Or, dès l'instant où l'emploi du véhicule et l'accident sont en lien avec un défaut de programmation, le risque d'accident tiendrait davantage du défaut de logiciel que d'une erreur de conduite[47].

Quant à la défectuosité du véhicule[48], elle ne libère pas son détenteur et ce, en application de l'art. 59 al. 2 LCR. Pour autant, d'aucuns ont exprimé l'avis selon lequel la situation pourrait être différente lorsque le défaut du système

---

46 Loi fédérale sur la circulation routière du 19 décembre 1958 (= LCR ; RS 741.01).

47 Cf. p. ex. FRANZ WERRO/VINCENT PERRITAZ, *Les véhicules connectés : un changement de paradigme pour la responsabilité civile?*, in : F. Werro/T. Probst (édit.), *Journées du droit de la circulation routière 23 - 24 juin 2016*, Berne 2016, pp. 7 et 8.

48 Cf. p. ex. les cas de systèmes défectueux cités MARC THOMMEN/SOPHIE MATJAZ, *Die Fahrlässigkeit im Zeitalter autonomer Fahrzeuge*, in : D. Jositsch/C. Schwarzenegger/W. Wohlers (édit.), *Festschrift für Andreas Donatsch*, Zurich 2017, p. 275 notes 12 et 13.

d'assistance provient d'un opérateur externe ; il pourrait y avoir en pareil cas un défaut informatique imputable à un tiers qui ne constituerait pas une défectuosité du véhicule. Cette circonstance pourrait être de nature, *de lege lata* déjà, à mettre en cause la responsabilité du détenteur selon la LCR[49].

2. *L'auxiliaire au service du véhicule (art. 58 al. 4 LCR)*

Celui qui offre une assistance électronique au pilotage du véhicule peut-il être qualifié aujourd'hui d'auxiliaire dont le détenteur répondrait en application de l'art. 58 al. 4 LCR ? Dans l'affirmative, même si la défectuosité devait être le fait d'un opérateur externe, le détenteur en répondrait ; dans la négative, il n'en répondrait pas. Or, ni l'une ni l'autre solution ne paraît satisfaisante. Faire répondre le détenteur pour un acte d'un tiers opérateur qui, par hypothèse aurait en main la maîtrise du véhicule ne rend pas un juste compte de la situation de fait, et charge le détenteur de façon injustifiée. D'un autre côté, permettre au détenteur de se libérer pourrait placer le lésé dans une situation difficile considérant que les autres chefs de responsabilité susceptibles d'entrer en ligne de compte pour lui (LRFP[50] notamment) n'offrent pas les mêmes garanties que celles qui découlent de la responsabilité fondée sur la LCR (obligation d'assurance, droit d'action directe, inopposabilité des exceptions, *etc.*).

3. *Le partage de véhicule (Car sharing)*

Diverses formes d'usage commun apparaissent et les modalités qui s'y rapportent sont susceptibles de prendre place aussi dans le contexte de l'économie collaborative ; un particulier peut alors mettre son véhicule à disposition d'un autre particulier par l'entremise d'une plateforme d'échange. On peut noter au passage que l'intermédiaire qui exploite le logiciel permettant l'usage partagé dispose de nombre d'informations qui le mettent en situation d'apprécier les caractéristiques du véhicule, cas échéant du conducteur ; autrement dit le « *big data* » lui permettrait une certaine maîtrise des risques, une circonstance qui pourrait justifier une forme de responsabilité. Aux États-Unis, certains sont allés jusqu'à considérer que celui qui exploite la plateforme d'échange endosse une responsabilité de détenteur quand bien même il n'aurait jamais été propriétaire du véhicule, ni même mis en possession[51]. On peut imaginer des formes plus évoluées encore, dans

---

49 Même si, comme le rappellent à raison WERRO/PERRITAZ, p. 6, la présomption de l'art. 59 al. 1 LCR rendra difficile la démonstration de l'absence d'une défectuosité du véhicule par son détenteur ; par ailleurs, la faute de l'opérateur devrait être grave.

50 Loi fédérale sur la responsabilité du fait des produits du 18 juin 1993 (= LRFP ; RS 221.112.944).

51 Cf. p. ex. DAVID BERKE, *Products Liability in the Sharing Economy*, Yale Journal on Regulation 33/II/2016, pp. 603 ss (646) cité par VINCENT BRULHART, *Sign up & drive : quelles assurances ?*

lesquelles le véhicule partagé bénéficie d'un fonctionnement autonome. Certains défendent en effet l'avis selon lequel les véhicules autonomes auraient un très grand potentiel de développement précisément dans le contexte du *car sharing* : par un « clic », il deviendrait possible de commander un véhicule à la location et de le faire venir vers soi, un procédé qui aurait nombre de conséquences positives, notamment sur l'environnement[52]. Dans le même temps, ces formes de partage pourraient conduire à une dilution de la détention, considérée traditionnellement comme une notion de fait qui se rapporte à celui qui tire le bénéfice de l'usage et qui exerce la maîtrise sur le véhicule[53]. Cela pourrait en particulier poser la question de savoir qui est tenu à l'obligation d'assurance.

4. Le recours de l'assureur RC

4.1. Le fondement du recours

On considère donc aujourd'hui qu'un véhicule autonome sur roues reste soumis aux règles de responsabilité de la LCR et que le problème de la responsabilité concurrente du constructeur, du concepteur de logiciel, voire du vendeur, s'examine sous l'angle du recours de l'assureur RC. C'est donc bien au travers de cette action récursoire que l'on aborde aujourd'hui les nouvelles formes de responsabilités susceptibles de résulter de la mise en œuvre de véhicules connectés et autonomes. Notre réflexion suivra dès lors ce chemin dans un premier temps, pour se demander dans un second temps si ces responsabilités, que l'on considère actuellement en deuxième ligne (à savoir une fois la victime indemnisée par le détenteur), ne devraient pas prendre peu à peu une place plus importante dans le dispositif d'indemnisation, voire apparaître en première ligne, directement face au lésé.

Le fondement du recours de l'assureur RC du détenteur à est l'origine de plusieurs controverses. La première vise la question de savoir si les art. 60 al. 2 et 61 al. 1 LCR sont applicables : certains nient que l'assureur RC du détenteur puisse s'en prévaloir, d'autres soutiennent que tel pourrait être le cas[54]. La

Remarques sur l'émergence de l'économie collaborative et ses dépendances envers l'assurance, in : B. Kahil-Wolff Hummer/J. Juge (édit.), *Le droit social numérique*, Berne 2018, p. 57 note 27.

52 Cf. MEIER, p. 56 ; ERICA PALMERINI *et al.*, *D6.2 Guidelines on Regulating Robotics - RoboLaw*, Pise 2014, p. 42.

53 Cf. p. ex. ANDRÉ BUSSY *et al.*, *Art. 58 LCR*, in : *CS CR commenté*, 4e éd., Bâle 2015, p. 701 N 4.3.

54 Cf. p. ex. MANFRED DÄHLER/RENÉ SCHAFFHAUSER (édit.), *Handbuch Strassenverkehrsrecht*, Bâle 2018, p. 76 § 1 N 315 ; BUSSY *et al.*, *Art. 60 LCR*, pp. 736 ss N 2.12 et *Art. 61 LCR*, pp. 745 ss N 2.6 ; ROLAND BREHM, *La responsabilité civile automobile*, 2e ed., Berne 2010, pp. 381 ss N 999.

question a pu se poser également sous l'angle de l'art. 51 al. 2 CO (cascade en cas de solidarité imparfaite) ; le point est discuté également[55].

Il est généralement admis aujourd'hui que l'assureur RC du détenteur peut se prévaloir de l'art. 72 LCA, une disposition dont le Tribunal fédéral vient d'élargir le champ, en supprimant notamment la restriction qui a longtemps prévalu selon laquelle le recours de l'assureur n'était possible qu'à l'encontre de celui qui répond d'une responsabilité pour faute au sens de l'art. 41 CO[56]. Le projet de révision partielle de la LCA en cours devrait fixer la question de manière définitive[57].

4.2. LRFP

Il n'est guère douteux que le constructeur du véhicule réponde d'une défaillance d'un système d'assistance en application de la loi sur la responsabilité du fait des produits. Il est admis en effet que de pareilles installations tombent sous le coup de la définition du « produit » au sens de la loi. Lorsque l'assistance est intégrée dès l'origine dans une machine, dans un appareil ou dans un « *hardware* », c'est l'appareil ou la machine dans son ensemble qui sont défectueux. À défaut d'être intégré, le logiciel constitue lui-même un produit, lequel peut être affecté d'un dysfonctionnement susceptible d'engager la responsabilité de son producteur[58]. Il est vrai que la notion de produit au sens de la LRFP se rapporte en principe à une chose mobilière, mais il est sans doute possible, sinon souhaitable, d'y assimiler le logiciel, à tout le moins s'il revêt un caractère standard[59].

4.3. La défectuosité

Sous l'angle de la responsabilité du destinataire, il convient tout d'abord de se poser la question du défaut du système d'assistance, défaut qui constitue un préalable à toute forme de responsabilité dont l'origine est à chercher dans un problème de fonctionnement. La question a déjà été abordée, notamment sous l'angle du dysfonctionnement technique des systèmes d'assistance (défaillance

---

55 Cf. p. ex. FRANZ WERRO/VINCENT PERRITAZ, *La remise en cause de l'ordre des recours de l'art. 51 al. 2 CO*, PJA 10/2018, pp. 1179 ss (1181) note 19 ; sur la notion de solidarité imparfaite, voir VINCENT PERRITAZ, *Le concours d'actions et la solidarité*, thèse, Zurich 2017, pp. 69 ss.

56 Cf. ATF 144 III 209 ; à noter que l'on considère que l'assureur RC peut faire valoir son recours par une application analogique de l'art. 72 LCA ; l'assureur RC ne couvre pas le dommage du lésé en effet (sur ce point VINCENT BRULHART, *Droit des assurances privées*, 2e éd., Berne 2017, pp. 380 ss et 447 ss.

57 Cf. à cet égard, Message du Conseil fédéral suisse concernant la révision de la loi fédérale sur le contrat d'assurance (LCA) du 28 juin 2017, FF 2017 4767, pp. 4808 ss.

58 CHRISTOPH MÜLLER/JONATHAN GRETILLAT, *Le recours de l'assurance RC du détenteur contre le constructeur en cas de dysfonctionnement d'un système d'aide à la conduite de véhicule*, Circulation routière 2/2015, pp. 37 ss (41).

59 Cf. WERRO/PERRITAZ, p. 10.

du régulateur de vitesse, de l'assistant de démarrage en côte, de l'assistant de parcage, etc.). On a débattu tout d'abord la question de savoir ce que recouvre la notion de « défaillance ». Certains ont exprimé l'avis selon lequel le défaut ne devrait pas se définir en fonction des règles relatives à la responsabilité contractuelle, dans la mesure où ces dernières reposent sur une conception subjective découlant de la volonté des parties. Or les obligations de sécurité en matière de circulation routière doivent être déterminées sur la base d'un fondement objectif. Aussi a-t-on envisagé un parallèle avec l'art. 58 CO (vice de construction ou défaut d'entretien), puis avec l'art. 59 al. 1 LCR qui fait état de la « défectuosité du véhicule ». Cette dernière notion englobe toute insuffisance technique ou fonctionnelle du véhicule qui a joué un rôle dans la survenance de l'accident ; la référence est prise de l'état de la technique et des prescriptions légales. Et l'on songera naturellement aussi à la loi fédérale sur la responsabilité du fait des produits[60] ; en cette matière en effet, la sécurité attendue s'apprécie de façon objective : elle dépend des attentes du consommateur moyen et non de celle d'un utilisateur déterminé[61].

4.4. La responsabilité du conducteur

La question se pose ici de la mesure de la diligence attendue. L'introduction des systèmes d'assistance n'a, à ce jour, guère modifié les règles relatives au comportement que l'on peut raisonnablement attendre des conducteurs. Ce sont plutôt les questions relatives à l'admissibilité de ces systèmes qui font l'objet de réglementations nouvelles. Même dans le domaine du transport aérien, aucun nouveau critère permettant de fixer la diligence attendue n'a été défini. D'une façon générale, la tendance actuelle reste de tabler sur le fait que l'utilisateur doit conserver la maîtrise de sa machine, et qu'il répond d'éventuels dommages susceptibles de résulter de sa mise en œuvre[62].

Pour compréhensible qu'elle soit au premier regard, cette manière d'envisager le problème a cependant ses limites. Il faut rappeler tout d'abord que les systèmes d'assistance ont pour but d'améliorer les conditions de sécurité en éliminant les erreurs humaines à l'origine des accidents[63]. D'une façon générale, ils ont précisément pour vocation de soulager l'utilisateur dans ses tâches de pilotage. Dans certaines situations, le fait de ne pas s'y fier peut entraîner des conséquences plus dommageables que le résultat qu'aurait entraîné la seule mise en œuvre du système d'assistance. Si bien que l'utilisateur peut être pris en étau dans l'alternative suivante : soit il répond

---

60 Cf. MÜLLER/GRETILLAT, p. 38.

61 *Loc. cit.*

62 C'est ainsi qu'il a été jugé qu'un dommage lié au défaut d'un système d'assistance au parking est imputable au conducteur du véhicule, cf. AG Munich du 10.07.20117, 275 C 15658/07 cité par THOMMEN/MATJAZ, p. 286 note 65.

63 Cf. p. ex. PALMERINI *et al.*, p. 40 ; MEIER, p. 51.

parce qu'il a repris la maîtrise de son véhicule en situation critique, soit il répond précisément parce que confronté à une telle situation, il n'a pas repris la maîtrise de son véhicule, se fiant au système d'assistance[64].

À cela s'ajoutent les difficultés liées aux interfaces personne-machine. Cette circonstance constitue d'ailleurs une des difficultés qui pourraient, de l'avis de certains, retarder, voire entraver, la généralisation des systèmes d'assistance[65].

Et puis, rendre l'utilisateur responsable du défaut, n'est-ce pas refuser la conception selon laquelle l'assistance est à l'avantage de la collectivité ? Cela pourrait induire en effet une conclusion selon laquelle le système serait au bénéfice exclusif de son utilisateur, lequel en tire donc profit (en augmentant par exemple son confort), ce qui conduit à le rendre responsable de la défaillance cas échéant. Ainsi considérée, la décision de recourir aux systèmes d'assistance n'appartiendrait qu'à l'utilisateur, à ses risques et périls. Si, en revanche, l'assistance est regardée comme un progrès collectif, et que son usage soit considéré comme offrant un avantage important pour la communauté (diminution notable des risques d'accident[66]), alors il n'appartiendrait plus à l'individu de choisir d'y recourir, mais son utilisation deviendrait une sorte d'obligation. En pareille hypothèse, faire répondre l'usager d'une défaillance reviendrait alors à lui faire supporter le risque d'un système que la collectivité lui impose, ce qui paraît constituer un résultat peu satisfaisant.

4.5. Utilisation malveillante

L'attentat de Nice du 14 juillet 2016 a montré, s'il en était encore besoin, que les véhicules peuvent être d'authentiques armes. Or, on peut nourrir de ce point de vue d'autres craintes encore, sachant qu'il pourrait être bientôt possible d'engager des véhicules à distance, sans conducteur, en vue de causer des dommages à autrui[67]. Le procédé n'en serait que plus aisé, ce qui peut augmenter d'autant le potentiel dommageable. En l'état, si le véhicule est immatriculé, le détenteur en répond. Si le véhicule n'a pas de détenteur connu, le Fonds national de garantie peut être appelé à intervenir, comme ce pourrait être le cas si la somme d'assurance devait être insuffisante[68].

Pour autant, une telle intervention du Fonds de garantie suppose une responsabilité selon la LCR. Peut-on encore considérer que le dommage est en pareil cas lié à l'emploi d'un véhicule, ou celui-ci n'est-il au fond que le média

---

64 Cf. p. ex. THOMMEN/MATJAZ, p. 287.

65 Cf. p. ex PALMERINI *et al.*, p. 44.

66 Cf. p. ex. MEIER, p. 52.

67 Cf. p. ex. MEIER, pp. 52 ss.

68 Cf. art. 76 al. 2 let. a ch. 1 LCR ; VINCENT BRULHART, *Droit des assurances privées*, pp. 62 et 138 ss ; FF 2002 4093, pp. 4108 ss.

permettant la réalisation de sombres projets qui n'ont en soi rien à voir avec le déplacement que doit normalement garantir l'usage de véhicules automobiles ? Autrement dit est-il juste de faire supporter la réparation de tels dommages à la collectivité des détenteurs d'automobiles ? À terme, la question pourra se poser, ce qui mettra en cause par là même le problème de l'indemnisation.

5. Conclusion intermédiaire

À ce stade, force est donc constater que les régimes en place, notamment de la LCR, ne paraissent pas encore complètement dépassés ; certaines considérations montrent cependant qu'à terme, ils ne saisiront que difficilement les conséquences juridiques d'un recours généralisé aux véhicules autonomes.

B. Responsabilité *de lege ferenda*

1. Généralités

La notion de détention recouvre deux aspects : la question de savoir qui exerce la maîtrise de fait sur le véhicule et celle de savoir qui a un intérêt prépondérant à l'emploi de ce véhicule.

À qui faut-il attribuer la maîtrise de fait sur un véhicule autonome ? Il est probable que celui qui le pilote à distance ou qui conçoit le logiciel de pilotage doit être sérieusement considéré à ce titre. Quant à l'intérêt à l'emploi, la question pourra recevoir des réponses nuancées : plus que celui qui utilise le véhicule pour un trajet déterminé, on pourra considérer à ce titre celui qui met le véhicule à disposition pour un temps déterminé, quitte à le mettre à disposition d'un autre utilisateur ensuite.

Quel que soit le résultat de ces réflexions, les usagers perçoivent, aujourd'hui déjà, que la maîtrise des véhicules autonomes leur échappe ; dès lors, ils pourraient progressivement refuser d'assumer un risque et une responsabilité en lien avec des engins sur lesquels ils exerceront de moins en moins d'influence. Un phénomène qui revêt d'ailleurs, au-delà de son volet juridique, une composante commerciale, ce qui n'a pas échappé aux constructeurs, lesquels offrent désormais publiquement d'assumer la totale responsabilité – disent-ils –, pour les dommages liés à l'utilisation de véhicules autonomes. Au-delà de l'aspect publicitaire, il faut encore se demander quelle est la portée juridique de tels engagements.

2. *Le constructeur peut-il écarter la responsabilité du détenteur ?*

L'autonomisation des véhicules a pour objet le transfert de la conduite de la personne aux commandes vers le système d'intelligence artificielle. Partant, le conducteur/détenteur est de moins en moins acteur de la conduite du véhicule tandis qu'il reste pleinement responsable en cas d'accident[69]. Sur le plan du droit de la responsabilité, cette évolution pose immanquablement la question de la disparition de la responsabilité du détenteur et de sa substitution par celle du constructeur.

Si le cadre légal n'est pas (encore) allé jusque-là, le cap a été franchi par certains constructeurs qui proposent, en cas d'accident, de se substituer au détenteur lorsque le véhicule est en mode autonome. Le constructeur Volvo, par l'intermédiaire de son PDG, a été le premier à proposer d'endosser l'entière responsabilité des conséquences d'un accident lorsque le véhicule est en mode autonome[70]. Le PDG de la marque a fait les déclarations suivantes :

« Si la voiture est en mode tout automatique, que quelque chose arrive, et qu'il est prouvé que la voiture est responsable, alors nous endosserons toute la responsabilité. Nous rembourserons à la fois les compagnies d'assurance et les propriétaires de véhicules. »[71] ;

« *Volvo assumera l'entière responsabilité* dès lors qu'un véhicule de la marque sera conduit en mode autonome »[72].

Dans l'hypothèse où ces déclarations doivent se concrétiser dans les engagements contractuels du constructeur (hypothèse que nous désignerons ci-après « clause Volvo »), il convient de s'interroger sur leur qualification et leur portée en particulier vis-à-vis du lésé.

Deux cas de figure doivent être envisagés : le premier correspond à la situation ordinaire où le constructeur n'a pas de relation contractuelle avec le

---

69 Cela a pour corollaire de permettre aux constructeurs de développer des systèmes tests dont ils ne sont pas tenus responsables (du moins directement), cf. CASSART, p. 337 N 44.

70 Déclaration du 19 octobre 2015 du PDG de Volvo Car Group M. Hakan Samuelsson, cf. *Volvo Cars responsable des actes de ses voitures autonomes*, p. « https://www.volvocars.com/fr/univers-volvo/nos-innovations/intellisafe/conduite-autonome/actualite/responsabilite-voitures-autonomes » (consulté le 11 novembre 2018) ; LEFIGARO.FR, *Voiture autonome, quelle responsabilité en cas d'accident ?*, p. « http://voiture-autonome.lefigaro.fr/voiture-autonome-quelle-responsabilite-cas-daccident/ » (consulté le 22 juillet 2019) ; LESECHOS.FR, article du 05.06.18 de R. Demichelis, *Volvo veut endosser la responsabilité de ses voitures autonomes*, p. « https://www.lesechos.fr/intelligence-artificielle/veille-technologique/0301765363885-dans-la-presse-etrangere-volvo-veut-une-voiture-autonome-responsable-2181423.php » (consulté le 22 juillet 2019) ; LEMONDE.FR, article du 08.1015, *Voitures sans chauffeur : Volvo assume ses responsabilités en cas d'accident*, p. « https://lesclesdedemain.lemonde.fr/technologie/voiture-sans-chauffeur-volvo-assume-ses-responsabilites-en-cas-d-accident_a-88-5353.html » (consulté le 22 juillet 2019).

71 LESECHOS.FR, article du 05.06.18.

72 Cf. la brochure *Auton'homme Vision 2020*, p. « https://www.volvocars.com/fr/univers-volvo/notre-vision/voiture-autonome/conduite-autonome/future-of-driving » (consulté le 11 novembre 2018).

propriétaire/détenteur (*cf. infra* 2.1) ; le second cas de figure envisagé est celui où constructeur et propriétaire/détenteur sont contractuellement liés (*cf. infra* 2.2), situation qui est appelée à se généraliser avec le développement des plateformes de services proposant la mise à disposition temporaire de véhicule (*Car sharing, cf. supra* III.A.3). Ces compagnies sont propriétaires/détentrices des véhicules et ont généralement des relations directes avec les constructeurs.

2.1. En l'absence de relation contractuelle entre propriétaire/détenteur et constructeur

Actuellement, le propriétaire/détenteur du véhicule n'a pas de relation contractuelle avec le constructeur, mais seulement avec l'importateur du véhicule. On est donc en présence de deux relations contractuelles. Il existe, d'une part, un premier contrat de vente entre le constructeur et l'importateur et, d'autre part, un second contrat de vente entre l'importateur et le propriétaire/détenteur. En outre, ce dernier répond du dommage qu'il cause au lésé sur la base de l'article 58 LCR.

Dans ce cadre, on peut voir dans la « clause Volvo » une garantie contractuelle du constructeur vis-à-vis de l'importateur prévoyant que lorsque le détenteur doit répondre d'un dommage suite à un accident de la circulation (alors que le véhicule est en mode autonome), le constructeur prendra en charge les conséquences pécuniaires dudit dommage.

L'engagement du constructeur est une *res inter alios acta*, il ne produit pas d'effet à l'encontre du propriétaire/détenteur et du lésé faute de rapport contractuel avec ces derniers. Ledit engagement doit donc nécessairement prendre la forme d'une stipulation pour autrui (art. 112 CO) pour déployer des effets en leur faveur. Le constructeur a alors la qualité de promettant, l'importateur celle de stipulant et enfin le propriétaire/détenteur et/ou le lésé celle de bénéficiaire (la formulation de la « clause Volvo » variant à cet égard, voir ci-dessus).

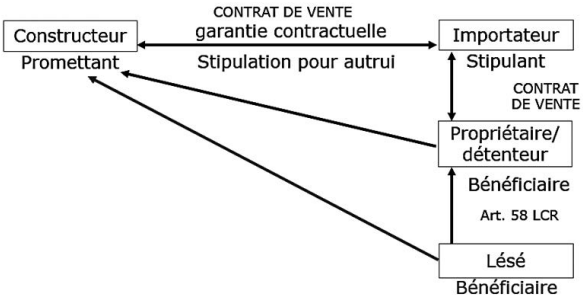
Pour créer un droit direct du lésé contre le constructeur, cette garantie doit prendre la forme d'une stipulation pour autrui parfaite (art. 112 al. 2 CO). Contrairement à la stipulation pour autrui imparfaite, la stipulation pour autrui parfaite prévoit que le bénéficiaire peut recevoir la prestation, mais aussi la réclamer en son nom puisqu'il dispose d'une créance propre[73].

L'interprétation de la « clause Volvo » devrait permettre de conclure au caractère parfait de la stipulation en faveur du lésé. En cas de silence du

[73] Cf. PIERRE ENGEL, *Traité des obligations en droit* suisse, 2e éd., Berne 1997, p. 420 N 92 ; PATRICK KRAUSKOPF, *Der Vertrag zugunsten Dritter*, thèse, Fribourg 2000, p. 12 N 37 et pp. 223 ss N 884 ss ; SILVIA TEVINI DU PASQUIER, *Art. 112 CO*, in : F. Werro/L. Thévenoz (édit.), *CoRo Code des obligations I* (art. 1-529 CO), 2e éd., Bâle 2012, N 16 ; ROLF WEBER, *Art. 112 CO*, *BeKomm. Band VI : Obligationenrecht 1. Abteilung: Allgemeine Bestimmungen. 6. Teilband: Beziehungen zu Dritten (Art. 110-113 OR)*, Berne 2002, N 6 et 47 ss.

contrat, même si la stipulation pour autrui parfaite ne se présume pas, la jurisprudence reconnaît un droit propre au tiers lorsqu'il s'agit de le protéger[74]. Compte tenu du contexte et des buts de la « clause Volvo », cette condition nous semble réalisée en l'espèce. Partant, le lésé, en sa qualité de bénéficiaire de la stipulation pour autrui, serait lui-même habilité à demander l'exécution de la prestation en sa faveur au constructeur/promettant en vertu de la garantie contractuelle (qui figure dans l'accord entre ce dernier et l'importateur stipulant).

Représentation schématique :



2.2. *Nouvelles tendances, contrat entre le détenteur et le constructeur*

Avec les nouvelles tendances d'utilisation des véhicules automobiles, on se dirige de plus en plus vers la mise à disposition d'un véhicule par une plateforme de type *Car sharing*. Cela traduit la perte d'intérêt progressive pour la possession d'un véhicule[75]. Selon ce modèle, la société qui exploite et met à disposition le véhicule est appelée à en devenir le détenteur de fait. Cette société achète généralement le véhicule auprès du constructeur, il en découle une relation juridique directe entre le détenteur/propriétaire et le constructeur.

Dans cette hypothèse, on peut qualifier la « clause Volvo » de reprise de dette interne (art. 175 CO), à savoir un accord entre le reprenant et le débiteur par lequel le premier promet de libérer le second de sa dette envers un tiers créancier[76]. Transposé à notre hypothèse, cela signifie que le constructeur s'engage en qualité de reprenant avec le propriétaire/détenteur – débiteur initial – à libérer celui-ci de ses dettes potentielles vis-à-vis de futurs lésés – créanciers.

---

[74] Cf. TEVINI, *Art. 112 CO* N 9 et les références citées.

[75] Cf. CASSART, p. 319 N 2.

[76] Cf. THOMAS PROBST, *Art. 175 CO*, in : F. Werro/L. Thévenoz (édit.), *CoRo Code des obligations I* (art. 1-529 CO), 2e éd., Bâle 2012, N 1.

La reprise de dette interne est une promesse de libération, elle ne transfert pas la dette, mais constitue un engagement de reprise (*Befreiungsversprechen)*[77]. La libération peut se faire soit en acquittant la dette directement, soit par une reprise privative de dette externe, hypothèse que nous excluons ici compte tenu du fait que le constructeur et le lésé n'ont aucune relation contractuelle[78]. La reprise est dite interne, car elle ne concerne pas les droits du créancier, elle n'engage que le reprenant envers le débiteur[79].

En vertu du contrat de reprise de dette, le reprenant doit libérer le débiteur de la dette envers le créancier, ce qui intervient en général au travers de l'exécution de la prestation (en payant la somme due par exemple, art. 175 al. 1er CO)[80]. Le débiteur peut exiger l'exécution de la prestation en mains du créancier dès que la dette est exigible[81].

Toutefois, selon le principe de de la relativité des contrats, la reprise de dette interne n'a d'effets qu'entre le reprenant et le débiteur initial[82]. Pour que le créancier jouisse de droits propres, la reprise de dette doit, comme précédemment, être accompagnée d'une stipulation pour autrui parfaite (art. 112 al. 2 CO). Ainsi, le lésé (également créancier dans la reprise de dette et bénéficiaire de la stipulation pour autrui) est lui-même habilité à demander l'exécution de la prestation en sa faveur au constructeur (reprenant et promettant) en vertu de la reprise de dette conclue par ce dernier avec le détenteur (débiteur initial et stipulant).

---

77 Cf. ATF 121 III 256 consid. 3b ; THOMAS PROBST, *Intro. art. 175-183 CO*, in : F. Werro/L. Thévenoz (édit.), *CoRo Code des obligations I* (art. 1-529 CO), 2e éd., Bâle 2012, N 5.

78 PROBST, *Intro. art. 175-183 CO*, N 5.

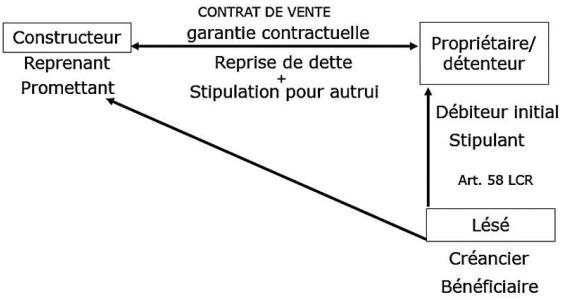
79 PROBST, *Intro. art. 175-183 CO*, N 5.

80 Cf. PROBST, *Art. 175 CO,* N 4. On peut aussi envisager dans notre hypothèse que l'on se trouve en présence d'une reprise cumulative de dette soit l'accord par lequel un tiers se constitue débiteur solidaire aux côtés du débiteur initial sans que celui-ci soit libéré de sa dette (art. 143 ss CO). Le créancier peut alors faire valoir sa dette contre les deux débiteurs solidaires, cf. ENGEL, pp. 902 ss N 281 ; PROBST, *Intro. art. 175-183 CO,* N 6. Le lésé verrait ainsi sa position de créancier renforcée puisqu'il pourrait faire valoir sa créance contre les deux débiteurs solidaires, le constructeur et le détenteur/propriétaire. Bien qu'il existe un recours interne entre eux (art. 149 CO), ledit recours ne devrait être ouvert qu'au détenteur et non pas au constructeur, ce dernier s'étant engagé à réparer tout le dommage. De façon générale, les développements ci-dessous valent *mutatis mutandis* pour la reprise cumulative de dette.

81 Cf. PROBST, *Art. 175 CO,* N 5.

82 ATF 121 III 256 consid. 3b.

Représentation schématique :



Dans les deux cas de figure mentionnés plus haut (*cf. supra* 2.1 et 2.2), il convient d'apporter les précisions suivantes.

Toute dette peut faire l'objet d'une reprise. La dette reprise par le tiers peut être litigieuse ou non, actuelle ou future. Dans ce dernier cas, la dette doit toutefois être suffisamment déterminable[83]. Il en va de même pour la prestation en faveur du bénéficiaire dans la stipulation pour autrui[84]. Quant au tiers, il peut s'agir d'une personne ou d'une entité non encore déterminée, il suffit que le tiers soit déterminable au moment de recevoir la prestation[85]. La stipulation pour autrui et la reprise dette ne sont en principe sujettes à aucune condition de forme, elles peuvent donc être conclues oralement ou par actes concluants[86].

En principe, on considère que la reprise de dette peut intervenir simultanément ou postérieurement à la naissance de l'obligation entre le débiteur initial et le créancier[87]. Or, en l'espèce, l'engagement du constructeur est antérieur à la naissance de l'obligation. Cet écueil ne nous semble pas rédhibitoire. D'une part, la reprise de dette envisagée ici prend la forme d'une stipulation pour autrui qui peut être conclue avant la naissance de l'obligation[88]. D'autre part, rien ne s'oppose à ce que la reprise de dette – comme la stipulation pour autrui – soit soumise à une condition[89]. *In casu*, on peut donc considérer que l'engagement du constructeur est subordonné à la

---

83 Cf. ENGEL, p. 898 N 280 ; PROBST, *Intro. art. 175-183 CO,* N 20.

84 Cf. KRAUSKOPF, pp. 55 ss N 212 ss.

85 Cf. ENGEL, p. 421 N 92 ; TEVINI, *Art. 112 CO* N 7.

86 Cf. ENGEL, p. 421 N 92 ; KRAUSKOPF, pp. 123 ss N 482 ss ; PROBST, *Intro. art. 175-183 CO,* N 10 et 2 ; TEVINI, *Art. 112 CO* N 7.

87 Cf. ENGEL, pp. 902 ss N 281 ; PROBST, *Intro. art. 175-183 CO,* N 7.

88 Cf. KRAUSKOPF, p. 46 N 170 ss.

89 Cf. ENGEL, p. 898 N 280 ; KRAUSKOPF, pp. 273 ss N 1069 ss ; PROBST, *Intro. art. 175-183 CO,* N 20.

réalisation d'une condition suspensive (art. 151 ss CO) : la survenance d'un accident de la circulation lorsque le véhicule est en mode autonome.

Enfin, dans toutes les hypothèses envisagées le consentement du lésé n'est pas un prérequis[90]. Pour ce qui est de l'exécution par un tiers de la garantie, le lésé n'a pas d'intérêt à ce que le détenteur exécute personnellement son obligation[91]. En cas de reprise de dette doublée d'une stipulation pour autrui, le tiers lésé voit sa position renforcée et n'est soumis à aucune obligation ni aucune charge[92]. Toutefois, le tiers lésé n'est pas contraint d'accepter la prestation stipulée en sa faveur[93].

2.3. *Disparition programmée de la responsabilité du détenteur ?*

On peut se demander si la « clause Volvo » exposée ci-dessus n'est pas de nature à remettre en cause la responsabilité du détenteur consacrée par la LCR.

Ladite clause présente un avantage certain pour le détenteur. Cependant, son attractivité pour le lésé est moins évidente. L'art. 58 LCR prévoit une responsabilité causale en faveur du lésé victime d'un accident de la circulation routière. Il suffit à ce dernier de démontrer son dommage, l'emploi d'un véhicule automobile, le lien de causalité entre le préjudice et l'emploi du véhicule pour que le détenteur dudit véhicule soit responsable. À l'inverse, la « clause Volvo » impose que le lésé établisse la responsabilité du détenteur, que l'accident est survenu en mode autonome, enfin, et l'existence d'une stipulation pour autrui parfaite en sa faveur. Même si la preuve de la première condition ne devrait pas poser de problème, que celle de la seconde pourrait être facilitée par des systèmes d'enregistrement à bord (de type « boîtes noires » que l'on retrouve dans les aéronefs), le lésé n'a aucun moyen, sauf s'il est renseigné par le détenteur, de démontrer l'existence et les modalités d'une éventuelle stipulation pour autrui.

Dans tous les cas, on voit mal pourquoi le lésé entreprendrait ces démarches dans la mesure où, pour un résultat identique, la mise en œuvre de la « clause Volvo » serait beaucoup plus difficile[94]. D'autant plus que, compte tenu du droit d'action directe du lésé contre l'assureur (art. 65 LCR), la garantie de solvabilité que représente le constructeur n'a pas réellement d'intérêt.

---

90 Cf. ENGEL, p. 421 N 92 ; KRAUSKOPF, pp. 72 ss N 291 ss ; PROBST, *Intro. Art. 175 CO,* N 1 ; TEVINI, *Art. 112 CO* N 16 ; WEBER, *Art. 112 CO*, N 109 ss.

91 Cf. FABIENNE HOHL, *Intro art. 68-83 CO* et *Art. 68 CO*, in : F. Werro/L. Thévenoz (édit.), *CoRo Code des obligations I* (art. 1-529 CO), 2e éd., Bâle 2012, respectivement N 2 et N 3 ss.

92 Pour la reprise cumulative de dette : cf. PROBST, *Intro. art. 175-183 CO,* N 8 ; pour la reprise de dette interne : PROBST, *Intro. Art. 175 CO,* N 1.

93 Cf. ENGEL, p. 426 N 94 ; KRAUSKOPF, pp. 294 ss N 1157 ss ; TEVINI, *Art. 112 CO* N 23 et 11 ; WEBER, *Art. 112 CO*, N 116.

94 Le détenteur sera vraisemblablement aussi impliqué dans la procédure entre le lésé et le constructeur ce qui ne manquera pas de compliquer le déroulement de cette dernière.

Par ailleurs, on ignore si la « clause Volvo » ne vise que les situations dans lesquelles le véhicule a exercé une influence directe dans la survenance de l'accident ou si elle s'applique plus généralement.

En l'état actuel, on peut donc envisager une coexistence entre la responsabilité causale de l'article 58 LCR et la « clause Volvo ». Le lésé disposerait d'un concours d'actions (l'une délictuelle, l'autre contractuelle) à l'encontre du détenteur et du constructeur. Toutefois, si la « clause Volvo » peut être une option distincte de la responsabilité du détenteur, sa mise en œuvre est complexe et donc peu attractive pour le lésé, ce d'autant plus lorsque le constructeur est une société étrangère et que se posent des problèmes de for et de droit applicable.

Par conséquent, la « clause Volvo » ne remet pas formellement en cause la responsabilité du détenteur du véhicule. Cela étant, on peut néanmoins considérer qu'au-delà d'un simple coup de publicité, la « clause Volvo » est une sorte de signal des constructeurs automobiles à l'attention du législateur : les modalités de responsabilité pourraient être appelées à évoluer[95].

3. Fonction préventive du droit de la RC

Outre la compensation classique, la prévention redevient une composante essentielle du droit de la RC, à plus forte raison que l'évolution, notamment technologique, peut être à l'origine de dommages dont l'ampleur et la nature sont susceptibles de rendre une réparation totale bien difficile. Que l'on songe aux préjudices de masse ou encore aux préjudices écologiques. Il s'impose alors de tout entreprendre pour en éviter la survenance, et le droit de la RC peut apporter à cet égard une contribution appréciable.

Dans l'avant-projet français de révision du droit de la responsabilité civile (2017), la prévention fait l'objet d'une forme de consécration. Selon cette conception, le juge peut prescrire toute mesure permettant de prévenir le dommage ou de faire cesser un trouble illicite[96]. Il est vrai que l'on a en vue en particulier le préjudice écologique ; pour autant, la réflexion revêt un caractère plus général. En droit suisse, certains ont exprimé l'avis selon lequel la prévention serait devenue la fonction principale du droit de la RC, considérant

[95] À remarquer cependant que selon une communication récente, le même constructeur paraît revenir sur son engagement, cf. LETEMPS.CH, article du 14.11.18, *Y a-t-il un pilote dans l'auto ?*, p. « https://www.letemps.ch/lifestyle/y-atil-un-pilote-lauto » (consulté le 22 juillet 2019).

[96] Cf. art 1266 du projet : « en matière extracontractuelle, indépendamment de la réparation du préjudice éventuellement subi, le juge peut prescrire les mesures raisonnables propres à prévenir le dommage ou faire cesser le trouble illicite auquel est exposé le demandeur ».

en particulier le fait que la majorité des dommages sont désormais pris en charge par les institutions d'assurance sociale[97].

La fonction préventive du droit de la RC renvoie à des considérations de nature économique[98]. Si celui qui est à l'origine d'un acte susceptible d'entraîner des conséquences dommageables ne les prend pas en compte dans ses décisions, le coût privé de son activité est inférieur au coût social ; le niveau de prévention n'est pas optimal. Pour atteindre un niveau de prévention socialement approprié, il faut imposer à l'auteur la prise en compte du coût des conséquences extérieures dommageables qu'il fait subir aux autres[99].

Ce résultat peut être obtenu par deux voies. Cela peut intervenir d'abord au travers d'instruments réglementaires (l'auteur est tenu au respect de certaines normes de comportement). Mais on peut aussi laisser à l'auteur une marge de manœuvre plus large, tout en définissant des mécanismes économiques qui l'incitent, sur un plan privé, à adopter un comportement efficient. Ces instruments économiques peuvent être de trois types : les taxes, les permis d'émission négociables (atteintes à l'environnement), ainsi que les règles de la responsabilité civile. Ces dernières reposent alors sur la crainte de supporter des coûts a posteriori, ce qui peut inciter l'agent à adopter un niveau de prévention optimal a priori.

L'hypothèse est donc la suivante : si l'on veut éviter autant que faire se peut les dommages liés à l'utilisation de véhicules autonomes, il convient de faire porter le poids de la responsabilité prioritairement et directement à celui qui crée le risque et qui est en mesure d'en éviter la survenance. Ainsi considérée, cette responsabilité ne peut donc porter sur l'utilisateur, mais bien sur le constructeur du véhicule autonome, ou celui qui élabore le logiciel de pilotage automatique s'il s'agit d'une entité juridique différente. Ce glissement peut intervenir de deux manières : soit par une extension de la notion de détenteur en direction du constructeur (le constructeur est celui qui met le risque en circulation, qui en tire profit et exerce la maîtrise de fait), soit par l'institution d'une responsabilité indépendante à charge du constructeur.

On pourra objecter que le constructeur peut être, aujourd'hui déjà, pris à partie au travers du recours de l'assureur RC du détenteur. Il faut cependant considérer qu'une responsabilité de « seconde ligne » exerce un effet dissuasif moins puissant qu'une responsabilité directe. La responsabilité dont il est fait

---

97 Cf. à cet égard WALTER FELLMANN/ANDREA KOTTMANN, *Schweizerisches Haftpflichtrecht - Band I. Allgemeiner Teil sowie Haftung aus Verschulden und Persönlichkeitsverletzung, gewöhnliche Kausalhaftungen des OR, ZGB und PrHG*, Berne 2012, p. 3 N 8 ; FRANZ WERRO, *La responsabilité civile*, 3e éd., Berne 2017, p. 10 N 21.

98 En plus, notamment, de considérations à caractère moral, cf. à cet égard FELLMANN/KOTTMANN, p. 28 N 71 ; WERRO, p. 26 N 49.

99 Certains parlent à cet égard « d'internalisation de l'externalité négative », cf. BIDENAM KAMBIA-CHOPIN, *Règles de responsabilité civile et prévention des risques environnementaux*, Revue d'économie politique 2/2007 (Vol. 117), pp. 285 ss.

état dans une action récursoire est en effet indirecte : elle peut être affectée par les conditions de l'exercice du droit de recours ou de la subrogation ; elle peut être partagée cas échéant avec d'autres coresponsables, peut devoir s'exercer dans un contexte de droit international, *etc.*, autant de facteurs susceptibles de faire d'une telle action une procédure aléatoire qui, tout en réduisant la menace d'être tenu à la réparation, en diminue la vertu préventive. Faire répondre le constructeur directement face à la victime constitue de ce point de vue une mesure autrement efficace. Mais il est vrai que l'effet attendu dépendra finalement aussi des conditions auxquelles ce constructeur répond à l'égard du lésé.

4. Harmonisation internationale des solutions

La circulation routière est un phénomène de fait qui ignore aujourd'hui les frontières nationales. Nombre d'accidents de la circulation routière revêtent un caractère international. Le règlement de ces sinistres est facilité par des directives communautaires sur l'assurance, et par des conventions internationales permettant de déterminer la loi applicable. Ces mécanismes de réparation reposent avant tout sur des modalités d'assurance. Ce sont les assureurs RC des détenteurs (ou assureurs automobiles) qui interviennent à l'égard des victimes, au besoin par des systèmes de représentation dans les États membres dans lesquels le détenteur s'est rendu pour y causer un accident[100]. Il reste que cela suppose en particulier une compréhension commune de la notion de détenteur assuré dans les différents ordres juridiques, ce qui est actuellement plus ou moins le cas[101]. Des différences apparaissent, aujourd'hui déjà, sur les conditions de cette responsabilité, ainsi que sur les modalités de la responsabilité du conducteur. Si l'on imagine demain un réseau de véhicules connectés, on pourrait alors se trouver, faute de conceptions communes, face à une situation dans laquelle tel ordre juridique regardera l'utilisateur comme un détenteur, tandis que tel autre envisagera la situation différemment. Or, à défaut de garantir des fondements de responsabilité communs, les mécanismes relatifs à l'assurance, qui reposent précisément sur ces fondements, ne peuvent opérer de façon satisfaisante. Autrement dit, un réseau de véhicules connectés circulant en dehors de frontières nationales suppose une compréhension uniforme des règles de responsabilité et d'assurance.

---

[100] Sur le système, cf. p. ex. MARTIN METZLER, Das nationale Versicherungsbüroschweiz (NVB) und der Nationale Garantiefonds Schweiz (NGF) als Versicherungseinrichtungen zur Schadendeckung im nationalen und internationalen Strassenverkehr, in : M. Metzler/S. Fuhrer (édit.), Mélanges du Bureau National Suisse d'Assurance et du Fonds national Suisse de Garantie, Bâle 2000, pp. 251 ss.

[101] Cf. p. ex. les différences entre la notion de détenteurs selon la LCR et le droit français (responsabilité du fait des choses).

Il est loin d'être certain que la situation actuelle puisse constituer la base d'un régime futur. Et, si tel devait être le cas, cela supposerait à tout le moins confirmation par tous les ordres juridiques concernés. Or, nous avons vu déjà nombre de facteurs susceptibles d'influencer cette discussion. On peut douter dès lors que le régime de responsabilité du détenteur fasse sans autre l'objet d'une reprise par tous les ordres juridiques dans le contexte de l'utilisation de véhicules autonomes. D'autres traits communs à la mise en œuvre de véhicules autonomes pourraient bien apparaître peu à peu, qui pourraient conduire à un glissement vers une responsabilité du constructeur. On pourrait envisager également une responsabilité liée à l'utilisation de robots qui constituerait une catégorie supérieure ou, du moins, pourrait permettre l'identification des caractéristiques d'une éventuelle nouvelle forme de responsabilité.

5. *Lex Robotica ?*

La question de la responsabilité liée à l'utilisation de robot est considérée comme cruciale par les instances internationales. On observe à cet égard que les robots disposent de capacités décisionnelles grandissantes, leur conférant ainsi un certain degré d'autonomie de nature à bousculer les catégories juridiques traditionnelles, notamment la *summa divisio* qui oppose les choses aux personnes. Les robots pourraient constituer une catégorie additionnelle, dotée pour certains d'une personnalité juridique, pour devenir des « personnalités électroniques responsables ». On passerait ainsi d'une responsabilité du fait du robot à une responsabilité du robot ; resterait à examiner les questions de solvabilité. C'est dans ce sens que s'est prononcé par exemple le Parlement européen dans une recommandation adressée à la Commission en 2017[102]. À cela, d'autres opposent une conception selon laquelle la responsabilité, en fin de compte, incombera toujours à un être humain (« *human in command* »)[103], notamment pour des raisons qui tiennent au rôle préventif reconnu au droit de la RC. Un moyen terme pourrait consister à retenir à une responsabilité de toutes les personnes impliquées proportionnelle au niveau réel d'instructions données à un robot[104] ; mais il reste que si ce dernier augmente ses capacités d'apprentissage, il échappera progressivement à l'influence de son concepteur, puis de son formateur, ce qui reposera la question de sa propre personnalité ; ce phénomène n'a pas échappé aux organes de l'UE.

---

[102] Cf. Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil robotique (JO C 252 du 18 juillet 2018, pp. 239 ss (252)).

[103] Cf. Résolution du Parlement européen du 16 février 2017, p. 249 N 56.

[104] *Loc. cit.*

IV. Bibliographie

BENSOUSSAN Alain/BENSOUSSAN Jérémy, Le droit des robots, Paris 2015.

BERKE David, Products Liability in the Sharing Economy, Yale Journal on Regulation 33/II/2016, pp. 603 ss.

BREHM Roland, La responsabilité civile automobile, 2e éd., Berne 2010.

BRULHART Vincent, Droit des assurances privées, 2e éd., Berne 2017.

BRULHART Vincent, Sign up & drive : quelles assurances ? Remarques sur l'émergence de l'économie collaborative et ses dépendances envers l'assurance, in : B. Kahil-Wolff Hummer/J. Juge (édit.), Le droit social numérique, Berne 2018, pp. 43 ss.

BUSSY André et al., CS CR commenté, 4e éd., Bâle 2015.

CASSART Alexandre, Aéronefs sans pilote, voitures sans conducteur : la destination plus importante que le voyage, in : H. Jacquemin/A. de Streel (édit.), L'intelligence artificielle et le droit, Bruxelles 2017, pp. 319 ss.

COMITÉ MARITIME INTERNATIONAL, CMI International working group position paper on unmanned ships and the international regulatory framework, p. « https://comitemaritime.org/wp-content/uploads/2018/05/CMI-Position-Paper-on-Unmanned-Ships.pdf » (consulté le 22 juillet 2019).

DÄHLER Manfred/SCHAFFHAUSER René (édit.), Handbuch Strassenverkehrsrecht, Bâle 2018.

DANESI René et al., Rapport d'information du Sénat sur la stratégie de l'Union européenne pour le véhicule autonome N 117 du 27 novembre 2017.

BJORTUFT ELLINGSEN Christian/TONDEL Espen, Maritime law in the wake of unmanned Vessel, p. « https://svw.no/en/news/news/2017/august/maritime-law-in-the-wake-of-the-unmanned-vessel/ » (consulté le 22 juillet 2019).

ENGEL Pierre, Traité des obligations en droit suisse, 2e éd., Berne 1997.

FANTI Sébastien/MIZEL Cédric, L'homologation de nouveaux systèmes techniques routiers et la problématique des voitures intelligentes, Circulation routière 2/2015, pp. 10 ss.

FELLMANN Walter/KOTTMANN Andrea, Schweizerisches Haftpflichtrecht - Band I. Allgemeiner Teil sowie Haftung aus Verschulden und Persönlichkeitsverletzung, gewöhnliche Kausalhaftungen des OR, ZGB und PrHG, Berne 2012.

FOX Sarah Jane, The Rise of the Drones: Framework and Governance-Why risk it ?, The Journal of Air Law and Commerce vol. 82, 2017, pp. 683 ss.

HOHL Fabienne, Art. 68 CO, in : L. Thévenoz/ F. Werro (édit.), CoRo Code des obligations I (art. 1-529 CO), 2e éd., Bâle 2012.

HOHL Fabienne, Intro art. 68-83 CO, in : L. Thévenoz/F. Werro (édit.), CoRo Code des obligations I (art. 1-529 CO), 2e éd., Bâle 2012.

HUTTUNEN Mikko, Unmanned, Remotey Piloted, or Something Else ? Analysing the Terminological Dogfight, Air & Space Law 42, 2017, pp. 349 ss.

JACQUEMIN Herve/DE STREEL Alexandre (édit.), L'intelligence artificielle et le droit, Bruxelles 2017.

JOSITSCH Daniel/SCHWARZENEGGER Christian/WOHLERS Wolfgang (édit.), Festschrift für Andreas Donatsch, Zurich 2017.

KAMBIA-CHOPIN Bidenam, Règles de responsabilité civile et prévention des risques environnementaux, Revue d'économie politique 2/2007 (Vol. 117), pp. 285 ss.

KAHIL-WOLFF HUMMER Bettina/JUGE Johan (édit.), Le droit social numérique, Berne 2018.

KRAUSKOPF Patrick, Der Vertrag zugunsten Dritter, thèse, Fribourg 2000.

LEFIGARO.FR, Voiture autonome, quelle responsabilité en cas d'accident ?, p. « http://voiture-autonome.lefigaro.fr/voiture-autonome-quelle-responsabilite-cas-daccident/ » (consulté le 22 juillet 2019).

LEMONDE.FR, article du 08.1015, Voitures sans chauffeur : Volvo assume ses responsabilités en cas d'accident, p. « https://lesclesdedemain.lemonde.fr/technologie/voiture-sans-chauffeur-volvo-assume-ses-responsabilites-en-cas-d-accident_a-88-5353.html » (consulté le 22 juillet 2019).

LETEMPS.CH, article du 14.11.18, Y a-t-il un pilote dans l'auto ?, p. « https://www.letemps.ch/lifestyle/y-atil-un-pilote-lauto » (consulté le 22 juillet 2019).

LESECHOS.FR, article du 05.06.18 de R. Demichelis, Volvo veut endosser la responsabilité de ses voitures autonomes, p. « https://www.lesechos.fr/intelligence-artificielle/veille-technologique/0301765363885-dans-la-presse-etrangere-volvo-veut-une-voiture-autonome-responsable-2181423.php » (consulté le 22 juillet 2019).

MEIER Peter-Martin, Bringt automatisierte Fahrt auch Wohlfahrt ?, Circulation routière 1/2018, pp. 49 ss.

METZLER Martin, Das nationale Versicherungsbüroschweiz (NVB) und der Nationale Garantiefonds Schweiz (NGF) als Versicherungseinrichtungen zur Schadendeckung im nationalen und internationalen Strassenverkehr,

in : M. Metzler/S. Fuhrer (édit.), Mélanges du Bureau National Suisse d'Assurance et du Fonds national Suisse de Garantie, Bâle 2000, pp. 251 ss.

METZLER Martin/FUHRER Stephan (édit.), Mélanges du Bureau National Suisse d'Assurance et du Fonds national Suisse de Garantie, Bâle 2000.

MÜLLER Christoph/GRETILLAT Jonathan, Le recours de l'assurance RC du détenteur contre le constructeur en cas de dysfonctionnement d'un système d'aide à la conduite de véhicule, Circulation routière 2/2015, pp. 37 ss.

OACI-COMITE JURIDIQUE, Questionnaire sur les aspects juridiques des systèmes d'aéronefs télépilotés, p. « https://www.icao.int/Meetings/LC37/Documents/LC37%20WP%202-1%20FR%20Remotely%20Piloted%20Aircraft.pdf » (consulté le 22 juillet 2019).

OFFICE FÉDÉRAL DE L'AVIATION CIVILE (OFAC), Fiche d'information Régime d'autorisation suisse en matière de drone, p. « https://www.bazl.admin.ch/bazl/fr/home/bonasavoir/drones-et-modeles-reduits/autorisations-d_exploiter-des-drones-au-dessus-dun-rassemblement.html » (consulté le 22 juillet 2019).

OFFICE FÉDÉRAL DES ROUTES (OFROU), Aide-mémoire concernant la réalisation de projets pilotes en Suisse du 05.12.2017, p. « https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/pilotversuche.html » (consulté le 22 juillet 2019).

PALMERINI Erica et al., D6.2 Guidelines on Regulating Robotics - RoboLaw, Pise 2014.

PERRITAZ Vincent, Le concours d'actions et la solidarité, thèse Fribourg, Zurich 2017.

PROBST Thomas, Art. 175 CO, in : L. Thévenoz/F. Werro (édit.), CoRo Code des obligations I (art. 1-529 CO), 2e éd., Bâle 2012.

PROBST Thomas, Intro. art. 175-183 CO, in : L. Thévenoz/F. Werro (édit.), CoRo Code des obligations I (art. 1-529 CO), 2e éd., Bâle 2012.

RPAS WORKING GROUP DE L'OFAC, Les drones en Suisse – Un nouveau défi, rapport du 7 février 2016, p. « https://www.bazl.admin.ch/bazl/fr/home/bonasavoir/drones-et-modeles-reduits.html » (consulté le 22 juillet 2019).

TEVINI DU PASQUIER Silvia, Art. 112 CO, in : L. Thévenoz/F. Werro (édit.), CoRo Code des obligations I (art. 1-529 CO), 2e éd., Bâle 2012.

THEVENOZ Luc/WERRO Franz (édit.), CoRo Code des obligations I (art. 1-529 CO), 2e éd., Bâle 2012.

THOMMEN Marc/MATJAZ Sophie, Die Fahrlässigkeit im Zeitalter autonomer Fahrzeuge, in : D. Jositsch/C. Schwarzenegger/W. Wohlers (édit.), Festschrift für Andreas Donatsch, Zurich 2017, p. 273 ss.

WEBER Rolf, Art. 112 CO, BeKomm. Band VI: Obligationenrecht 1. Abteilung : Allgemeine Bestimmungen. 6. Teilband : Beziehungen zu Dritten (Art. 110-113 OR), Berne 2002.

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

WERRO Franz/PERRITAZ Vincent, La remise en cause de l'ordre des recours de l'art. 51 al. 2 CO, PJA 10/2018, pp. 1179 ss.

WERRO Franz/PERRITAZ Vincent, Les véhicules connectés : un changement de paradigme pour la responsabilité civile?, in : F. Werro/T. Probst (édit.), Journées du droit de la circulation routière 23 - 24 juin 2016, Berne 2016, pp. 1 ss.

WERRO Franz/PROBST Thomas (édit.), Journées du droit de la circulation routière 23 - 24 juin 2016, Berne 2016.

ZURKINDEN Nadine, AI and driverless cars : from international law to tests runs in Switzerland to criminal liability risks, in : H. Jacquemin/A. de Streel (édit.), L'intelligence artificielle et le droit, Bruxelles 2017, pp. 341 ss.

Les nouvelles technologies et la responsabilité des avocats

La cybersécurité et l'intelligence artificielle

Jérôme Gurtner, docteur en droit*

Table des matières

I. Introduction générale 46
II. La responsabilité des avocats et la cybersécurité 46
A. Introduction 47
B. Les menaces et les vulnérabilités les plus fréquentes 48
C. Les conséquences d'une atteinte à la cybersécurité 49
1. Les premières répercussions 49
2. La responsabilité disciplinaire 49
3. La responsabilité pénale 53
4. La responsabilité civile 54
5. La responsabilité en matière de protection des données 57
D. Les recommandations pour réduire les risques 61
III. La responsabilité des avocats et l'intelligence artificielle 64
A. Introduction 64
B. Quelques applications utilisant l'IA 65
1. La révision de documents contractuels 65
2. La justice prédictive 66
3. La recherche juridique 68
4. Les agents ou robots conversationnels (chatbots) 69
C. Les conséquences de l'IA pour les avocats 70

* 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.

D. L'utilisation des nouvelles technologies en tant que devoir de diligence 71
E. L'imputation de la responsabilité 73
1. Le contexte 73
2. La notion d'agent et son degré d'autonomie 73
3. Réflexions concernant le droit actuel et le droit désirable 76
F. Les « boîtes noires » et l'indépendance des avocats 83
1. L'opacité des algorithmes 83
2. La tentative de rendre les algorithmes transparents 86
3. Les conséquences pour les avocats 89
IV. Conclusions 90
V. Table des abréviations 92
VI. Bibliographie 94

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*]

La responsabilité des hébergeurs pour *fake news*

Dr Michel José Reymond[1]

Table des matières

I. Introduction 105
II. Définition du phénomène lié aux *fake news* 107
A. Exemples pratiques 108
B. Identification d'une définition 109
C. Enjeux du point de vue du droit de la responsabilité civile 110
III. État actuel du droit suisse 111
A. Actions défensives 111
B. Actions réparatrices 113
IV. Importance pratique de l'autorégulation 115
V. Conclusion 116
VI. Bibliographie 117

I. Introduction

Le phénomène de désinformation de masse permis par les outils numériques est aujourd'hui au centre de nombreuses préoccupations et de nombreux débats. Aux Etats-Unis, où le terme *fake news* est depuis 2016 entré dans le langage populaire, ce phénomène a été reconnu portant possiblement un danger pour le bon déroulement de la démocratie. En France, où ce phénomène est également désigné sous le terme de « infox », le législateur a adopté en décembre 2018 une loi pour spécifiquement lutter contre la désinformation numérique lors des périodes électorales. La loi prévoit notamment une procédure accélérée permettant de requérir le retrait ou le maintien dans les 48 heures d'une fausse nouvelle ou d'une information

[1] Docteur en droit de l'Université de Genève ; avocat stagiaire. Le présent écrit constitue le pendant écrit de la présentation prononcée par l'auteur le 4 septembre 2018 à l'occasion de la journée de la responsabilité civile, qui a eu lieu à l'Université de Genève. Certaines références – et notamment celles relatives au droit étranger – ont cependant été mises à jour depuis lors.

fallacieuse présente chez un hébergeur de l'internet par saisine d'un juge de référé[2]. En Angleterre, enfin, un rapport rendu en février 2019 par un comité de la House of Commons a conclu que la désinformation numérique était une problématique d'une ampleur telle qu'une réglementation des médias sociaux en ligne apparaissait comme nécessaire[3]. Le gouvernement anglais a par ailleurs tout aussi récemment débloqué un fonds de 18 millions de livres sterling destiné à encourager la lutte contre ce phénomène[4].

Les inquiétudes liées à la prolifération des *fake news* touchent également notre contrée. D'après un sondage publié par la firme Sotomo en octobre 2018, quatre personnes sur cinq en Suisse considèrent que la prolifération de *fake news* porte un danger pour la démocratie[5]. Quant au Conseil fédéral, celui s'est, à l'occasion d'un rapport sur le cadre juridique pour les médias sociaux publié en 2017, penché sur ce phénomène qu'il a reconnu comme ayant atteint une ampleur particulière[6]. Cela étant, et contrairement aux réactions trouvées en France et en Angleterre, il conclut que le droit suisse était, pour le moment en tout cas, apte à traiter de cette problématique sans qu'il y ait besoin d'une intervention législative.

La présente contribution – pendant écrit de la présentation faite par l'auteur le 4 septembre 2018 – se situe dans le sillage du rapport du Conseil fédéral de 2017 et se propose d'en décoder les conclusions. En particulier, il sera soutenu que les *fake news*, loin d'incarner une problématique nouvelle, se situent dans le prolongement de domaines déjà relativement bien encadrés par le droit, ceux-ci étant la responsabilité traditionnelle du droit de la presse et le droit de la responsabilité des hébergeurs en ligne.

En premier lieu, nous délimiterons le champ du phénomène désigné par le terme *fake news* afin d'en saisir les enjeux pour le droit de la responsabilité civile (II.). Ensuite, un bref tableau des moyens offerts aux victimes de *fake news* par le droit suisse de la responsabilité civile sera dressé (III.). Enfin, le

---

2 Loi no 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, Journal officiel de la République française n°0297 du 23 décembre 2018.

3 *Disinformation and 'fake news': Final Report*, House of Commons, Digital, Culture, Media and Sport Committee, 18 février 2019, HC 1791 ; voir p. ex. p. 89, par. 3 : "*There is now an urgent need to establish independent regulation. We believe that a compulsory Code of Ethics should be established, overseen by an independent regulator, setting out what constitutes harmful content. The independent regulator would have statutory powers to monitor relevant tech companies ; this would create a regulatory system for online content that is as effective as that for offline content industries*".

4 *UK Steps up fight against fake news,* Communiqué de presse du 7 juillet 2019 du gouvernement du Royaume-Uni, disponible sur https://www.gov.uk/government/news/uk-steps-up-fight-against-fake-news (25.07.19).

5 Accessible sur : https://sotomo.ch/site/wp-content/uploads/2018/10/Studie-Wahrheit-und-L%C3%BCge-stapferhaus.sotomo.pdf (25.07.19).

6 *Un cadre juridique pour les medias sociaux : Nouvel état des lieux*, Rapport du Conseil fédéral du 10 mai 2017.

rôle majeur que joue l'autoréglementation des hébergeurs sera mis en exergue (IV.) avant de mener l'auteur à formuler quelques conclusions (V.).

II. Définition du phénomène lié aux *fake news*

La définition du phénomène désigné par le terme *fake news* est, à deux égards, un exercice aussi délicat que controversé.

En premier lieu, le terme *fake news* manque de précision et est empreint de subjectivité. Aux États-Unis, ce terme est employé indifféremment pour désigner des théories conspirationnistes tendant à la manipulation de l'information mais également pour discréditer les nouvelles rapportées par des organes de presse établis et reconnus. A ce titre, le compte Twitter du président Donald Trump, partagé entre la promotion de telles théories[7] et la condamnation de CNN et de la BBC en tant qu'ennemis de la démocratie, en est un exemple frappant[8]. Même en dehors du contexte de la politique américaine, le terme de *fake news* est ambigu. Il mêle d'un même trait l'inexactitude journalistique, le canular et la tromperie informationnelle, le rendant sémantiquement peu utile pour isoler et décrire le phénomène de désinformation virale qu'il tente de désigner[9]. C'est à ce titre que la Commission d'enrichissement de la langue française a recommandé l'emploi du néologisme « infox », mélange d'information et d'intoxication, pour désigner plus précisément la désinformation mensongère[10].

En deuxième lieu, il faut garder à l'esprit que la publication d'informations trompeuses, tout autant que la manipulation de l'opinion publique par le biais de propagande, ne sont pas des pratiques nouvelles, et que ce domaine est déjà saisi par les règles traditionnelles de la protection de la personnalité et du droit de la presse. La problématique posée par les *fake news* n'est donc pas en soi novatrice et sa délimitation peut s'opérer par une identification de ses caractéristiques saillantes par rapport aux pratiques de désinformation déjà existantes.

---

7 Voir p. ex. son message du 6 août 2016, dans lequel il a prétendu que le certificat de naissance du président d'alors, Barack Obama, était falsifié alors qu'il n'en était rien ; disponible à l'adresse suivante : https://twitter.com/realdonaldtrump/status/232572505238433794?lang=en (25.07.19).

8 Voir p. ex. son message du 13 novembre 2018 : " The story in the New York Times concerning North Korea developing missile bases is inaccurate. We fully know about the sites being discussed, nothing new - and nothing happening out of the normal. Just more Fake News. I will be the first to let you know if things go bad!", disponible à l'adresse suivante : https://twitter.com/realDonaldTrump/status/1062391577807601664 (25.07.19).

9 LAURENT.

10 « Recommandation sur les équivalents français à donner à l'expression fake news », Commission d'enrichissement de la langue française, Journal Officiel de la République Française, 4 octobre 2018, Texte 113 sur 142, NOR CTNR1826048K.

Ces deux écueils étant exposés, nous allons, dans un premier temps, exposer trois exemples de *fake news* qui sont illustratifs de ce phénomène (A.). Ensuite, nous allons, sur la base des exemples présentés, tenter de dégager une définition des *fake news*. (B.). Enfin, nous aborderons les enjeux spécifiques liés à cette problématique dans le contexte de la responsabilité civile.

A. Exemples pratiques

L'exemple de *fake news* le plus frappant est l'incident dit du *Pizzagate,* qui eut lieu en 2016 dans le contexte des élections présidentielles américaines[11]. En mars de cette année, le compte courriel appartenant à John Podesta, alors chef de campagne de la candidate Hillary Clinton, fut compromis par des pirates informatiques. De mars à novembre 2016, le contenu de ses courriels a été progressivement révélé au public par le biais du site WikiLeaks[12]. Suite à cela, plusieurs utilisateurs sur le média social Twitter, ainsi que sur les forums en ligne 4chan et Reddit, ébruitèrent une rumeur selon laquelle les courriels reproduits sur WikiLeaks contiendraient des messages cachés et/ou codés laissant entendre que les membres du parti démocrate américain, et notamment ceux liés à la campagne électorale de Hillary Clinton, exploitaient un réseau de pédophilie et de traite d'êtres humains. S'appuyant sur la ressemblance entre le terme *Cheese Pizza*, retrouvé dans les courriels révélés par WikiLeaks, et *Child Pornography*, les partisans de cette théorie avancèrent que le centre des opérations de ce réseau se trouvait dans une pizzeria nommée le Planet Ping-Pong et située à Washington D.C. Cette théorie du *Pizzagate* fut partagée à de nombreuses reprises sur les médias sociaux et des forums en ligne pour ensuite être reprise par des sites de nouvelles affiliés à l'extrême droite américaine, et notamment le site Infowars.com[13]. Elle finit par atteindre une ampleur telle que la presse généraliste, et notamment la BBC, y consacrèrent des articles démontrant sa fausseté[14]. A ce moment, cependant, il était trop tard car le *Pizzagate* avait déjà trouvé crédit auprès d'une partie du grand public. Ainsi, le 4 septembre 2016, un habitant de la Caroline du Nord se déplaça jusqu'à Washington D.C. et, ayant pour but de libérer les enfants supposément enfermés dans le Planet Ping-Pong, attaqua le restaurant muni d'une arme à feu pour finalement se rendre compte qu'aucun réseau de traite d'êtres humains ne s'y trouvait[15].

---

11 Pour un résumé critique de cet incident, voir WENDLING.

12 https://wikileaks.org/podesta-emails/ (25.07.19).

13 L'exploitant du site en question s'est par la suite distancé du Pizzagate, en s'excusant d'avoir véhiculé cette fausse nouvelle, voir DOUBEK.

14 WENDLING.

15 GOLDMAN.

Suite au *Pizzagate*, les théories conspirationnistes avancées au sujet du parti démocrate américain se sont multipliées. Dans ce contexte, on mentionnera la théorie dite *The Storm*, principalement véhiculée par un utilisateur du forum en ligne 4chan, identifié sous le nom de « Q » et qui se dit être en possession de documents secrets liés au cabinet du président américain Donald Trump. D'après ses dires, ledit président serait impliqué dans une guerre secrète contre le parti démocrate, plus particulièrement contre Hillary Clinton et l'ex-président Barack Obama, qui seraient liés à de malversations diverses allant de la traite d'êtres humains au satanisme[16].

Les *fakes news* ne sont cependant pas exclusivement liées à la vie politique américaine et peuvent également être employées afin de manipuler les marchés financiers. Par exemple, en juin 2017, un billet posté sur le forum en ligne 4chan annonça le décès de Vitalik Buterin, l'un des architectes de la cryptomonnaie Ethereum. Suite à cette nouvelle, le cours de ladite cryptomonnaie chuta fortement jusqu'au moment où l'intéressé prouva par photographie sur Twitter qu'il était bel et bien en vie. De façon générale, le monde des cryptomonnaies est par ailleurs un terrain fertile pour les *fake news* du fait de l'absence de législation venant réglementer la conduite des acteurs qui l'animent[17].

B. Identification d'une définition

Les trois exemples ci-dessus nous permettent d'isoler plusieurs caractéristiques propres aux *fake news*, qui en font une catégorie spécifique de fausses nouvelles. Ces caractéristiques sont les suivantes :

- **But de manipulation de l'opinion publique.** Contrairement à la simple erreur factuelle faite de bonne foi par un organe de presse, les *fake news* tendent à la manipulation de l'opinion publique par la révélation d'une fausse nouvelle choquante ou surprenante visant à provoquer une réaction émotionnelle chez le public visé. C'est le cas des faits entourant le *Pizzagate* et par *The Storm*. S'agissant de mettre à jour une classe politique secrète qui serait mêlée aux pires malversations, ces *fake news* étaient à même de choquer le public, d'exploiter son intérêt naturel pour les théories conspirationnistes, et d'ainsi pousser ce même public à l'action, comme ce fut le cas pour l'attaque du Planet Ping-Pong. L'exemple de la *fake news* véhiculée au sujet d'Ethereum, a pareillement exploité l'effet de panique provoqué par la nouvelle de la mort de Vitalik Buterin afin de manipuler le cours de cette cryptomonnaie.

16 WONG.

17 DARBELLAY/REYMOND, p. 60.

- **Propagation virale par le biais des technologies de l'information.** Les *fake news* n'ont pas de point d'origine aisément identifiable tel qu'un article de presse ou un billet de blog. Au contraire, elles trouvent leur source dans des séries de *tweets,* de billets, et d'articles de blog propagandistes, éparpillés au travers de réseaux sociaux, de forums de discussion en ligne, et de blogs. Ces divers points d'information s'accumulent de façon virale de manière à donner corps à la fausse nouvelle et à lui conférer une apparence de légitimité, ce qui lui permet par la suite de s'infiltrer dans la conscience du grand public. De façon corollaire, les *fake news* ne peuvent pas être attribuées à un ou plusieurs auteurs identifiables. Elles sont le fruit itératif d'une pluralité d'auteurs anonymes, usagers de médias sociaux ou de forums en ligne, qui, chacun, reproduisent leur contenu à l'attention de leur réseau en y ajoutant éventuellement de nouveaux éléments.

La définition proposée ci-dessus rejoint en substance celle développée par le Conseil fédéral dans son rapport de 2017 sur les médias sociaux, dans lequel cet organe définit les *fake news* en tant qu'*« informations factuelles erronées exprimées de mauvaise foi et (1) diffusées dans un but de manipulation politique, pour des intérêts financiers ou d'autres motifs personnels, et (2) qui tirent leur puissance de la nouvelle dynamique des réseaux sociaux (anonymat des auteurs, attention prêtée aux choses surprenantes, diffusion virale, c'est-à-dire extrêmement rapide et intensive)* »[18].

C. Enjeux du point de vue du droit de la responsabilité civile

Au vu des considérations qui précèdent, la problématique des *fake news* soulève deux enjeux pour une victime souhaitant agir par la voie de la responsabilité civile :

- **Identification de la partie défenderesse.** Les *fake news* étant le produit d'une pluralité d'auteurs anonymes, probablement dispersés géographiquement, et agissant chacun à titre individuel, il sera difficile, voire pratiquement impossible, de les retrouver afin d'engager leur responsabilité civile. En conséquence, la victime de *fake news* s'adressera plutôt aux acteurs qui hébergent le contenu des *fake news* sur le réseau internet, comme par exemple les plates-formes d'hébergement telles que Youtube ou les réseaux sociaux tels que Twitter ou Facebook, ainsi

[18] *Un cadre juridique pour les medias sociaux : Nouvel état des lieux*, Rapport du Conseil fédéral du 10 mai 2017, p. 11-12.

que les acteurs qui facilitent la diffusion des *fake news* auprès du grand public, comme par exemple les moteurs de recherche tels que Google[19].

- **Modalités du retrait des *fake news*.** Plus que les dommages-intérêts, la victime d'une *fake news* sera surtout intéressée à ce la *fake news* soit retirée le plus rapidement possible du réseau afin de faire cesser l'atteinte à sa réputation. Dans ce contexte, les modalités de ce retrait ainsi que la célérité et le coût de la procédure y afférant seront d'une importance majeure pour celle-ci.

En somme, les enjeux soulevés par les *fake news* ne sont pas fondamentalement différents de ceux identifiés en matière de responsabilité des hébergeurs de l'internet, et en particulier en ce qui concerne les atteintes à la propriété intellectuelle ou l'exercice du droit à l'oubli[20]. Nous y reviendrons plus bas.

III. État actuel du droit suisse

Le droit suisse ne dispose pas de législation spéciale encadrant la responsabilité civile des hébergeurs. En conséquence, la problématique des *fake news* est régie par les règles générales du droit de la protection de la personnalité, soit les articles 28ss du Code Civil[21]. En particulier, on considérera, d'une part, les actions défensives de l'art. 28 al. 1 CC (A.) et, d'autre part, les actions réparatrices de l'art. 28 al. 3 CC (B.).

A. Actions défensives

En matière de *fake news*, l'action en cessation prévue par l'art. 28a al. 1 CC revêt une importance toute particulière puisque qu'il s'agit du moyen pour la victime de faire retirer le contenu fallacieux publié à son encontre. Dans son arrêt *Tribune de Genève* de 2013, le Tribunal fédéral a confirmé que telle action était opposable aux intermédiaires informationnels qui accueillent le contenu illicite sur leurs serveurs pour les mettre à la disposition du grand public, que

---

19 La terminologie applicable à ces entités n'étant pas uniforme, nous emploierons le terme « hébergeur » pour les désigner collectivement. Pour une description de ces acteurs, voir WERRO/SONNEY, p. 120.

20 DE WERRA, p. 293-297. Voir également les *Geneva Internet Dispute Resolution Policies 1.0* (Topic 2) ainsi que les *Manila Principles on Intermediary Liability*, qui discutent des enjeux soulevés par la problématique de la responsabilité des hébegeurs en ligne et soumettent des principes directeurs pour y faire face.

21 Nous laissons ici volontairement de côté les aspects liés à la loi sur la protection des données, à la loi sur la concurrence déloyale, et aux lois afférentes à la protection de la propriété intellectuelle. En effet, les objets de ces lois ne touchent pas directement les aspects propres aux *fake news*.

nous qualifierons d'hébergeurs dits directs[22]. S'agissant de déterminer si la plate-forme de blog offerte par le site de la Tribune de Genève était tenue de retirer un billet portant atteinte à la personnalité d'un politicien, notre Haute Cour a notamment conclu que :

« […] [L]'atteinte à la personnalité résulte de la publication d'un texte rédigé par B._____ sur internet, soit plus précisément sur le blog de ce dernier, hébergé par X._____ sur son propre site internet. Si le prénommé est l'auteur originaire de la lésion aux intérêts personnels, la recourante, en lui fournissant l'espace internet sur lequel il a pu créer son blog, a permis la diffusion du billet incriminé auprès du public et d'un large cercle de lecteurs. Elle ne dit d'ailleurs pas autre chose lorsqu'elle déclare se borner à "mettre à disposition des internautes une structure de communication" et n'être "qu'un intermédiaire qui participe [...] à la propagation" de l'information et la rend "accessible sans en être l'auteur". En définitive, si elle n'est pas l'auteur de l'atteinte, elle a contribué à son développement et, partant, y a participé conformément à l'art. 28 al. 1 CC. »[23]

Ainsi, l'hébergeur direct d'une *fake news*, disposant de la légitimation passive, pourra être poursuivi en cessation de l'atteinte[24]. Cela étant, il garde toujours la possibilité de retirer, sur demande, le billet litigieux avant que la victime ne saisisse la voie judiciaire[25].

On peut cependant se demander si un hébergeur indirect ou médiat, tel que par exemple un média social sur lequel ne circule qu'un lien menant vers une *fake news* ou un moteur de recherche qui ne ferait qu'aiguiller ses utilisateurs vers elle, disposerait également de la légitimation passive. Cette question reste incertaine : d'une part, dans un arrêt de 2015, le Tribunal fédéral a considéré que la publication d'un lien menant généralement sur la page de garde d'un site sur lequel se trouvait une atteinte n'était pas un acte analogue à une participation au sens de l'art. 28 al. 1 CC, ce qui fait ressortir que le seul fait de publier un lien n'est pas suffisant[26]. D'autre part, il n'est pas certain que cette jurisprudence s'applique au cas du lien menant directement l'internaute vers la ressource mis en cause – tel cas n'ayant pas encore été traité par notre haute Cour. Une zone d'incertitude subsiste donc au sujet de la légitimation passive d'hébergeurs accueillant des liens permettant au public de retrouver directement le contenu litigieux. Cette lacune est particulièrement malheureuse dans le contexte des *fake news*, dont le mode de reproduction – fait de partages de liens et de retweets successifs – repose principalement sur ce type de liens.

---

22 Arrêt 5A_792/2011 du 14 janvier 2013, confirmé par ATF 141 III 413.

23 Arrêt 5A_792/2011., considérant 6.3.

24 Pour les autres conditions : voir FRANCEY, p. 170ss § 391ss.

25 FANTI, p. 78.

26 Arrêt 5A_658/2014 du 6 mai 2015, considérant 4.2.

Un autre écueil relatif aux actions défensives concerne le moyen employé pour faire cesser l'atteinte, qui doit respecter le principe de la proportionnalité. En matière de responsabilité des hébergeurs, il existe plusieurs moyens d'obtenir la cessation de l'atteinte, chacun ayant un caractère plus ou moins incisif[27]. De façon résumée, ces moyens sont :

- **Le retrait du contenu (*take down*),** soit l'obligation de retirer le contenu illicite directement visé par l'action cessatoire ;
- **L'obligation de prévention de la remise en ligne (*stay down*)**, qui impose à l'hébergeur l'obligation de surveiller le contenu qui lui est soumis par ses utilisateurs pour prévenir la remise en ligne du contenu sujet de l'action cessatoire[28] ;
- **L'obligation de notification du contenu**, qui impose de plus à l'hébergeur de notifier à tout autre hébergeur analogue le retrait du contenu afin de leur imposer une obligation concurrente de *stay down*[29].

On peut considérer que l'obligation de *take down* serait, à elle seule, insuffisante pour faire cesser l'atteinte véhiculée par une *fake news* à cause de la nature virale de sa propagation. En effet, une fois ce *take down* effectué, la fausse nouvelle sera simplement remise en ligne par un autre utilisateur ou auprès d'un autre hébergeur. En revanche, les obligations plus incisives de *stay down* et de notification de contenu peuvent être difficiles à mettre en place pour les hébergeurs – et notamment ceux de petite ou moyenne envergure. En absence de jurisprudence ou d'autres lignes directrices, il apparaît donc que le juge chargé de traiter une action en cessation devra se livrer à un délicat jeu d'équilibrisme entre les intérêts de la partie lésée, ceux de l'hébergeur et le droit à l'information du public.

B. Actions réparatrices

On peut également considérer les actions réparatrices de l'art. 28a al. 3 CC qui englobent tant l'action en dommages et intérêts (art. 41 CO) qu'en tort moral

---

27 Pour une discussion approfondie des moyens de blocage pris sous l'angle de la proportionnalité, voir BENHAMOU, pp. 523-525.

28 Une telle obligation de *stay down* est par exemple prévue sous certaines conditions par le projet de réforme de la LDA à son art. 39d, selon lequel « Le fournisseur d'un service d'hébergement Internet qui sauvegarde les informations saisies par les usagers est tenu d'intervenir afin de prévenir qu'une œuvre ou un autre objet protégé soit à nouveau rendu accessible de manière illicite à des tiers par le biais de son service ».

29 C'est par exemple le mécanisme institué en matière de droit à l'oubli par le Règlement général sur la protection des données, voir 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *OJ L 119*, pp. 1-88, Art. 17 (2).

(art. 47 et 49 CO), et en remise de gain (art. 423 CO)[30]. S'agissant de *fake news* – et gardant en tête ici que l'obtention d'une réparation pécuniaire est souvent subsidiaire en importance par rapport au retrait de l'information en question – on s'intéressera tout particulièrement à la question de la faute et à celle de la quantification du dommage, qui peuvent apparaître comme problématiques.

Dans son arrêt *Tribune de Genève* déjà abordé ci-dessus[31], le Tribunal fédéral a mentionné que le « *devoir d'attention et de contrôle requis de chacun* » relevait de la question de la définition de la faute imputable à un hébergeur, sans toutefois expliquer plus en avant comment cette notion devait s'interpréter en matière de responsabilité des hébergeurs[32]. En l'absence de telles lignes directrices, la doctrine considère que l'hébergeur « *commet une faute lorsqu'il diffuse un contenu illicite d'un tiers alors qu'il le connaissait ou aurait dû connaitre son existence* »[33]. Il appartiendrait donc à la victime de signaler à l'hébergeur la présence du contenu illicite sur ses serveurs pour que celui-ci soit contraint, en vertu de son devoir de diligence, de retirer ledit contenu. En d'autres termes, le droit suisse instituerait par cette exigence une procédure dite de *notice and take down*, que l'on connaît déjà en droit de l'Union européenne conformément à l'art. 14 de la Directive sur le commerce électronique[34], ou en droit américain sous le *Digital Millenium Copyright Act* de 1998 en ce qui concerne les atteintes à la propriété intellectuelle[35]. *A contrario*, les hébergeurs ne sont pas soumis à un devoir général de surveillance de leurs contenus, sauf en cas d'indices concrets de l'illicéité de l'un des contenus qu'ils hébergent[36]. On peut également concevoir que les hébergeurs ont un devoir sous-jacent de structurer leurs services de façon à minimiser les risques d'atteintes, par exemple en filtrant certains mots-clés ou en ne permettant pas le chargement anonyme de contenu sur leurs serveurs.

Les *fake news* prenant leur essor par le fait de l'accumulation de contenus placés par des auteurs différents sur des plates-formes éparses, il n'en reste pas moins que la quantification du dommage, subi par la victime du fait du manque de diligence d'un hébergeur-défendeur isolé, sera en pratique difficile à conduire, ce qui rend les actions réparatrices inintéressantes, voire illusoires, pour celle-ci.

---

30 Pour un aperçu général, voir FRANCEY, p. 181ss § 313ss.

31 Voir ci-dessus, note de bas de page 22 et texte y relatif.

32 Arrêt 5A_792/2011, considérant 6.3.

33 CIOLA-DUTOIT/COTTIER, p. 121 ; FRANCEY, p. 189 § 345.

34 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, OJ L 178, 17.7.2000, p. 1–16.

35 *Digital Millenium Copyright Act of 1998,* accessible sur https://www.copyright.gov/legislation/dmca.pdf (25.07.19) ; pour un survol de cet instrument et de la procédure de *notice and take-down* qu'il institue, voir CIOLA-DUTOIT/COTTIER, p. 118-119.

36 FRANCEY, § 448ss.

IV. Importance pratique de l'autorégulation

L'impact des moyens prévus par le droit suisse se doit d'être relativisé par l'importance pratique des mécanismes d'autorégulation institués par les hébergeurs. En effet, nombre d'hébergeurs proposent déjà des procédures de *notice and take down* permettant aux justiciables de leur signaler du contenu illicite et d'en demander le retrait. Après examen de la demande, l'hébergeur retire le contenu en question, ou décide de le maintenir. De cette façon, ces hébergeurs peuvent de façon préventive remplir leur devoir de diligence – le contentieux judiciaire n'intervenant qu'en cas de maintien du contenu. En Suisse, ce mode de résolution des conflits est notamment promulgué par le biais du Code de conduite d'hébergement de la Swico - l'association suisse des entreprises du numérique- qui en ses articles 6 et 7, prévoit une procédure de *notice and take down* à l'attention de ses membres[37].

Plus en avant, certains hébergeurs ont institué des mécanismes visant à traiter spécifiquement du problème des *fake news*, comme par exemple l'initiative Factcheck de Facebook, qui, en partenariat avec un organisme de vérification factuelle des informations institué par l'Université de Pennsylvanie, affiche les liens soupçonnés de comporter des *fake news* avec une mention indiquant leur fiabilité douteuse[38].

L'importance de l'autorégulation pour régler le problème des *fake news* n'est pas à sous-estimer. A cet égard, le Conseil fédéral, dans son rapport sur les médias sociaux de 2017, a expressément considéré que ces mesures étaient pour le moment suffisantes, expliquant alors sa décision de renoncer à légiférer sur la question[39].

Un autre élément expliquant l'importance des mécanismes d'autorégulation dans le domaine des *fake news* est lié au fait que ledit phénomène dépasse la plupart du temps les frontières d'un seul Etat, ne serait-ce que parce que les hébergeurs de grande envergure, tels que Facebook ou Twitter, sont situés aux Etats-Unis. Or, la détermination de la compétence des tribunaux et du droit applicable aux atteintes à la personnalité reste une question délicate qui n'est pas encore clairement tranchée par le droit international privé[40]. Ainsi, l'accès direct à un mécanisme de *notice and take*

---

37 Accessible sur https://www.swico.ch/fr/connaissances/normes-et-standards/code-de-conduite-hebergement/#code-of-conduct (22.07.19) ; voir également FANTI, p. 80.

38 Voir l'annonce du 15 décembre 2016 sur le site officiel de FactCheck : https://www.annenbergpublicpolicycenter.org/factcheck-org-to-work-with-facebook-on-exposing-viral-fake-news/ (25.07.19).

39 *Un cadre juridique pour les medias sociaux : Nouvel état des lieux*, Rapport du Conseil fédéral du 10 mai 2017, p. 12.

40 REYMOND, p. 5-8.

down reste en pratique plus sûr, rapide, efficace, et donc attrayant pour la victime d'une *fake news* que l'engagement d'une action judiciaire.

V. Conclusion

Il n'est pas certain que la problématique des *fake news* soulève, en tant que telle, des questions novatrices en matière de responsabilité civile. D'une part, les fausses nouvelles sont, depuis l'âge de la presse papier, traitées adéquatement par les règles traditionnelles de la responsabilité délictuelle. D'autre part, le droit de la responsabilité des hébergeurs de l'internet n'est pas – ou plutôt plus – une *terra incognita* propre à remettre en question l'application desdites règles traditionnelles au cyberespace.

Au final, la problématique soulevée par les *fake news* nous semble principalement liée à des interrogations d'ordre procédural. Face à la prolifération virale de fausses nouvelles, les moyens de droit se doivent d'être tant rapides qu'efficaces. En ce sens, l'exemple de la loi française contre les manipulations de l'information[41] – proposant une voie spéciale pour le traitement judiciaire d'une demande en retrait du contenu - mérite d'être examiné.

[41] Voir ci-dessus, note 2.

VI. Bibliographie

BENHAMOU Yaniv, « Blocages de sites web en droit suisse », in *Expert Focus 8/17*, p. 524-530.

Cadre juridique pour les médias sociaux, Rapport complémentaire du Conseil fédéral sur le postulat Amherd 11.3912 du 10 mai 2017.

DARBELLAY Aline/REYMOND Michel, « Le régime de responsabilité civile en matière d'émissions publiques de jetons digitaux (ICO) », in *RSDA* 2018, p. 48-66.

De WERRA Jacques, « Alternative Dispute Resolution in Cyberspace : The Need to Adopt Global ADR Mechanisms for Addressing the Challenges of Massive Online Micro-Justice », in *Swiss Review of International and European Law 2016*, p. 289-306.

Disinformation and 'fake news' : Final Report, House of Commons, Digital, Culture, Media and Sport Committee, 18 février 2019, HC 1791.

DOUBEK James, « Conspiracy Theorist Alex Jones Apologizes For Promoting 'Pizzagate'", *NPR*, 26 Mars 2017, https://www.npr.org/sections/thetwo-way/2017/03/26/521545788/conspiracy-theorist-alex-jones-apologizes-for-promoting-pizzagate?t=1542093892807&t=1542143286930 (12.11.18).

FANTI Sebastien, « Commentaire d'arrêt 5A_792/2011 », in *Medialex* 2013, p. 78-80.

FRANCEY Julien, *La responsabilité délictuelle des fournisseurs d'hébergement et d'accès Internet*, Zurich (Schulthess, Travaux de la Faculté de droit de l'Université de Fribourg) 2017.

Geneva Internet Dispute Resolution Policies 1.0, https://geneva-internet-disputes.ch (22.07.19).

GOLDMAN Anna, « The Comet Ping Pong Gunman Answers Our Reporter's Questions », *The Washington Post,* 7 décembre 2016, https://www.nytimes.com/2016/12/07/us/edgar-welch-comet-pizza-fake-news.html?smid=fb-nytimes&smtyp=cur (12.11.2018).

GUILLET Kevin, « La responsabilité de l'hébergeur en réparation du dommage pour des violations du droit de la personnalité », in *Blog Droit 2.0 et nouvelles technologies*, https://kevinguillet.ch/2017/02/13/fake-news-la-responsabilite-de-lhebergeur-en-reparation-du-dommage-pour-des-violations-du-droit-de-la-personnalite/ (12.11.2018).

LAURENT Samuel, "« Infox », « intox », « canular » ou « mensonge », pourquoi il ne faudrait pas parler de « fake news »", Le Monde, 4 octobre 2018, https://www.lemonde.fr/les-decodeurs/article/2018/10/04/infox-intox-

canular-ou-mensonge-pourquoi-il-ne-faudrait-pas-parler-de-fake-news_5364674_4355770.html (25.07.19).

La responsabilité civile des fournisseurs de services Internet, Rapport du Conseil fédéral du 11 décembre 2015, https://www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-f.pdf (25.07.19).

Manila Principles on Intermediary Liability, https://www.manilaprinciples.org (25.07.19).

« Recommandation sur les équivalents français à donner à l'expression fake news », Commission d'enrichissement de la langue française, *Journal Officiel de la République Française*, 4 octobre 2018, Texte 113 sur 142, NOR CTNR1826048K.

REYMOND Michel, *La compétence internationale en cas d'atteinte à la personnalité par Internet*, Thèse, Genève, etc. (Schulthess) 2015.

Un cadre juridique pour les médias sociaux : Nouvel état des lieux, Rapport complémentaire du Conseil fédéral sur le postulat Amherd 11.3912 "Cadre juridique pour les médias sociaux" du 10 mai 2017.

WENDLING Mike, « The saga of 'Pizzagate' : The fake story that shows how conspiracy theories spread », *BBC Trending*, 2 décembre 2016, https://www.bbc.com/news/blogs-trending-38156985 (25.07.19).

WERRO Franz/SONNEY Virginie, « Les services Internet et la responsabilité civile », in *Medialex* 2008, p. 119-132.

WONG Julia Carrie, « What is QAnon? Explaining the bizarre rightwing conspiracy theory », The Guardian, 31 juillet 2018, https://www.theguardian.com/technology/2018/jul/30/qanon-4chan-rightwing-conspiracy-theory-explained-trump (25.07.19).

World Internet Liability Map, The Stanford Center for Internet & Society, https://wilmap.law.stanford.edu (25.07.19).

Liability for damages caused by AI in medicine : Progress Needed

Valérie Junod*

Intelligence is the ability to avoid doing work,
yet getting the work done.

Linus Torvalds

Table des matières

I. Introduction 120
II. Liability related to the use of AI 122
A. Liability of health care professionals 122
B. Liability of the AI provider-producer-developer 125
1) Liability under the Product Liability Act (PLA) 126
2) Liability under Article 55 CO 129
C. Liability of researchers 131
III. Recommendations 133
A. Recommendations to improve the current liability regime . 134
B. Other recommendations 136
C. Further considerations 138
1) Some cost issues 138
2) Some antitrust issues 139
3) Some ethical issues 140
IV. Conclusion 142
V. Reference list 144

* Professor at the University of Geneva and and the University of Lausanne.

I. Introduction

Medicine is the field where Artificial Intelligence (AI[1]) has been claimed to have the greatest immediate potential[2]. Some of these claims are almost certainly "hype"[3], while others appear more tangible[4]. Several scientific studies have been published which demonstrate that AI can do as well as or better than human experts for some specific medical tasks[5]. For example, AI can diagnose certain cancers better than expert physicians[6] ; some AI tools can read chest X-rays better than most doctors ; AI has even been shown to predict patients' suicides with a remarkable accuracy[7] ! The uses of AI can extend well beyond diagnosis : AI can suggest the best cancer treatment from an array of possible medications ; it can help synthesize the relevant medical literature for a given case[8]. The areas of medicine where AI can be exploited are constantly growing ; some suggest that patients' medical history could be captured more reliably by an AI robot ; medical research may also be accelerated thanks to AI[9]. However, scientific evidence of efficacy remains limited to specific areas (i.e., narrow AI) ; hope for a broad general AI has yet to materialize[10]. Hence, AI will not replace doctors altogether– at least not in the near future.

---

1 "There is no universally agreed definition of AI ; the term broadly refers to computing technologies that resemble processes associated with human intelligence, such as reasoning, learning and adaptation, sensory understanding and interaction". Nuffield Council on Bioethics (2018), p. 1. See also GUIHOT ET AL. (2017), pp. 393-396 ; Académie des technologies (2018), pp. 15-20.

2 TERRA NOVA, p. 5 ; BAMBAUER (2017), p. 383 ; GREENBERG (2017) ("AI, along with personalized big data, is projected to be the next disruptive technology that will transform medicine").

3 On the history of "hype" in the field of AI, see European Parliament Research Service (May 2018), p. 10 ; also SCHWARTZ ET AL. (1987), pp. 685-686.

4 On the development of IBM's Watson AI, see ALLAIN (2013) ; CHUNG (2017), p. 37 ; CHUNG/ZINK (2017) ; DELOITTE (2015). Explaining recent setbacks : DAVID H. FREEDMAN, *A Reality Check for IBM's AI Ambitions*, Business Report, Technology Review, 27 June 2017.

5 See LOH (2018) ; WISE (2018) ; CHOI ET AL. (2016) ; DIPROSE/BUIST (2016) ; GOLDEN (2017), p. 2184.

6 A correct diagnosis is of course essential, as this is the first necessary step for the subsequent correct treatment. Diagnostic errors (either a missed health condition or a wrongly identified health condition) can have dramatic consequences, leading to early deaths or decreased quality of life. According to GREENBERG (2017), "misdiagnoses are the leading cause of malpractice claims in both Canada and the United States". More generally, "the true number of premature deaths associated with preventable harm to patients [at hospitals in the United States] was estimated at more than 400,000 per year. Serious harm seems to be 10- to 20-fold more common than lethal harm." JAMES J. T., *A new, evidence-based estimate of patient harms associated with hospital care*, 9(3) Journal of Patient Safety. pp. 122-128, September 2013.

7 See GREENBERG (2017).

8 "Rien que dans la base de données PubMed, qui regroupe les articles de médecine et de biologie, environ 3'000 nouveaux articles sont indexés chaque jour. Un expert, s'il réussissait à lire trois articles par jour, ne lirait qu'un millième de ce qui est publié. Plus aucun humain ne peut donc lire, comprendre, inférer et résumer tout cela sans le secours d'un outil puissant." TERRA NOVA (2017), p. 7.

9 See GIL ET AL. (2014), p. 171.

10 On singularity as the ultimate step, see GUIHOT ET AL. (2017), pp. 397-399.

This is not to imply that AI will not become increasingly common in hospitals, clinics and perhaps even private medical practices. The economic interest in proposing AI products or AI services (hereafter : AI tools[11]) is certainly present. Major companies are investing in this area and field testing their innovative solutions. The high cost of healthcare[12] and the high revenues generated by health care services certainly provide the necessary incentives.

Whereas Switzerland welcomes several established companies and many startups specializing in AI[13], it has yet to introduce AI routinely into its medical establishments. For this reason, the present article on the liability resulting from the use of AI anticipates future and somewhat uncertain events[14]. Caution is "de rigueur"[15]. We will limit our analysis to what may occur now or in the next few years[16]. Fear of an all-powerful AI ruling over humans is best left to science fiction novels[17].

The article is divided in three chapters. The first answers the question of the extent to which a health care professional, a health care institution or an AI producer may be found liable when a patient is injured following the use of an AI tool. The second chapter puts forward recommendations to improve the current liability system and analyzes the broader implications of AI use. The conclusion highlights the need for harmonization.

Beyond the scope of the paper are the damages that professionals themselves (e.g., hospitals, physicians) may incur because of AI tools ; also beyond its scope is deliberate hostile or criminal use of AI, regardless of whether it harms patients or institutions (e.g., AI being hacked to access patient data illegally)[18]. Finally, the paper only focuses on AI use in the context of patients' medical care, although one can imagine that AI could also be deployed more broadly in health care settings, for example in preparing hospital invoices or supervising medical staff.

---

11 Of course, choosing the term "tool" is not entirely innocent, as it implies someone else, i.e., a person, using the tool.

12 In Switzerland, health care expenses reached CHF 80.7 billion in 2016, a 3.8% increase over 2015. Overall, these expenses represent 12.2% of GDP. See Federal Office for Statistics, Press release of 19 April 2018.

13 ANOUCH SEYDTAGHIA, La Suisse, leader en intelligence artificielle, Le Temps du 31 janvier 2018 ; from the same author, En Suisse, l'intelligence artificielle est devenue omniprésente, Le Temps du 15 novembre 2017.

14 As would be expected, no lawsuit because of AI-caused damages has yet taken place in Switzerland – nor could I find reports of such judgments abroad.

15 See, e.g., TOM MORISSE (2017).

16 I leave aside the proposal advanced by some authors (e.g., CHUNG (2017) ; CHUNG/ZINK (2017)) that AI will become and behave so "human-like" that it should be granted "legal personhood". I am not convinced by the usefulness of such a proposal – at least for the mid-term future. For a more thorough discussion of the issue, see PETRELLUZZI/MILIOTIS (2017) ; see already in 1981, LEHMAN-WILZIG, pp. 452-453.

17 See EUROPEAN PARLIAMENT RESEARCH SERVICE (May 2018).

18 On these issues, see, e.g., TSCHIDER (2018).

II. Liability related to the use of AI

A. Liability of health care professionals

Imagine the following hypotheses : a software using AI reaches the "conclusion" that patient X suffers from a certain cancer, although this actually not the case ; an AI tool concludes that patient Y does not suffer from cancer, when in fact she does ; an AI program recommends a certain course of drug treatment for patient Z, whereas another treatment would have cured the disease. In all three hypotheses, the patient incurs harm : added medical costs, loss of wages, possibly permanent body lesions or even death. Had the AI tool not been used, the outcome for the patient would have been different and, in all likelihood, better.

Should the physician handling the treatment of the patient in a private medical practice be held liable ? Similarly, should the private clinic taking care of the patient face liability ?

Under current Swiss law, a service provider – whether a doctor or a medical institution[19] – is liable if the injured party can prove that the health care contract binding the two was breached[20] ; the claimant must also prove having incurred a damage, whether financial or moral (pain and suffering)[21] ; this damage must have been caused by the above-mentioned breach of contract. Finally, depending on the fact pattern, a fault is presumed (the defendant can escape liability if she proves not to have been at fault[22]) or not required (in case of vicarious liability of a private institution for the acts of its employees[23] or in case of an action against a State actor, e.g., most cantonal public hospitals)[24].

The first difficulty for the injured patient is to prove that the contract was indeed breached. When health care is delivered, the contract is typically one of mandate. A contract of mandate obliges the service provider to show the greatest diligence when delivering her services[25]. Hence, the contract is breached if a reasonable health care provider, placed in the same

---

19 I will leave aside the liability of public hospitals, although ultimately it is not very different from the liability of private clinics.

20 Articles 398, 97 or 101 of the Swiss Code of obligations (CO).

21 Articles 42, 47 and 49 CO ; BAUME (2015), pp. 60-65, noting that they are no punitive damages under Swiss law.

22 Article 97 CO.

23 Article 101 al. 1 CO – the exculpatory evidence to be provided by the defendant is nearly impossible to bring.

24 On the legal regime of liability for public hospitals, see, e.g., Baume (2015), pp. 30-48.

25 In the context of medical liability, see BAUME (2015), pp. 58-59.

circumstances, would have ordinarily exhibited a greater degree of diligence[26]. In our hypothesis, it boils down to whether a diligent health care provider would have used the AI in the same manner. The questions to be answered are for example whether a reasonable provider would have used the AI tool at all, whether it would have cross-checked the AI's recommendations with other sources of information (e.g., a human medical expert), whether it would also have relied "blindly" on the AI recommendations, and whether it would have followed the implementation of the AI recommendations more closely or more regularly.

As this list of questions reveals, this requires a highly fact-intensive inquiry. For certain medical services, for example certain diagnostics, there may be scientific evidence that the AI performs so much better than human doctors that the diligent course of action is to rely on the AI recommendations, without confronting them with the perspective of human doctors[27]. This would be the case if, for example, a relevant peer-reviewed study had established that the AI diagnostic tool reaches 99% sensitivity (true positive rate) and 99% specificity (true negative rate), while human experts in the field exhibit much lower scores (let's say 40%). In that case, even if the unfortunate patient falls in the 1% error rate due to AI, the actions of the health care provider are still diligent and no breach of contract can be shown.

The interesting questions may then turn to the cutoff point where "blind" reliance on AI becomes admissible. If AI has only 70% sensitivity and 70% sensibility, whereas human experts are at 60%, should the two combine their efforts ? These questions are best answered by medical experts, usually in the course of a judicial expertise and/or by medical societies issuing recommendations to their members (e.g., "when doing a chest X-ray for breast cancer, we advise checking the recommendations of the AI against the reasoned opinions of two medical experts").

A problem that we are likely to encounter is how to quantify the performance of the AI tool. This problem stems from the fact that AI is designed to learn constantly by incorporating new data. Of course, it may be tested in a clinical setting when it is launched, but afterwards it keeps on "tweaking" its abilities. Thus, the AI may achieve 90% accuracy as compared to experts at time t1, but no one knows how it scores at time t2 when the patient was injured. It is hoped that its performance will keep on improving,

---

26 See WERRO (2012), p. 2397 et ss.

27 See FROOMKIN ET AL., (2018). An additional issue is which kind of doctors should constitute the relevant baseline. Should it be primary care doctors ? Doctors specialized in this particular field ? Experts in the field ? If, in a rural area, the primary doctor is also offering basic dermatologist services to the population, should her diligence when using an AI tool be compared to that of other rural doctors not using AI ? Or to public hospital experts even if these experts are not readily available to her patients ?

but there will be little or no scientific evidence for time t2[28]. Even worse, it will be very difficult and perhaps even impossible to acquire - after the facts - information about its t2 performance[29]. Similarly, it will be very difficult or impossible to know how the AI reached its recommendation in the case of the individual (injured) patient (the "black box" effect[30]). Finally, conclusion reached for one AI tool (i.e., this one is defective) will not be transposable to a second AI tool, because the two, even when designed together, will have – over time - learned and evolved differently[31]. As a result, the legal decision regarding a possible lack of diligence will have to be taken based on possibly outdated and certainly incomplete information. This is not entirely unusual, as this also occurs in other medical malpractice cases, but it is an uncomfortable situation. All the more so since patients bear the burden of proof and failure to prove a breach of contract will lead to denial of indemnification.

Assuming that this first obstacle is overcome, the patient still has to prove causality[32]. This requirement is known to be difficult to satisfy in medical cases[33]. It is hard to determine what would have happened to the patient, had a different medical course of action been decided upon. Would her life have been saved if her cancer had been diagnosed sooner ? Would she have lived longer thanks to a more carefully chosen treatment ? How much longer ? These questions are even more difficult to answer if the patient is already very

---

28 On the additional risk of data decay, see CHEN / ASH (2017), p. 2507.

29 "[I]n the field of robotics, it could be difficult to distinguish between a defect which was present at the moment in which the robot was put into circulation from a defect that appeared after that moment, given the characteristics of self-learning systems." ERNST & YOUNG (2018), p. 85.

30 Black box refers to the fact that the AI tool is designed in such a manner that it cannot explain which factors it used to reach its conclusions, nor can its human users. See WISE (2018). This concept is sometimes opposed to (the need for) "explainability" or "transparency". See U.K. SCIENCE AND TECHNOLOGY COMMITTEE (2016), p. 17. As the EUROPEAN COMMISSION (April 2018) explains ; "in order to increase transparency and minimize the risk of bias or error, AI systems should be developed in a manner which allows humans to understand (the basis of) their actions". See also EUROPEAN PARLIAMENT (2017), point 12 ("it should always be possible to supply the rationale behind any decision taken with the aid of AI that can have a substantive impact on one or more persons' lives") ; FROOMKIN ET AL., (2018), p. 60 ;TERRA NOVA (2017), p. 22 ("l'affirmation d'un principe général de transparence des algorithmes risque d'être vaine ; elle serait d'alleurs susceptible de nuire au respect du secret industriel et pourrait potentiellement freiner l'innovation."). See also PACKING/LEV-ARETZ.

31 The judgment of the EU Court of Justice in C-503/13 of 5 March 2015.

32 See BAUME (2015), pp. 65-66. In addition, because each AI tool is likely to be viewed as an individual and different product, since each will have "learned" differently, it will not be possible to infer that the present AI suffers from a defect, because another AI has already been proved to be defective. This adds another practical difficulty (compare with European Court Judgment of 5 March 2015, C-503/13, in case of classic products).

33 When the contract breach resides in an omission – as opposed to an action – then causality must be determined hypothetically. According to the Federal Tribunal's case law, a strict level of proof (evidence) is not required. A preponderance of evidence suffices. The plaintiff must still demonstrate that if the proper medical action had been undertaken in her case, she would have been more likely than not to have avoided the damage. See, e.g., Judgment of July 4, 2006 in case 4C.125/2006. See also on the burden of proof, VIGNERON (2018), pp. 45-46.

sick and when the disease is known to have a high fatality rate[34]. The problem is compounded by the fact that, once AI becomes broadly used, there will be few other benchmarks to make a comparison[35]. If most medical practices use the same AI or even if they use different AI tools, how is the judge to decide what would have happened if no AI had been used. Moreover, the fact that AI tools will be put on the market based of (some) clinical evidence of their efficacy will make it hard to say that an alternative course would have led to a better outcome. If the AI has been shown to be, say, 10% better than experts, how could the judge rule that *not* using the AI in the specific situation of the injured patient would have avoided part or all of the harm ? The availability of pre-launch clinical evidence for safety and efficacy of the tool is likely to tip the balance (regarding the causal pathway) in favor of AI use[36].

Finally, courts will find it increasingly difficult to understand the technical evidence presented to them[37]. Expertise reports that they will have to assess will need to be prepared by interdisciplinary teams made of software and hardware engineers, doctors, biostatisticians.

B. Liability of the AI provider-producer-developer

While the exact business models of AI suppliers are yet to be precisely defined, it can safely be assumed that AI will be developed by companies which are not primarily health care providers. The AI tool will most likely be licensed as a program ; it might also be incorporated in a hardware, which will be sold, leased or licensed to health care providers.

When thinking of the liability of companies providing medical goods, it is obviously the Federal Product Liability Act (PLA ; SR 221.112.944) that comes to mind. Although this Act has not been frequently applied by Swiss courts[38],

---

34 For cancers for which patients' life expectancy after diagnosis is low, it is difficult to prove that an earlier diagnosis would have led to an overall cost saving. It is only for diseases which respond well to early treatment that such proof is available, at least based on statistical data. Moreover, since the Federal Tribunal has rejected the loss of chance theory ("théorie de la perte d'une chance"), the patient is faced with an all-or-nothing dilemma : she succeeds in proving causality and obtains indemnification for the entire damage – or she fails and obtains nothing. See VIGNERON (2018), pp. 46-51 ; BAUME (2015), pp. 63-64.

35 FROOMKIN ET AL., (2018) ("If a set of symptoms is consistently producing an erroneous ML [machine learning] diagnostic, and physicians act on that erroneous diagnostic, where will ML get the data to suggest a different diagnosis which lead to better treatment ? If the answer is "nowhere" then we have a problem. Worse, it is not even clear that either the ML system or an outside observer necessarily would know that the results were sub-optimal.").

36 See in a slightly different context, EUROPEAN PARLIAMENTARY RESEARCH SERVICE (February 2018), p. 33.

37 "[E]ven experts may find it difficult to understand defects in new technological developments, because of the increasing number of chain events where possible causal connections are not understandable." ERNST & YOUNG (2018), p. 85.

38 In Switzerland, only five cases decided by the Federal Tribunal applied directly the PLA (4A_365/2014 of 5 January 2015 ; 4A_16/2011 of 18 March 2011 ; 4A_319/2010 of 4 October

it is meant as a pro-consumer tool[39] to allocate liability for defective products. Additional objectives include encouraging safe product design[40] and ensuring the availability of sufficient information about proper use. Together these goals operate to guarantee people's trust in the products that they buy and use. Such trust is particularly important in the field of medicine.

The first legal difficulty that we encounter is that the PLA only applies to goods, and not to services[41]. When software is incorporated into some hardware, it qualifies as a good under the PLA. However, pure software, e.g., a website where data can be entered by the user to receive the result of computer calculations, is not deemed a good[42]. This good/service distinction has already been criticized as outdated[43]. It does not make much sense to apply a completely different regime depending on whether the software is available on a USB device or purely on-line, when the key functions of the software remain the same. In the context of AI, several authors have already recommended considering all AI tools as goods under product liability regimes[44].

In the first part of this section, we will assume that AI qualifies as a "good" under the Swiss PLA. Then, we'll study the opposite hypothesis.

1) Liability under the Product Liability Act (PLA)

Under the PLA, a patient can be compensated for the economic and moral harm incurred if she proves that this harm was caused by a defective good put into circulation by a producer[45].

The producer is broadly defined[46]. The company developing and selling/licensing the AI is to be viewed as a producer. The importer into Switzerland and (to some extent) even the final supplier are also producers[47]. Depending on the circumstances, the health care institution using the AI could

2010 ; 4A_255/2010 of 29 June 2010 ; 4C.298/2006 of 19 December 2006). In the European Union, the equivalent Directive 85/374 has not been very much used either. "[M]ost product liability claims between 2000 and 2016 [a total of 798] were actually settled out of Court [46%]". EUROPEAN COMMISSION (May 2018), p. 4.

39 Worth mentioning in passing is the fact that provisions of the PLA are mandatory and cannot be contracted away (Article 8 PLA). This can be a notable advantage compared to contractual or tort liability, where exonerative clauses are admissible within the limits of Articles 100 and 101 CO.

40 See, e.g., ALLAIN (2013), p. 1067.

41 Articles 1 and 3 PLA.

42 See VOKINGER ET AL., (2017), p. 17.

43 See, e.g. ERNST & YOUNG (2018), p. 71 ; ALLAIN (2013), p. 1070.

44 See VOKINGER ET AL., (2017), p. 18.

45 Article 1 PLA, with Article 2 defining the producer, Article 3 defining the product, Article 4 defining the defect.

46 See MARCHAND (2018), pp. 24-25.

47 Id. pp. 25-26.

also qualify as a producer, particularly if it improves on the program by feeding it data (see below)[48]. However, should AI come to be developed in an open-source environment, identifying who added which lines of code might prove increasingly difficult. Thus, identifying all AI developers, or at least the most "guilty" coders among them, will be a challenge. A possible solution would be for the law to pinpoint (at least) one available "defendant" ; thus, the plaintiff and injured party would always know who, in Switzerland, could and should be sued. This is only partly the case today since the local supplier/seller can only be sued under the PLA if it failed to indicate upon request the name of the producer or the importer[49].

The main issue for the injured patient is whether she can prove the AI to be defective. Defect is defined in an objective manner as the lack of the level of security which reasonable users can expect (of such a product)[50]. One must first ascertain who the intended user is. Because the AI will generally be used by doctors, and not by patients directly[51], the relevant user is the physician (or team of physicians, depending on the situation) ; the security expectations of the patient are not relevant[52]. As is the case for medicines, the expectations of the physician will be shaped by the information she is given. In the Federal Tribunal's judgment regarding Bayer's Yasmin contraceptive pill[53], the existence of a defect was negated because the professional notice of use clearly stated the medical risk which materialized in the case of the patient[54]. Since physicians were explicitly warned of the (largely unavoidable) risk, they could not claim that the pill was defective. If this legal doctrine were to be transposed to AI, it would mean that the existence of a defect would be dismissed whenever users were clearly warned of the corresponding risk – at least so when the mentioned risks are unavoidable. For example, if the company offering the AI warns that the incidence of a false positive is 5% (the patient is told she has cancer, but has none) and the incidence of a false negative is 3% (the patient is told not she does not suffer from cancer, but does), then this should negate the defect if the patient is unlucky to fall within these percentages. A defect could still be admitted if the actual incidence of mistakes turns out to be 10% and 6%. However, in practice, clinical study

---

48 In normal situations, simple users of products are not producers. See Judgment of 21 December 2011, C- 495/10.

49 Article 2 paragraphs 2 and 3 PLA.

50 Article 4 PLA. See MARCHAND (2018), p. 27 ("le critère est celui de la sécurité à laquelle le consommateur peut légitimement s'attendre").

51 In a more distant future, one can imagine each person having her or his own AI machines at home to provide medical services. But today, this seems more like the stuff of movies (e.g., the 2013 film Elysium) than impeding reality.

52 On the "learned intermediary doctrine" in the United States, see ALLAIN (2013), p. 1069.

53 Federal Tribunal's judgment 4A_365/2014 = 4A_371/2015 of 5 January 2015.

54 See also WERRO's comment of the Federal Tribunal judgment, WERRO (2018), pp. 95-102. See also EUROPEAN COMMISSION Staff Working Document (May 2018), p. 25.

results which rectify numbers initially provided rarely become available after launch. Therefore, the physician may suspect that the AI is not quite as reliable as claimed, but she may find it impossible to prove this to the required evidentiary standard[55]. Moreover, relying on (human) expert evidence will be very difficult too ; as mentioned above, the injured party may not find an expert that can credibly attest that the AI failed to work as claimed. Indeed, the skills to qualify as such an AI expert will be multiple and highly sophisticated. Identifying and retaining these experts for the purpose of court proceedings will not be easy.

More generally, AI producers will be inclined to include broad warnings. They may (truthfully) highlight that AI tools keep on learning (based on the data they are fed) and that, while it is hoped that this learning will constantly improve performance, this cannot be guaranteed. The AI producers may call for users to exercise caution and not to rely blindly on the AI results. Such warnings are likely to increase the liability of health care providers and to lower that of AI producers. Of course, Article 8 PLA prohibits liability waivers, but inevitable genuine risks inherently resulting from use of a good should not fall within the scope of this prohibition.

We have shown that injured patients may find it difficult to prove that the AI which was used in their medical care is defective[56]. The next legal obstacle in their path toward indemnification is Article 5 paragraph 2 letter e of the PLA. Producers can escape liability (once the conditions of good, defect, damage[57], causality have been proved by the claimant) if they can establish that, at the time the AI was put into circulation, they were not aware and could not have been aware of the risk which materialized[58]. This escape route has been labeled "the development risk"[59]. Switzerland makes this broadly available to all producers, except for those offering transplants[60]. In the case of AI, a producer could convincingly explain that it tested its AI before release, that it has clinical data to prove that the AI performed better than physicians at

---

55 Generally on "consumers' difficulties in obtaining compensation in the pharmaceutical/medical sector", ERNST & YOUNG (2018), p. 28.

56 According EUROPEAN COMMISSION (2018), "based on the desk research at national level, the most frequent reason for rejecting a claim for defective product [in any field, not specifically AI or medicine] is related to the burden of proof, and specifically to : (i) prove the defect (32% of cases) ; and (ii) prove the link between the defect and the damage (21% of cases)." (p. 27).

57 As per Article 6 al. 1 PLA, only damages to things exceeding CHF 900 is covered by the Act. This limit has been criticized as unduly discouraging small claims, which – although small by themselves – would add up to high overall damages.

58 On the scope of this exception, see, e.g., MARCHAND (2018), p. 19.

59 For an analysis and a general background on this exception, see TRAN/ETIER (2018), pp. 106-128.

60 In the European Union, Member States are free to retain or to reject this exception to liability. A minority of countries has chosen to make producers liable also for development risks. Some countries (Finland, Luxembourg, France) have a regime whereby this exculpatory factor is not available when the defect is due to pharmaceuticals or to products derived from the human body. See EUROPEAN COMMISSION (May 2018), p. 4. Also PICHONNAZ/WERRO (2018), p. 21.

the time of release, and that it has no reason to suspect that the way the AI was programmed could lead to a defect in the course of its use. The situation of the AI producer is similar to that of a pharmaceutical producer. A company like Bayer can persuasively argue that it tested its contraceptive pill carefully and that, to the best of its knowledge, the clinical trials it had to conduct gathered all possibly identifiable risks and that it could not have known of a risk that was not flagged during pre-launch clinical trials. In the pharmaceutical context, the development risk clause results in pharmaceutical companies rarely being found liable for adverse side effects not revealed in the Phase I, II and III clinical trials (i.e., the studies taking place before marketing authorization).

For AI, one added difficulty, that we already alluded to, is that the product is meant to evolve[61]. An AI used for diagnostic purposes is supposed to gain more accuracy the more diagnoses it performs ; an AI tasked with identifying the proper drug treatment is expected to improve with each increment of patient data it analyzes. This means that the tool continually changes as it is used. Data stemming from the original pre-launch clinical testing may no longer be relevant one year after the AI tool has first been put into circulation. However, this learning will probably not occur under the control of the AI producer-developer, but under the control of the health care provider (e.g., a university hospital). Can the initial developer still incur liability if further learning by the AI occurred under the control of third parties ? Should this situation be compared to that of a car maker which sells a car which is later modified ("tuned") by its new owner ? Or should the situation be distinguished because the AI is inherently meant to be "fine-tuned" by its new owner, so that this further third-party learning should be expected and even anticipated by the product developer ? In practice, the answer may depend also on the concrete terms of the licensing agreement between the AI developer and the AI user (i.e., the hospital). Because the legal issue is undeniably thorny, it should be dealt with by the legislature, rather than by case-by-case interpretations.

2) *Liability under Article 55 CO*

Let us now turn to the second hypothesis : the software is not incorporated into any leased-licensed-sold hardware, but is, for example, a free-standing

[61] Developers could also argue that they should no longer be liable for defects that arise after the release of the product. Indeed, under Articles 4 and 5 para 1 letter b PLA, the defect must be present at the time of release ("mise en circulation") ; it is for the producer to establish that the defect must have arisen later. In my view, such exculpatory evidence should not be accepted in the case of a product which is designed specifically to evolve. The developer is selling a tool under the business proposition that this tool should get better and better at its tasks. In such circumstances, the developer should be held to its promises. It should be considered that the AI tool was designed so that, from the start, the origin of the later-materialized defect was present.

internet decision-aide, in other words more akin to a service. If the PLA is held not to apply, then the injured party must rely on the Code of obligations (CO ; SR 220) and its provisions on tort liability. Traditionally, before the entry into force of the PLA in 1993, Article 55 CO was the topical provision, although Article 41 CO also enters into consideration, since the patient is not bound by contract to the AI developer. Under Article 55, the patient must show an injury (economic loss or moral harm), an illicit act within the sphere of control of the defendant, and a causal link ; proof of fault is not required, but the defendant can escape liability if it can bring certain exculpatory evidence. The first step is to assess whether there is an illicit act or an illicit omission. Bodily harm is illicit because it infringes on the absolute right to personal integrity. An incorrect AI-led diagnostic or an ill-advised AI-recommended treatment may very well directly cause bodily harm, because the patient had to undergo treatment for nothing, because she did not undergo treatment that could have saved or helped her, or because a better chosen treatment would have been more effective. Once or if it can be shown that the AI was "wrong", it then becomes clear that this mistake was the causal factor in the adverse outcome. We will assume here that the mistake was not so obvious that any reasonable physician should have noticed and corrected it. Because the patient has satisfied her burden of proof under Article 55 CO, the question turns to whether the AI producer can bring forth the exculpatory evidence allowed under this provision. If the AI was properly developed and tested before release, the producer can show that its employees and auxiliaries were well chosen, well instructed and well supervised. Since the AI was clinically tested before being put into the market, the producer can also show that it implemented a proper quality control. There is no reason to doubt that there should be a faulty system organization within the company producing the AI. Once more, the situation can be compared to that of a pharmaceutical company which releases a new drug or a new device that has been tested according to current regulations and guidelines before marketing. In conclusion, except in cases when the development work on the AI was faulty (e.g., hypothetical testing guidelines not followed), the AI developer will be able to provide the needed evidence to escape liability.

A last question under this section is whether the findings reached for the AI developer should be extended to the medical facility using the AI. Indeed, AI are likely to be released within hospitals, where they will continue to be trained chiefly or partly by the hospital staff ; AI will learn from patient data that the hospital will feed them. One can suppose that after a few years of use, an AI tool will function differently from when it was first released. Because the operation of the AI will have been altered by the hospital (its staff), should the hospital qualify as a producer ? We know that a pure user of a product is not a producer under the PLA ; for example, under these rules, a hospital using a MRI machine is not considered a producer. This changes, however, once the

hospital starts modifying a piece of equipment to further its needs. When data are fed into an AI program, the internal functioning of the AI changes. This is substantively different from using a software to fill cells in a form ; in case of an AI tool, with enough new data, the program itself is changed. For example, if erroneous data are systematically fed into the AI (e.g., by a dishonest employee), then the AI will start to give wrong recommendations or incorrect diagnoses even when, later on, correct information is being entered. In our view, the hospital faces a producer liability if it has the ability to change the functioning of the AI and has indeed done so[62].

Whether the hospital-producer will actually be held liable for damages is more difficult to ascertain. Unlike the initial developer, the hospital will not have tested the AI while or after the hospital-led changes occurred to the program. On the one hand, this makes it harder for the hospital to explain that it did all it could to avoid the occurrence of defects. On the other hand, the hospital will have no reason to suspect that providing additional data to the AI could lead to defects, because AI is precisely meant to function this way, i.e., to improve based on additional data. Of course, if a corrupt hospital employee intentionally caused the AI to malfunction, the situation would be different and the question would then turn to whether the hospital properly chose, instructed and supervised its work force.

To sum up, we have shown that the action of an injured patient will face significant hurdles and is most likely to fail, even if she can show that the AI tool was in some sense "wrong". We should add that even showing that the AI was wrong may become increasingly difficult if the use of AI becomes more and more common. For example, if all AI tools recommend treatment 1 in case of cancer, and all hospitals implement this proposal, how will the patient be able to show that treatment 2 would have been better ? After a while, there may no longer be any established point of comparison. It will just be assumed that treatment 1 works well, since the alternatives are no longer being field-tested.

C. Liability of researchers

Before AI tools are released on the market, they will have to be tested. The purpose of this testing will be to ensure their safety and efficacy, the two notions being here closely intertwined[63]. For instance, the AI developer will need to show that its AI diagnostic tool can diagnose conditions better than

[62] "[T]he longer a robot's 'education' has lasted, the greater the responsibility of its 'teacher' should be". DIRECTORATE-GENERAL FOR INTERNAL POLICIES (2016), p. 17.

[63] Expressed in greater details by SHORTLIFFE/SEPULVEDA (2018), "[a] CDSS [clinical decision support systems] should have rigorous, peer-reviewed scientific evidence establishing its safety, validity, reproducibility, usability and reliability".

most doctors can, or that its treatment selection tool offers better recommendations. The data produced during medical testing will be submitted – along with proper analysis – to the authorities to decide whether the product can be put in circulation. We argue that AI tools are medical devices[64] and ought to be classified – at least at the beginning – as high-risk devices, making it necessary to obtain a State authorization before marketing[65]. As explained by Tschider, the typology of risks that need to be examined for AI devices is much broader than for standard medical devices[66]. Thus, in Switzerland, Swissmedic should be declared competent to decide whether the clinical data in the submitted file are enough to allow launch[67] and whether additional clinical trials after launch are necessary.

During the phase of clinical testing, the AI sponsor will have to set up insurance coverage to indemnify test subjects having incurred damages. According to the Therapeutic Products Act (TPA), clinical trials of uncertified medical devices can only take place if the liability of the sponsor is properly insured[68]. Typically, the sponsor enters into an insurance contract with an insurance company. The insurance policy must cover all damages caused by the clinical trial irrespective of fault. In theory, neither the insurance company nor the sponsor can invoke any exculpatory evidence to avoid liability[69]. Contrary to the Product Liability Act, ignorance of the defect cannot be claimed to escape sponsor's liability. Therefore, at least in principle, test subjects (during the clinical trials) should benefit from a broader liability coverage than patients (once the product has been authorized on the market).

---

64 See the Federal Administrative Tribunal judgment of September 17, 2018 in the case C-669/2016. In that case, the Tribunal found that a basic diagnostic app was indeed a medical device if it was designed, based on the user's individual data, to give back medical information (here when the user was most fertile or not fertile so as to either favor or avoid a pregnancy). See also VOKINGER ET AL., (2017), p. 7 ; TSCHIDER (2018), part II ; ALLAIN (2013), pp. 1071-1072 ; BAMBAUER (2017), p. 388. For the more complex situation in the United States, see Food and Drug Administration (FDA), Software as a Medical Device (SAMD) : Clinical Evaluation, Guidance for Industry and FDA Staff (December 8, 2017). See also BARAK RICHMAN, *Health Regulation for the Digital Age – Correcting the Mismatch*, 379:18 New England Journal of Medicine 2018 pp.1694-1695.

65 This is not how the classification works currently. Yet, given the number of patients who may be affected by the use of AI, we recommend implementation of higher safeguards, at least until it is established that the risks are not markedly higher. Of a more nuanced opinion, see VOKINGER ET AL. (2017).

66 "New technology, however, introduces patient safety risks connected to backend systems and infrastructure, rather than devices interacting with the physical body. These new types of risks either necessitate a new formula for panel or expertise selection or require complementary reviews from experts who understand new technology functionality." TSCHIDER (2018), p. 200.

67 The question of how long an AI tool should spend in clinical trial(s) could prove delicate. It seems that the more time the AI spends in a controlled learning environment, the better it performs. How will scientists then decide that the AI tool has reached its optimal learning point ?

68 Article 20 of the Federal Act of 30 September 2011 on research involving human beings ("HRA" ; RS 810.30).

69 See however Articles 10.1.c and 10.2 of the Ordinance on Clinical Trials in Human Research (ClinO ; SR 810.35).

This begs the question of whether it makes sense to distinguish between a product under testing and a product released for circulation in the case of AI. Indeed, one key characteristics of AI is that it keeps on learning, constantly incorporating the new data that it is provided with. Given that the AI tool is constantly evolving, how can one decide when it is leaving the testing phase ? It could be argued that the constant fine-tuning of AI tools means that they remain in a testing phase for a long time, and possibly forever.

It might therefore be necessary to introduce a rule to decide when the AI is used in the context of research – with the ensuing application of the protective regime of the TPA – and when it has reached a sufficiently solid level of development where the TPA is no longer applicable and the PLA applies instead. However, if our proposed recommendation to transform the current liability regime into a true "no-fault" system (see chapter IV below), this would become moot.

III. Recommendations

This section is divided in two parts. First, we outline recommendations meant to improve the liability regime. Next, we lay forth other more general recommendations which go somewhat beyond narrowly-defined liability issues.

Before delving into this matter, a more general issue is determining what the overall objectives of a liability system should be[70]. Many companies have claimed that AI development should be encouraged and that liability should therefore be limited, excluded or capped. They claim that actual lawsuits and even sometimes the threats of potential lawsuits will discourage research and then adoption of AI solutions. Because there is a race between scientists and between (most) countries[71] to be the first to develop and then launch new AI tools, the countries with the most beneficial legal regime and its scientists are most likely to win it[72]. A comparison is sometimes made with other innovative medical techniques, which were first introduced without absolute guarantee of safety, but would never have been tried if such guarantees had been required from the start. For example, looking back in time, no one would have risked an

---

70 On this issue with also the benefit of a historical overview, see PICHONNAZ/WERRO (2018), pp. 2-26 ; still on this issue, but under U.S. law and with regard to AI, KOWERT.

71 The Swiss government does not appear to be very interested by AI technology. Its September 2018 "Plan d'action Suisse numérique" mentions several initiatives, but AI is in no way highlighted (see its page 27 and point 7.5).

72 "The global AI developing ecosystem is already in a frenzy. […] Funding more than tripled between 2016 and 2017 alone, to reach over 11 billion euro". EUROPEAN POLITICAL STRATEGY CENTRE (2018), p. 2. See also EUROPEAN COMMISSION (April 2018) ; European Commission's press release of 25 April 2018 titled "Artificial intelligence : Commission outlines a European approach to boost investment and set ethical guidelines".

organ transplant or in vitro fertilization if any mishaps – and there were many – would have resulted in lawsuits and victorious claims. A historical comparison can also be made to cars : the first automobiles were dangerous, at least judged by today's standards ; it is only because the law allowed their producers to progressively add security features that they quickly became such successful products.

Others have claimed the reverse[73]. It is only if the patients and the physicians have full confidence in AI that AI tools will be adopted. Full confidence requires strong patient rights, which include strong rights to claim compensation. Moreover, the threat of lawsuits will push developers to create better and safer products. They are the parties best positioned to incorporate safety considerations into their design early on ; they are also best positioned to properly test their AI. Therefore, strong liability rules may create a virtuous circle, in which good AI tools are created and then exploited for the greater good, while actual lawsuits remain rare.

At this stage, there are no empirical ways to test the two viewpoints. For transparency's sake, I will admit my preference for the second perspective. Trust is essential in medicine. The potential for large-scale harm is so great that innovations ought to be carefully tested and accompanied by proper safeguards. The threat of lawsuits, at least to a certain extent, operates as such a safeguard. The history of pharmaceuticals' and medical devices' regulations shows that, without such a credible threat, massive harms can occur (e.g., elixir sulfanilamide, thalidomide, breast implants).

This preference also leads me to suggest improvements that mainly favor the interests of injured patients.

A. Recommendations to improve the current liability regime

In my view, based on the developments above, the following measures should be implemented :

a) All AI tools should fall within the scope of the PLA, regardless of whether or not they are incorporated into hardware. The distinction between products and services makes less and less sense with respect to IT tools. Since the risks and benefits are the same, whether or not the product is physically incorporated, the legal regime should be the same. This corresponds to the reasonable expectations of users. A patient does not

[73] "[C]alls for innovation without any regulation must be viewed critically". GUIHOT ET AL. (2017), p. 419. The authors look carefully at the various regulatory schemes, including self-regulation, that could come into consideration. See also CHUNG (2017), p. 38.

know whether the AI recommendations was issued on-line or stemmed from a tangible machine – and it should make no difference.

b) The development risk exception (Article 5, letter e PLA) should be removed and AI should follow the fate of transplants[74]. There are inherent risks in AI that cannot be assessed with certainty by pre-launch testing, risks which will evolve as the AI continues to learn on its own[75]. Because a development risk escape clause will almost always bar patients' lawsuits, the public interest in a fairer social regime calls for discarding this exception.

c) Solidarity rules should be carefully considered[76]. The present system of the PLA is that any producer is jointly and severally liable towards the injured patient for the entire amount of the damage[77] ; only after having paid what is owed to the patient, can this producer sue the other liable parties in the chain of production. This system could become increasingly unfair if the entity being sued has little to do with the defect that caused the harm. Ideally, a liability system should place liability on the person most capable of preventing or mitigating the harm[78]. In this way, liability claims or threats of such claims can truly act as a deterrent for dangerous commercial practices. If the system operates so that Swiss suppliers or Swiss importers are the only parties being sued by patients in Switzerland, while the AI developers in China or in the United States remain de facto sheltered, this objective of product liability regime will hardly be attained.

d) Since the development of AI is likely to involve multiple parties in multiple countries, the most efficient solution might be to introduce mandatory insurance for each AI tool[79]. This is also the thinking behind vehicle insurance : people drive a variety of cars, including car which they do not own, across geographic frontiers. Victims should be indemnified, regardless of whether the car (or the AI) was built in one country, registered in a different one, owned by someone domiciled in a third country and (badly) used in a fourth one[80]. With a system of insurance

---

74 Article 5 al.1bis PLA ("organes, tissus ou cellules d'origine animale ainsi qu'aux transplants standardisés issus de ceux-ci destinés à être transplantés"). See also the regime for genetically modified organisms, explained by KRELL ZBINDEN/LANGHORST (2018), pp. 82-109.

75 See also PICHONNAZ/WERRO (2018), p. 25.

76 On this topic with regard to AI, but under U.S. law, see KOWERT, pp.202-203.

77 Article 7 PLA.

78 See EUROPEAN PARLIAMENT, point 56.

79 See EUROPEAN PARLIAMENT, point 57. In its Resolution, the European Parliament recommends adding a public fund "to ensure that reparation can be made for damage in cases where no insurance cover exists". In my view, it is still too early to decide whether there would really be gaps in insurance coverage that make a fund necessary. Others, on the contrary, have suggested introducing liability caps, so that the overall damages that could be claimed would be known to be limited to a certain ceiling. ALLAIN (2013), p. 1076.

80 Insurance may also somewhat simplify issues related to jurisdiction and applicable law.

coverage, victims would know that they would be properly indemnified in a relatively quick manner, without having to master the complete history of the AI product (e.g., who developed it where, who fed it data where, who imported it into Switzerland, who used it professionally). With the insurance company acting as the pivot point, it would then (i.e., after the patient received compensation) be easier to allocate responsibility among the involved parties, based either on their share of the guilt/fault or on other criteria (e.g., contract clauses).

We realize that these pro-consumer recommendations are likely to run into political obstacles. As Pichonnaz/Werro wrote : "Le futur de la responsabilité pour risque et sa généralisation sont des questions éminemment politiques"[81].

B. Other recommendations

This subsection sets forth additional recommendations more indirectly connected with liability. We comment only briefly on them, since a detailed justification would go beyond the scope of this paper.

a) The legislature should institute clear procedures for AI medical tools to be preauthorized, either by a medicine agency (e.g., Swissmedic in Switzerland) or by a specialized *ad hoc* agency. The authorization procedure should be strict, whether we apply the rules of high-risk medical devices or those for allopathic drugs. Self-certification or certification by notified bodies (as currently used for most medical devices) should not be held sufficient. The authorization process should be sufficiently transparent for professional users to know which level of security and efficacy to expect from the released AI tools.

b) Producers of AI should be obliged to keep on supervising and studying their tools even after release. Because an AI tool learns continuously, it should be tested and retested periodically. Indeed, reliability results at time t1 may no longer hold true at time t2. The law should specify how this ongoing testing is to be arranged, and whose responsibilities it should be (e.g, the initial producer only, the hospital now using the AI, or both of them together).

c) Patients should be told whether AI is or was used in the course of their medical care[82]. Because the accuracy of the data fed to the AI is so crucial, patients should be made aware of the importance of the information that they themselves provide. As the fictional Dr. House says “all patients lie” ;

[81] PICHONNAZ/WERRO (2018), p. 25.

[82] See also VOKINGER ET AL., (2017), pp. 15-16.

whereas good doctors may be able to spot a lie, AI is unlikely to master this social skill – at least in the near future.

d) Patients should also be given information about AI involvement in their medical care, as it will help them understand the "thought process" of their doctors. For example, if a patient is told that the doctor relied only on the diagnostic provided by the AI tool, she can challenge this conclusion and seek a different medical opinion elsewhere. Without this knowledge, the consent she would give to the suggested treatment course would not be truly informed[83].

e) Based on the autonomy principle, patients should have the final say as to whether to allow AI to access their medical files[84]. Whether consent is by opt-in or by opt-out remains open to discussion[85]. However, it should be held that patients' data in medical files can never be viewed as fully anonymized and that AI's access to such files falls under the legal notion of data processing[86]. Moreover, the data are sensitive data, since they contain health information. Therefore, in conformity with Data Protection Law, the individual is entitled to decide whether to confer or exclude access. The higher good hoped from AI data analysis and AI services should not bypass this requirement dictated by the fundamental interest in autonomy[87].

f) AI tools should not be allowed to pool or merge the data from different databases without patients' approval, and for sensitive fields, without a prior authorization by a competent authority. One can imagine a future where the AI uses data beyond medical dossiers, and hunts for data on-line regarding the patient (e.g, Facebook's postings)[88]. AI tools might also be programmed to allow the sharing of data among each other[89]. Being able to use data from government databases (e.g., the tax file) might also be tempting, since socioeconomic data can be very informative, including for

---

83 See NUFFIELD COUNCIL ON BIOETHICS (2018), p. 5.

84 Because patients' files at least in Switzerland are not (yet) standardized, it will be difficult for AI to just access and use these data directly. However, with the introduction of the patient electronic dossier, standardization may improve and usefulness of these files for AI tools will improve too.

85 On the difficulties related to patient's consent in relation with Big Data, see, e.g., DOCHERTY/LONE (2015), p. 470.

86 Article 3 letter e of the Swiss Federal Act of 19 June 1992 on Data Protection ("FADP" ; RS 235.1). In the European Union, see MAISNIER-BOCHÉ (2017), p. 25.

87 Witholding consent may become increasingly difficult, as CHAR ET AL. (2018) explain in their article at p. 983.

88 See NUFFIELD COUNCIL ON BIOETHICS (2018), p. 5.

89 See Directorate-General for Internal Policies (2016), p. 22 ("once robots have the skills to communicate and interact, not only will they exchange data […], but this communication may be imperceptible to humans").

medical purposes. Merging of data by AI tools should therefore not be allowed without strict legal requirements[90].

C. Further considerations

In this third subsection, we move away from liability issues to present a sampling of issues of significance related to the medical use of AI. Once more, our comments will be brief.

1) Some cost issues

A regular question cropping up in AI debates is the potential cost saving of AI medical tools. Some claims that AI has the potential to massively reduce health care costs. In our country where health care represents 12% of GDP, such a promise is enticing. Even slight reductions would be tempting. It is true that the main budget line is the wages of doctors, whether doctors in private practice or doctors in medical institutions. Thus, if AI could replace at least some of the doctors presently employed, significant savings could be achieved. For example, if far fewer dermatologists or radiologists were needed to diagnose patients[91], this would have an impact on medical expenses ; likewise if some tasks could be delegated to an AI rather than being performed by nurses (e.g., checking on patients). One might also reasonably suppose that if the diagnoses are more reliable, unnecessary and costly care will be entirely avoided ; for example, patients who would have been needlessly treated for a falsely-diagnosed breast cancer will no longer incur the pain and the costs, if the AI tool can better differentiate between benign tumors and those requiring treatment.

Others claim that AI will not dent the current trend of higher medical expenses. It will "behave" as any other medical tool put on this unique market ; it will not be cheap[92] and will generate its own additional costs. Possible savings will be offset by the possibility to offer even more or even better health care in another sector. For example, cancers will be diagnosed sooner in younger patients who will then have to undergo regular check-ups for the rest of their (long) lives.

The answer to this cost question has some (indirect) impact on liability. If an overall cost reduction is achieved, the impetus to use AI tools will be stronger. This may in turn cause more damages imputable to AI, simply

---

90 A different yet interesting question is whether AI systems could be forced to share their data in the name of "open science".

91 See BAMBAUER (2017), p. 393.

92 "Watson generates fees between $200 and $1000 per patient." CHUNG (2017), p. 38.

because their use will have become common. As mentioned earlier, this may also make it harder to reach a conclusion with respect to causality : How can the judge decide that the damage would not have incurred if no AI tool had been used, if there is no longer a human benchmark to make the comparison ?

Another relevance of cost has to do with the feasibility of offering compensation. If significant savings can be obtained, there is a stronger case for redirecting (part of) these savings towards damage indemnification. If the savings benefit the State as payer, the State could then create an indemnification fund or co-finance a social insurance system.

Finally, cost issues may also be viewed in the light of "de-skilling" risks. As Froomkin et al. write : "overreliance on these machines could render obsolete the human cultivation of medical skills and knowhow developed over centuries". Thus, certain medical professions could disappear or be profoundly altered. With European economies already suffering from the weighty financial burden of high unemployment rates and correspondingly low tax revenues, AI could make the situation even worse[93]. Thus, the savings achieved by having less need for doctors could be – at least in the short-run – offset by the need to pay social benefits to those professionals now without work. Hiring the human doctors made redundant to oversee the continuous efficacy of AI tools could be a (partial) solution[94].

2) *Some antitrust issues*

AI are being developed both by giant companies and by start-ups. However, it appears likely that the IT giants will be first on the market. Given that medical AI tools may be seen as high-risk devices, hospitals may well favor the most-established players. To know that IBM is behind an AI diagnostic tool is more reassuring than if it is a start-up still relying on venture capital to make ends meet. However, this may imply an ever greater control of a few companies over our entire medical histories. The logic behind AI is that the more the data and the better the data[95], the more reliable the output[96]. However, making a huge volume of data available to just a few companies raises concerns. Merging of data across various databases is likely to make re-identification of

---

93 See GUIHOT ET AL. (2017), p. 411-413 ; GOUVERNEMENT FRANÇAIS, p. 2 ; LOH (2018) ; U.K. SCIENCE AND TECHNOLOGY COMMITTEE (2016).

94 See FROOMKIN ET AL. (2018), p. 63.

95 "The world is estimated to produce more than 2.5 quintillion bytes of data every day (a quintillion is 1 followed by 18 zeros)". DOUGLAS B. FRIDSMA, *Health informatics : a required skill for 21st century clinicians*, 362 BJM Editorial (July 2018). According to DELOITTE (2015) citing IBM, "90 percent of the world's data was generated just in the past two years".

96 See, e.g., EUROPEAN COMMISSION (April 2018) ("access to data is a key ingredient for a competitive AI landscape, which the EU should facilitate").

the individual patients possible ; harms caused by possible security breaches are then magnified.

Additionally, having a few companies exercising control over medical AI may trigger concerns about possible abuse of dominant positions[97]. These companies may charge unfair prices ; they may impose unfair conditions, for example relating to data access and data re-use ; they may discriminate between clients favoring some over others (e.g., larger hospitals securing better deals). Their behavior on the market may be viewed as opaque. They may discourage innovation from smaller players, given the high likelihood for a possible network or platform effect.

For these reasons, the development of medical AI should go hand in hand with careful surveillance of the market to avoid the emergence of dominant players[98]. Similarly, authorities should make sure that anticompetitive agreements are not entered into between AI developers and medical institutions. In particular, there should be no exclusivity clause blocking a health care facility with a certain AI developer. Access to medical data should be on fair and equal terms.

3) Some ethical issues

Use of AI will also drive us to question the patient-doctor relationship. AI is yet one more tool in the field of medicine that appears increasingly dehumanized[99]. Of course, a better diagnosis is better for patient, as is a better treatment choice. However, when more and more tasks can be delegated to a non-human tool, the place that was ascribed to this central patient-doctor relationship evaporates. If or when AI robots can do everything better than doctors, why would a patient still see a doctor ?

Yet in many cases the patient is helped by the kind words or the generally benevolent attitude of the doctor or of the nurse. Knowing that someone really cares is an efficient yet subtle aspect of health care. Patients may fare worse just because they can no longer talk with a human being, even if that talk had little to do with medical decision-making[100]. Social relationships matter, yet AI tools may lead us to discounting their effectiveness, as AI tools may exhibit

---

97 See more generally, BENSAMOUN (2017), p. 31. Also LUTZMANN (2017), p. 386.

98 "A proper enforcement of merger control, antitrust and state aid rules can prevent market distortions and the creation of bottlenecks in the digital value chain." See EUROPEAN POLITICAL STRATEGY CENTRE (2018), p. 11.

99 See e.g., LOPER (2018) ; SHAPSHAY (2014), p. 191.

100 As the EUROPEAN PARLIAMENT (2017) points out : "human contact is one of the fundamental aspects of human care ; […] replacing the human factor with robots could dehumanize caring practices" (point 32). Some authors believe that patients should be entitled to refuse the involvement of robots in their care. See, e.g., DIRECTORATE-GENERAL FOR INTERNAL POLICIES (2016), p. 21 ("not accepting this refusal would violate their dignity") ; KIEFER (2017).

higher specificity (true negative rate) and sensitivity (true positive rate) when delivering a diagnosis or when choosing the right treatment (as compared to human action). Human interactions may also come to be perceived as just too expensive, when their costs are compared to that an AI robot[101].

Thus, AI may force us to rethink the social nature of medicine. The new role of doctors may become less technical and more social. Of course, this is not – or not yet – what doctors have trained for. Such a radical change in the ascribed mission of doctors may feel uncomfortable to some. It may come with a loss in social status : the doctor may no longer be viewed as a respected medical expert, but more as a friend holding one's hand.

AI may also have direct adverse consequences on health care providers. Once AI tools become able to keep track of all human actions in a given medical setting, they may be used to point out the failure of human staff. For example, the AI may point out that the doctor did not wash her hands when entering the patient's room[102], that the surgeon did not follow the hospital procedure when operating, that the nurse failed to check on certain patients. Working in surroundings where AI constantly checks on the employees' behavior can lead to a toxic work environment. It will therefore be necessary to impose certain constraints or employee's safeguards as AI is deployed for surveillance functions.

Finally, the issue of bias in medicine is often highlighted, as AI may build on and amplify such bias[103]. Because AI learns directly from the data it is being fed with, often with very few human filters, AI is prone to reproduce the bias and mistakes of human doctors. It may even reinforce them[104]. For example, if a AI tool is being given pictures of possible melanoma on white and brown skins and the labeling benign vs. cancerous is more often false in the case of patients with brown skins, AI will repeat the same mistake over and over. Or if women suffering from heart attacks are usually offered a less aggressive pharmaceutical treatment than men, the AI tool may assume this is indeed the "normal" standard of treatment and suggest the same when interrogated by health care professionals. Similarly, data samples from which AI tools would learn may not represent the entire population, because patients in the samples only come from certain groups (e.g., richer patients visiting this private clinic or poorer patients going to an emergency service) ; if the data exploited by AI

---

101 "[A]s it will be less expensive for people to have robots than a human helper at home, there is a risk that machines becoming the norm and people the exception". DIRECTORATE-GENERAL FOR INTERNAL POLICIES (2016), p. 24.

102 See YEUNG ET AL. (2018), p. 1272.

103 NUFFIELD COUNCIL ON BIOETHICS (2018), p. 5 ; PACKIN/LEV-ARETZ ; LOH (2018), p. 3 ; CHEN/ASH (2017), p. 2507 ; CHAR ET AL. (2018), p. 982. For examples of AI bias beyond medicine, see EUROPEAN POLITICAL STRATEGY CENTRE (2018), p. 7.

104 See FROOMKIN ET AL. (2018). According to certain authors, "AI-based predictions should only be relied on if someone is continuously checking predictions against reality". Id. p. 48.

are not representative of the population[105], relevant characteristics unique to certain groups may be overlooked[106]. Because human beings are rarely aware of their biases or potential for bias, they are usually not able to educate AI tools to overcome them. In addition, broad scale use of AI tools may hide these biases, since AI often operates as a "black box" ; it would then be even harder to identify and correct these recurrent mistakes. Identifying solutions to this problem will not be easy[107].

IV. Conclusion

Ideally, an adequate regime of AI should be agreed upon internationally so that the standard adopted is harmonized. Having a unique or at least roughly equivalent standard would create a level-playing field where companies could compete in a prosocial manner. This would avoid a race to the bottom where the cheaper products would come at the price of inadequate patient safety (whether physical harm or privacy harm). In the case of AI, patients are not in a position to choose the safer products. Even medical institutions may not be able to make the right choice, because they too may not fully understand how AI functions. Moreover, AI is likely to be licensed based on complex contract terms, which physicians will certainly not read. Finally, if AI tools become available only in a purely dematerialized way (i.e., purely on-line), users may not even be able to locate where the AI developer is based (or the AI developers are based). These difficulties are already occurring now with some internet services.

Hence, it is crucial to ensure that all AI tools meet basic safety standards, regardless of where they were produced. This uniform regime should guarantee that patients are not barred from opening action in their own jurisdiction under the law of their own country.

As a further step, an internationally agreed-upon regime could propose a basic insurance format, obliging all AI product to be licensed with such a standard insurance coverage. Thus, a hospital subscribing a license for an AI tool would know that a portion of the price paid would be pooled by a duly appointed insurance company to cover certain patient damages.

AI has the potential to improve human health. Among the most important questions we may need to ask ourselves is whether this is the type of

---

105 See TERRA NOVA (2017), p. 30.

106 For example, the AI Watson performed poorly when used in a Korean hospital, apparently because it had been trained using the data from US patients. CHUNG/ZINK (2017), p. 5.

107 Proposing some solutions, GIANFRANCESCO ET AL. (2018), p. 1546. Most of these proposals, although relevant, are costly to implement (e.g., "ensure interdisciplinary approach and continuous human involvement" ; "conduct follow-up studies to ensure results are meaningful").

improvement that we most need. AI will be deployed – at least at the beginning – in specialized medical settings to deliver specialty health care. However, there are other areas where the basic health services are still sorely lacking[108]. Hence, excitement over such sophisticated tools seems a bit out of place when one realizes that millions of people still lack basic access to health care – let alone good and affordable health services. Even in Switzerland, many people encounter financial hardships when faced with medical bills[109] - because the medical services are not reimbursed (e.g., dental care), because of high deductibles, because of the high copay or because of the ever-increasing monthly premiums[110].

Investing in broader access to health care and in better preventive services is likely to lead to greater social returns than investing in AI. Choosing the right priorities for our times is perhaps more important than dreaming of futuristic tools. Of course, one is not necessarily exclusive of the other. However, medicine tends to focus and rely on technical tools, sometimes excessively – forgetting about the simple measures that make the greatest difference.

As a conclusion, we will remind ourselves that health is primarily determined by social factors – first among them the wealth, the social and the educative attainment level of the individual. Statistically speaking, being rich, highly-educated and well-integrated in society leads to an overall higher life expectancy in good health – as compared to those who are not so fortunate. At least for now, AI is unlikely to change this grim but fundamental truth. Honesty and fairness call for us doing our best to improve the situations of those most in need. AI may contribute to this goal, but how exactly is still open for debate.

---

108 For a short but poignant piece highlighting the gap between our medicine and the medicine of poorer countries, see LILIC (2018), p. 1202.

109 "Lorsqu'un assuré ne paie pas sa prime, c'est au canton de combler le manque à gagner des caisses à hauteur de 85%. En 2016, les cantons romands ont ainsi versé 163,7 millions de francs aux assureurs, selon les chiffres recueillis par la RTS. Le montant total des primes impayées en Suisse est quant à lui estimé à 843 millions de francs par l'Office fédéral de la santé publique (OFSP)." THÉO ALLEGREZZA, *Les cantons règlent des millions de francs de primes maladie impayées*, 12 October 2017, RTS, at https://www.rts.ch/info/suisse/8982179-les-cantons-reglent-des-millions-de-francs-de-primes-maladie-impayees.html (consulté le 1er août 2019).

110 "La hausse de 1,2% est inférieure à la moyenne des années précédentes. Depuis 2008, la prime moyenne a augmenté de 3,5% par an et de 3,9% par an depuis l'entrée en vigueur de l'assurance obligatoire des soins en 1996." Federal Office for Public Health, press release of 24 September 2018.

V. Reference list

Académie (française) des technologies, Renouveau de l'Intelligence artificielle et de l'apprentissage automatique, Rapport, March 2018, http://academie-technologies-prod.s3.amazonaws.com/2018/06/01/14/25/31/28/IA_Web.pdf (dernière consultation le 1er août 2019).

ALLAIN Jessica, From Jeopardy! to Jaundice : The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems, 73:4 Louisiana Law Review, 2013, pp. 1049-1078, https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=6423&context=lalrev (dernière consultation le 1er août 2019).

BAMBAUER Jane, Dr. Robot, 51:383 University of California, Davis, 2017, pp. 383-398, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3087983 (dernière consultation le 1er août 2019).

BAUME Cédric, Gestion des risques cliniques et responsabilité médoc-hospitalière, Collection IDS - Unine, 2015.

BENSAMOUN Alexandra, Intelligence artificielle et santé : l'intégration en droit de l'IA médicale, 17 Journal de droit de la Santé et de l'Assurance Maladie, 2017.

CHAR Danton S. et al., Implementing Machine Learning in Health Care – Addressing Ethical Challenges, 378:11 New England Journal of Medicine 2018, pp. 981-983.

CHEN Jonathan/ASCH Steven, Machine Learning and Prediction in Medicine – Beyond the Peak of Inflated Expectations, 376:26 New England Journal of Medicine, 2017, pp. 2507-2509.

CHOI Edward et al., Doctor AI : Predicting clinical events via recurrent neural networks, 56 Proceedings of Machine Learning for healthcare, pp. 301-3182016, http://proceedings.mlr.press/v56/Choi16.pdf (dernière consultation le 1er août 2019).

CHUNG Jason, What should we do about artificial intelligence in health care, 22:3 Health Law Journal, 2017, pp. 37-40.

CHUNG Jason/ZINK Amanda, Hey Watson, Can I sue you for malpractice ? Examining the liability of Artificial Intelligence in medicine, Asia-Pacific Journal of Health Law, Policy and Ethics, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3076576 (dernière consultation le 1er août 2019).

DELOITTE, Disruption ahead, Deloitte's point of view on IBM Watson, March 2015.

DIPROSE William/BUIST Nicholas, Artificial intelligence in medicine : humans need not apply? 129 NZMJ May 2016, pp. 73-76, https://www.nzma.org.nz/__data/assets/pdf_file/0007/49579/Diprose-2155FINAL1434.pdf (dernière consultation le 1er août 2019).

Directorate-General for Internal Policies (European Parliament), Policy Department, Citizens' Rights and Constitutional Affairs, European Civil Law Rules in Robotics, Study for the JURI Committee, 2016, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU%282016%29571379_EN.pdf (dernière consultation le 1er août 2019).

Ernst & Young (EY) with the support of Technopolis Group and VVA Consulting, European Commission, Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products, Final Report, January 2018, https://publications.europa.eu/en/publication-detail/-/publication/d4e3e1f5-526c-11e8-be1d-01aa75ed71a1/language-en (dernière consultation le 1er août 2019).

European Commission, Artificial Intelligence for Europe, Communication, COM(2018) 237 final, April 2018, https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

European Commission, Report on the application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), SWD(2018) 157 final, COM(2018) 246 final (May 2018), https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-246-F1-EN-MAIN-PART-1.PDF.

European Commission Staff, Evaluation of Council Directive 85/374/EEC of 25 July 1985, Working Document SWD(2018) 157 final, May 2018, https://ec.europa.eu/transparency/regdoc/rep/10102/2018/EN/SWD-2018-157-F1-EN-MAIN-PART-1.PDF.

European Parliament, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, P8_TA(2017)0051, 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//FR.

European Parliament Research Service (EPRS), Scientific Foresight Unit (STOA), Should we fear artificial intelligence ? In-Depth Analysis, Science and Technology Options Assessment, March 2018,

http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA%282018%29614547_EN.pdf.

European Parliamentary Research Service Scientific Foresight Unit (STOA), A Common EU approach to liability rules and insurance for connected and autonomous vehicles, European Added value Assessment, February 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf.

European Political Strategy Centre, The Age of Artificial Intelligence, Towards a European Strategy for Human-Centric Machines, EPSC Strategic Notes, March 2018, https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf.

FROOMKIN Michael et al., When AIs Outperform Doctors : The dangers of a tort-induced over-reliance on machine learning and what (not) to do about it, University of Miami Legal Studies Research Paper No. 18-3, available at SSRN : https://ssrn.com/abstract=3114347 or http://dx.doi.org/10.2139/ssrn.3114347.

GIANFRANCESCO Milena et al., Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data, 178 (11) JAMA Internal Medicine, 2018, https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2697394.

GIL Yolanda et al., Amplify scientific discovery with artificial intelligence, 346 Science Magazine 2014, pp. 171-172, http://science.sciencemag.org/content/346/6206/171/tab-pdf.

GOLDEN Jeffrey Alan, Deep learning Algorithms for Detection of Lymph Node Metastases from Breast Cancer, 318(22) JAMA 2017, pp.2184-2186, https://jamanetwork.com/journals/jama/fullarticle/2665757.

Gouvernement français, France Intelligence Artificielle, Rapport de synthèse, 2017, https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/174000247.pdf.

GREENBERG Anastasia, Artificial Intelligence in Health Care : Are the Legal Algorithms Ready for the Future ? McGill Journal of Law and Health (2017), https://mjlh.mcgill.ca/2017/10/06/artificial-intelligence-in-healthcare-are-the-legal-algorithms-ready-for-the-future/.

GUIHOT Michael et al., Nudging Robots : Innovative Solutions to Regulate Artificial Intelligence, Vanderbilt Journal of Entertainment and Technology Law, 20(2), 2017, pp. 385-456, https://eprints.qut.edu.au/109926/1/Guihot%20Matthew%20Suzor%2020017%20Nudging%20Robots.pdf.

JACQUEMIN Hervé/de Streel Alexandre, L'intelligence artificielle et le droit, Editeur Larcier, Collection CRIDS, 2017.

KIEFER Bertrand, L'IA, l'autre et le soignant, Revue médicale Suisse, 2017, p. 1816.

KOWERT Weston, The Foreseeability of Human-Artificial Intelligence Interactions, 96:1 Texas Law Review, 2017, pp. 181-204, https://texaslawreview.org/wp-content/uploads/2017/12/Kowert.pdf.

KRELL ZBINDEN Karola/Langhorst Maren, « Les organismes génétiquement modifiés – Une responsabilité de genie », in: Les responsabilités fondées sur le risque, Colloque du droit de la responsabilité civile 2017, Ed. F. Werro/P. Pichonnaz, Stämpfli, 2018.

LEHMAN-WILZIG Sam, Frankenstein Unbound, Towards a legal definition of Artificial Intelligence, Futures 1981, pp. 442-457, https://www.researchgate.net/publication/229067941_Frankstein_unbound_Towards_a_legal_definition_of_artificial_intelligence (dernière consultation le 1er août 2019).

LILIC Nikola, Murmurs of Politics and Economics, 379:13 New England Journal of Medicine, 2018, pp. 1202-1203, https://www.nejm.org/doi/pdf/10.1056/NEJMp1806115 (dernière consultation le 1er août 2019).

LOH Erwin, Medicine and the rise of the robots : a qualitative review of recent advances of artificial intelligence in health, BMJ Leander, June 2018, https://bmjleader.bmj.com/content/leader/early/2018/06/01/leader-2018-000071.full.pdf.

Loper Peter Louis, The Electronic Health Record and Acquired Physician Autism, 172(11) JAMA Pediatrics 2018, p. 1009, https://jamanetwork.com/journals/jamapediatrics/fullarticle/2703482 (dernière consultation le 1er août 2019).

LUTZMANN Steve, Digitalisierung und Rechssicherheit, GesKR (Gesellschafts- und Kapitalmarktrecht) 2017, pp. 383-386.

MAISNIER-BOCHÉ Lorraine, Intelligence artificielle et données de santé, 17 Journal de droit de la Santé et de l'Assurance Maladie, 2017, pp. 25-29.

MARCHAND Sylvain, « Les fondamentaux de la responsabilité du fait des produits – Exposé introductive : sources, for et droit applicable, producteur et défaut », in: La responsabilité du fait des produits, Journée de responsabilité civile 2016. Ed. Chappuis et Winiger, Schulthess 2018, pp. 11-30.

MORISSE Tom, « Enjeux et histoire de l'Intelligence Artificielle », in: Intelligence Artificielle, un nouvel horizon : Pourquoi la France a besoin d'une culture du numérique, Les Cahiers Lysias, 2017.

NUFFIELD COUNCIL ON BIOETHICS, Artificial Intelligence (AI) in healthcare and research, Bioethics Briefing Note May 2018, http://nuffieldbioethics.org/wp-content/uploads/Artificial-Intelligence-AI-in-healthcare-and-research.pdf (dernière consultation le 1er août 2019).

PACKIN NIZAN Geslevich/Lev-Aretz Yafit, Research Handbook of Law and AI (Woodrow Barfield & Ugo Pagallo eds.) Baruch College Zicklin School of Business Research Paper No. 2018-04-03, 2018.

PETRELLUZZI Julia/MILIOTIS Marie, L'intelligence artificielle : ses enjeux en droit civil européen, Editions Universitaires Europeénnnes (EUE), Editeure : M. Clément-Fontaine, 2017.

PICHONNAZ Pascal/WERRO Franz, « La responsabilité fondée sur le risqué : un état des lieux et quelques perspectives d'avenir », in Les responsabilités fondées sur le risque, Colloque du droit de la responsabilité civile 2017, Ed. F. Werro/P. Pichonnaz, Stämpfli, 2018, p.1-26.

SCHWARTZ William et al., Artificial Intelligence in Medicine, Where we stand ?, 316:11 New England Journal of Medicine, 1987, pp. 685, https://www.nejm.org/doi/pdf/10.1056/NEJM198703123161109 (dernière consultation le 1er août 2019).

SHAPSHAY Stanley, Artificial Intelligence, The Future of Medicine ? 140:3 JAMA Otolaryngology, 2014, p. 191, https://jamanetwork.com/journals/jamaotolaryngology/fullarticle/1812651 (dernière consultation le 1er août 2019).

SHORTLIFFE Edward/SEPÙLVEDA Martin, Clinical Decision Support in the Era of Artificial Intelligence, JAMA e1 (on-line), 2018, https://jamanetwork.com/journals/jama/fullarticle/2713901?guestAccessKey=73555101-6acd-47b6-b1bf-b7ffd6265b37&utm_source=silverchair&utm_medium=email&utm_campaign=article_alert-jama&utm_content=olf&utm_term=110518 (dernière consultation le 1er août 2019).

TERRA Nova, La santé à l'heure de l'intelligence artificielle, http://tnova.fr/notes/la-sante-a-l-heure-de-l-intelligence-artificielle (dernière consultation le 1er août 2019).

TRAN Laurent/ETIER Guillaume, « Responsabilité du fait des produits : le risque de développement », in: La responsabilité du fait des produits, Journée de responsabilité civile 2016. Ed. Chappuis et Winiger, Schulthess 2018, pp. 105-130.

TSCHIDER Charlotte, Deus ex Machina : Regulating Cybersecurity and Artificial Intelligence for Patients of the Future, 5 Savannah L. Rev. 177, 2018, available at SSRN : https://ssrn.com/abstract=3070000 (dernière consultation le 1er août 2019)

U.K (United Kingdom) Science and Technology Committee, House of Commons, Robotics and artificial intelligence, Fifth Report of Session 2016-17, 2016, https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf (dernière consultation le 1er août 2019).

VIGNERON-MAGGIO-APRILE Sandra, « Les fondamentaux de la responsabilité du fait des produits – Entre dommage et causalité : la perte d'une chance au secours du lésé », in: La responsabilité du fait des produits, Journée de responsabilité civile 2016. Ed. Chappuis et Winiger, Schulthess 2018, pp. 31-58.

VOKINGER, Kerstin Noëlle et al., Artificial Intelligence and Machine Learning in der Medizin, Jusletter du 28 août 2017.

WERRO Franz, « La responsabilité pour produits pharmaceutiques défectueux dans la jurisprudence récente », in: La responsabilité du fait des produits, Journée de responsabilité civile 2016., Ed. Chappuis et Winiger, Schulthess 2018, pp. 77-104.

WERRO Franz, Commentaire de l'art. 398 CO, in: Commentaire romand du Code des Obligations I, Ed. Thévenoz/Werro, Helbing Bâle 2012, p. 2397 et ss.

WISE Jacqui, AI system interprets eye scans as accurately as top specialists, 362 BMJ,August 2018, https://www.bmj.com/content/bmj/362/bmj.k3484.full.pdf (dernière consultation le 1er août 2019).

YEUNG Serena et al., Bedside Computer Vision – Moving Artificial Intelligence from Driver Assistance to Patient Safety, 378:14 New England Journal of Medicine 2018, pp. 1271-1273, https://www.nejm.org/doi/pdf/10.1056/NEJMp1716891 (dernière consultation le 1er août 2019).

Hot topics en matière de responsabilité civile : prescription et remise de gain

Christine Chappuis*

Table des matières

I. Introduction 152
II. Le nouveau droit de la prescription 152
A. En bref 153
1. L'origine et les étapes 153
2. L'allongement des délais 154
B. Cours et effets de la prescription 156
1. L'empêchement et la suspension de la prescription 156
2. La renonciation à la prescription 157
3. Autres règles nouvelles ou modifiées 161
C. Appréciation de la réforme 162
III. La remise du gain suite à une campagne médiatique attentatoire à l'honneur 164
A. Deux affaires à considérer 164
B. Quelles leçons pour la remise du gain ? 166
C. Perspectives d'avenir et élargissements possibles 169
IV. Conclusion 171
V. Ouvrages cités 172

* Professeure à la Faculté de droit de l'Université de Genève. L'auteure remercie Dino Vajzovic, assistant doctorant à la Faculté de droit de l'Université de Genève, de sa relecture précise et de ses commentaires critiques.

I. Introduction

Le sujet chaud de l'année en droit de la responsabilité civile est sans conteste la révision du droit de la prescription. Cette révision touche les règles générales, même si elle est issue de questions relatives au droit de la responsabilité civile. Elle aura un impact considérable sur les litiges dans ce domaine. Adoptée le 15 juin 2018 par les Chambres fédérales, elle entrera en vigueur le 1er janvier 2020[1] (I.). Sur le plan de la jurisprudence, l'on s'arrêtera à une décision de 40 pages[2], non traduite en français, constatant que deux entreprises de presse (*Tamedia & Espace Media*) avaient violé les droits de la personnalité de la victime par leur participation à une campagne médiatique, et les condamnant à la remise du gain en résultant conformément à l'art. 423 CO. Cette décision mérite une mise en perspective dans l'optique du complément qu'apporte la remise du gain aux classiques actions réparatrices (II.).

II. Le nouveau droit de la prescription

A titre préalable, il s'impose de relever que le chapitre de la prescription[3] est l'un des plus ratés du Code des obligations, dont la révision est réclamée de toutes parts avec insistance[4]. La multiplication de décisions dans les vingt dernières années en est un signe qui ne trompe pas. Tant la brièveté de certains délais (un an et dix ans, selon les art. 60 et 67 CO) particulièrement cruelle s'agissant des dommages différés, que l'absence de règlementation de la renonciation à la prescription si fréquente en pratique, ont encombré les tribunaux, voire les ont embarrassés.

Avant d'entreprendre ce voyage vers le futur, un mot sur la raison d'être de la prescription s'impose. L'exception de prescription est mal aimée. Elle permet au débiteur, qui ne conteste nullement l'existence de sa dette, d'en refuser l'exécution de manière définitive en raison du seul écoulement du temps, un argument généralement considéré comme faible. On parle à cet égard de paralysie du droit d'action liée à une créance qui continue d'exister. C'est l'intérêt public à la paix sociale et à la sécurité juridique qui commande qu'un créancier ne puisse plus s'en prendre à son débiteur lorsque trop de temps s'est écoulé depuis la naissance de la créance. L'institution juridique de

---

1 Code des obligations (Révision du droit de la prescription), Modification du 15 juin 2018, FF 2018 3655 ; RO 2018 5343. Nouvelles dispositions : ci-après nCO.

2 ATF 143 (2017) III 297, A. et B. AG contre Tamedia AG et Espace Media AG.

3 Le nouveau droit englobe les art. 127 à 142 CO, les autres règles du CO et celles des lois spéciales. Pour une brève présentation récente, voir PICHONNAZ, RSJ 2019, p. 248 s.

4 LOSER-KROGH (2003), p. 217 ss ; CHAPPUIS (2006), p. 190 s. ; PICHONNAZ (2007), *passim*. Voir aussi, OR CO 2020-HUGUENIN/HILTY, Einleitung vor Art. 1 ff, N 21 ; OR CO 2020-THOUVENIN/PURTSCHERT, Vorb. Art. 148-162 N 3-8.

la prescription se justifie également par la protection d'un intérêt privé, celui du débiteur à ne pas être recherché par son créancier des années après la naissance de la créance. L'idée est que le débiteur se trouverait dans l'impossibilité de se défendre efficacement à un moment où tant la mémoire que les documents nécessaires à la preuve des faits pertinents peuvent avoir disparu. Que l'on place l'intérêt public avant l'intérêt privé ou l'inverse, il est aujourd'hui acquis que l'institution de la prescription poursuit les deux types d'intérêt[5].

A. En bref

1. L'origine et les étapes

La modification du droit de la prescription trouve son origine dans l'avant-projet de modification du droit de la responsabilité civile qui contenait des règles sur la prescription (art. 55 à 55c AP)[6]. Abandonné en 2009, cet avant-projet a débouché sur une révision partielle dont le but, plus restreint, était d'allonger les délais de prescription en matière de responsabilité civile pour permettre aux victimes d'introduire une action en dommages-intérêts, même lorsque le dommage se produit à long terme[7] (dommage dit différé). Un avant-projet a été mis en consultation en 2011. Prenant acte des résultats de la procédure de consultation, le Conseil fédéral charge le Département de justice et police le (DFJP) d'élaborer un message en 2012, message qui est adopté l'année suivante[8].

Vu les résultats contrastés de la procédure de consultation, les autorités politiques ont renoncé à une unification totale et préféré une harmonisation des règles sur la prescription. La réforme poursuit désormais trois objectifs :

---

5 Sur cette question, CR CO I-PICHONNAZ, CO 127 N 2-3 et réf. cit. n. 4. Cf. aussi, ATF 143 III 348, 358 c. 5.3.2 : « L'institution de la prescription est justifiée, d'une part, par des intérêts publics que sont la sécurité et la clarté du droit et la paix juridique et, d'autre part, par la protection du débiteur, qui ne saurait être laissé durablement dans l'incertitude sur le point de savoir si une créance qui n'a pas été invoquée pendant longtemps le sera et être contraint de conserver indéfiniment des preuves de paiement (ATF 137 (2011) III 16 consid. 2.1) ».

6 Cf., en particulier, l'art. 55 al. 1 AP : « L'action en réparation du dommage se prescrit par trois ans à compter du jour où la personne lésée a eu connaissance du dommage ainsi que de la personne qui en assume la responsabilité ou la couverture ».

7 Communiqué du 21 janvier 2009 (et liens utiles), <https://www.bj.admin.ch/bj/fr/home/aktuell/news/2009/ref_2009-01-21.html > (consulté le 7.12.18).

8 Message relatif à la modification du code des obligations (Droit de la prescription) du 29 novembre 2013, FF 2014 221 ss (ci-après, Message, Droit de la prescription (2013)). Le message de 2013 conserve toute son importance pour les règles qui seront adoptées avec quelques modifications en 2018.

l'harmonisation du droit de la prescription, l'allongement des délais et l'élimination des points incertains[9].

L'ombre de l'amiante et de ses effets dévastateurs aura plané sur tout le processus de révision. Moteur de la révision, la réparation des dommages différés – en particulier ceux causés par une exposition à l'amiante – ne trouve en réalité pas de solution dans l'allongement des délais prévus par le projet, sauf si la survenance du dommage n'est pas différée de plus de vingt ans à compter du fait dommageable. C'est la constitution d'un *Fonds d'indemnisation des victimes de l'amiante (EFA)*[10] en mars 2017, qui aura permis de sortir de l'impasse grâce à l'aide rapide et sans bureaucratie inutile promise aux victimes de l'amiante et à leurs proches.

Quelques points particulièrement saillants de la réforme du point de vue de la responsabilité civile seront abordés ci-après.

2. *L'allongement des délais*

La durée des délais est modifiée non seulement dans le CO et le CC, mais également dans d'autres législations. Tout en conservant le système du double délai, les nouvelles dispositions font passer le délai relatif d'un an à trois ans (art. 60 al. 1 nCO). Le délai absolu reste fixé à dix ans, sauf pour l'indemnisation du dommage corporel (mort ou lésions corporelles), qui se prescrira désormais par vingt ans (art. 60 al. 1bis nCO). La prescription de vingt ans vaudra aussi lorsque le dommage corporel résulte d'une « faute contractuelle » (art. 128a nCO).

L'unification voulue par les nouvelles règles est de deux ordres. En premier lieu, en cas de dommage corporel, le régime de la prescription est le même, que le fondement de la prétention en réparation soit délictuel (art. 41 ss CO) ou contractuel (inexécution d'une obligation au sens des art. 97 ss CO)[11]. L'unification sur ce point est bienvenue. Lorsque la victime subit un dommage corporel, il n'y a aucune raison que le fondement de la réparation modifie la durée de la prescription de l'action en réparation du préjudice. A noter que, pour les dommages autres que corporels causés par une faute contractuelle, la prescription reste soumise aux règles générales selon lesquelles le délai (unique) de dix ans court dès que la créance et devenue exigible (art. 127 et 130 al. 1 CO). Par ailleurs, l'unification s'étend à la prétention en enrichissement

---

9 Message, Droit de la prescription (2013), p. 227.

10 <https://www.stiftung-efa.ch/fr/> (consulté le 7.12.18). Les victimes demandant une indemnisation à ce fonds sont apparemment moins nombreuses que prévu, si l'on en croit un article du Courrier du 23.1.19 : <https://lecourrier.ch/2019/01/23/victimes-de-lamiante-14-million-pour-les-survivant-e-s/> (consulté 29.1.19) ; voir aussi, communiqué de presse du 18.12.18 : <https://www.stiftung-efa.ch/fr/communique-de-presse-la-fondation-efa-verse-14-million-de-francs/> (consulté le 29.1.19).

11 Nouveaux art. 60 al. 1*bis* et 128a nCO.

illégitime à propos de laquelle le nouvel art. 67 al. 1 nCO prévoit que « [l]'action pour cause d'enrichissement illégitime se prescrit par trois ans à compter du jour où la partie lésée a eu connaissance de son droit de répétition et, dans tous les cas, par dix ans à compter de la naissance de ce droit ». À noter que les controverses liées à la prescription du droit à restitution du prix ensuite de l'invalidation d'un contrat pour erreur (art. 23, 24, 31 et 67 al. 1 CO) vont subsister[12]. En effet, ni le point de départ du délai absolu, ni la durée du délai (dix ans) ne sont modifiés.

En second lieu, le double délai de trois ans, respectivement dix, ans a été généralisé pour bon nombre de lois spéciales. Il en va ainsi de la réparation du dommage en matière de circulation routière par le biais d'un renvoi aux dispositions du CO (art. 83 al. 1 nLCR[13]). D'autres dispositions ont été adaptées sans renvoi au CO[14].

Certaines lois sont exceptées de cette vague unificatrice, ainsi les délais de prescription et de péremption en matière de responsabilité du fait des produits, dont la durée correspondait déjà aux nouvelles règles : les art. 9 et 10 LRFP, qui prévoient un délai de prescription de 3 ans et un délai de péremption de 10 ans, resteront inchangés du fait que ces dispositions constituent la reprise volontaire du contenu d'une directive européenne[15]. De même, les délais plus longs prévus par le droit actuel ne font pas l'objet de modification[16] (p. ex., l'art. 32 al. 1 LGG[17], qui prévoit un double délai de trois et de trente ans, ou l'art. 25 LAVI qui prévoit un délai de péremption de cinq ans[18]). La prescription des actions en responsabilité des entreprises de transport[19], régie par les art. 40a-f de la loi fédérale sur les chemins de fer (LCdF), profitera sans modification du renvoi de l'art. 40f LCdF au CO.

---

12 ATF 114 II 131, JdT 1988 I 508 (Picasso).

13 Art. 83 al. 1 nLCR : « Les actions en dommages-intérêts ou en réparation d'un tort moral relatives à des accidents impliquant des véhicules automobiles, des cycles ou des engins assimilés à des véhicules se prescrivent conformément aux dispositions du code des obligations sur les actes illicites » (mise en évidence ajoutée). Même type de renvoi entrant en vigueur au 1.1.2020, par exemple : art. 455 al. 1 CC ; art. 20 al. 1 de la loi sur la responsabilité de la Confédération du 14.3.1958 (LRCF, RS 170.32), art. 143 al. 1 de la loi sur l'armée du 3.2.1995 (RS 510.10), art. 65 al. 1 de la loi fédérale sur la protection de la population et sur la protection civile du 4.10.2002 (RS 520.1), art. 39 al. 1 de la loi sur les installations de transport par conduites du 4.10.1963 (RS 746.1), art. 68 de la loi sur l'aviation du 21.12.1948 (RS 748.0), art. 52 al. 3 de la loi fédérale sur l'assurance-vieillesse et survivants du 20.12.1946 (RS 831.10), etc.

14 Par exemple, les art. 21 nLRCF (droit de recours de la Confédération contre un fonctionnaire) et 23 nLRCF (droit à la réparation de la Confédération contre un fonctionnaire).

15 Message, Droit de la prescription (2013), p. 249 s.

16 Message, Droit de la prescription (2013), p. 250.

17 Loi sur le génie génétique du 21.3.2003 (RS 814.91).

18 Loi sur l'aide aux victimes du 23 mars 2007 (RS 312.5).

19 La liste des lois régissant les entreprises de transport auxquelles sont applicables ces règles de responsabilité figure dans le recueil systématique des lois fédérales sous chiffre 221.112.742.

B. Cours et effets de la prescription

Une fois fixés le point de départ et la durée de la prescription, encore faut-il déterminer comment la prescription s'écoule (1. et 2.) et quels sont ses effets une fois qu'elle est acquise (3.). Le nouveau droit comporte aussi des modifications sur ces trois points.

1. L'empêchement et la suspension de la prescription

Il convient de souligner d'emblée ce qui ne change pas. L'interruption de la prescription par un acte du débiteur ou par celui du créancier (art. 135 ch. 1 et 2 CO) n'a pas été modifiée, et continuera de faire courir un nouveau délai de même durée que le délai interrompu en vertu de l'art. 137 al. 1 CO[20]. La prescription ne court pas (empêchement) ou est suspendue (suspension) si elle avait commencé à courir pour l'une des causes énoncées à l'art. 134 al. 1 CO. Les modifications ont trait au ch. 6 de l'art. 134 CO, disposition qui a par ailleurs été augmentée de deux chiffres nouveaux (ch. 7 et 8).

Chiffre 6 (modifié). L'empêchement ou la suspension de la prescription en raison de l'impossibilité de faire valoir la créance en dommages-intérêts devant un tribunal (étatique ou arbitral) vaudra désormais non seulement pour les tribunaux suisses, mais pour tout tribunal même sis à l'étranger[21]. L'adjonction des mots « pour des raisons objectives » est destinée à souligner le fait que l'impossibilité doit tenir à des « motifs objectifs, totalement indépendants » de la volonté du créancier[22]. Selon l'arrêt cité par le Message[23], tel est le cas lorsqu'il n'existe pas de for en Suisse ; cependant, s'il existe des biens séquestrables en Suisse et que le créancier le sait de manière certaine, le créancier doit les faire séquestrer et peut agir en validation au for du séquestre. Dans ce genre de cas, rien n'empêche le créancier de faire valoir la créance devant un tribunal suisse. L'impossibilité visée par l'art. 134 al. 1 ch. 6 CO n'entre donc pas en ligne de compte.

Chiffre 7 (nouveau). Ce chiffre reprend le contenu de l'actuel art. 586 al. 2 CC, selon lequel la prescription des dettes de la succession est suspendue pendant l'inventaire qui empêche le créancier de faire valoir des poursuites. Cette règle pourrait concerner la victime créancière d'une prétention en réparation contre une personne décédée dont la succession fait l'objet d'un inventaire.

---

20 CR CO I-PICHONNAZ, CO 137 N 2 ; BSK OR I-DÄPPEN, CO 137 N 2. ATF 141 (2015) V 487 c. 2.3 ; ATF 121 (1995) III 270 c. 3c, SJ 1996 2.

21 Message, Droit de la prescription (2013), p. 244.

22 Message, Droit de la prescription (2013), p. 245, qui se réfère à l'ATF 134 (2008) III 294 c. 1.1, JdT 2010 I 75.

23 ATF 134 (2008) III 294 c. 1.1, JdT 2010 I 75.

Chiffre 8 (nouveau). Des discussions en vue d'une transaction, une médiation ou toute autre procédure extrajudiciaire visant la résolution du litige en responsabilité civile auront également pour effet d'empêcher ou de suspendre la prescription[24]. Il s'agit d'une véritable nouveauté. Cette disposition devrait être de première importance dans le domaine de la responsabilité civile, où l'on voit fréquemment de longues négociations avec l'assureur de la partie responsable. Elle est de nature à soulager la victime de démarches tendant à interrompre la prescription, et à éviter des poursuites à la partie responsable. Un bémol cependant. Il faut que les parties « en » soient convenues par écrit. De quoi exactement les parties doivent-elles convenir par écrit ? Suffit-il que les discussions mentionnées par le chiffre 8 prennent la forme écrite ? Le doute pouvant entourer le mot « en » est levé par le Message. Celui-ci précise que, pour des motifs de sécurité juridique, l'accord écrit des parties devra « indiquer précisément la période d'empêchement ou de suspension (par ex. en mentionnant les dates exactes), ainsi que les créances, ou du moins les rapports juridiques concernés »[25]. Si l'on imagine des négociations entre une victime inexpérimentée et un assureur rompu à la défense de ses propres intérêts, un accord écrit au sens de l'art. 13 CO manquera le plus souvent au dossier. La nouveauté bienvenue de ce cas d'interruption ou de suspension de la prescription ne pourra jouer un rôle positif que pour des victimes assistées d'un conseil ; pour les autres, le nouvel art. 134 ch. 8 CO risque bien de rester lettre morte faute d'un accord écrit au contenu juridique si spécifique. Cela dit, le contenu exact de l'accord des parties n'est nullement précisé par le texte légal. Et l'on voit mal un accord écrit sur un motif d'empêchement, qui ne mentionnerait pas les « dates exactes », rester sans valeur juridique. Le Message va inopportunément loin par rapport au texte légal tel qu'adopté.

2. *La renonciation à la prescription*

La pratique a développé, et depuis fort longtemps[26], la figure juridique essentielle de la renonciation à la prescription. Le débiteur peut se mettre à l'abri des poursuites du créancier destinées à interrompre la prescription (art. 135 ch. 2 CO) en renonçant à la protection que constitue pour lui l'exception de prescription. La renonciation, commode pour les deux parties, est restée juridiquement incertaine pendant des années, d'une part, en raison

---

24 Selon le nouveau texte, la prescription ne court pas ou est suspendue « pendant les discussions en vue d'une transaction, pendant une médiation ou pendant toute autre procédure extrajudiciaire visant la résolution d'un litige, si les parties en sont convenues par écrit ».

25 Message, Droit de la prescription (2013), p. 245.

26 L'ATF 112 (2006) II 231, 233 c. 3e.bb, constatait, en 1986 déjà, que « la renonciation à la prescription a pris une grande extension dans la pratique, notamment dans les relations avec les compagnies d'assurance » ; constatation rappelée dans l'ATF 132 (2006) III 226 c. 3.3.2 (cf. n. 24).

de l'art. 129 CO qui interdit de modifier les délais de prescription du titre 3e sur l'extinction des obligations, d'autre part, en raison de l'art. 141 al. 1 CO qui statue la nullité d'une renonciation anticipée à la prescription. Un arrêt fondamental de 2006[27] avait amélioré la sécurité juridique en admettant la possibilité de renoncer à l'exception de prescription une fois que le délai a commencé à courir, de même que lorsqu'il est échu, quelle que soit la durée du délai envisagée.

L'art. 141 CO a été modifié, tant dans sa note marginale que dans son texte (sous réserve des alinéas 2 et 3 qui ont été conservés tels quels), pour tenir compte de cette pratique ainsi que de la décision susmentionnée :

Art. 141 VII. Renonciation à soulever l'exception de prescription

1 Le débiteur peut renoncer à soulever l'exception de prescription, à chaque fois pour dix ans au plus, à compter du début du délai de prescription.

1bis La renonciation s'effectue par écrit. Seul l'utilisateur des conditions générales peut renoncer dans celles-ci à soulever l'exception de prescription.

[2 La renonciation faite par l'un des codébiteurs solidaires n'est pas opposable aux autres.]

[3 Il en est de même si elle émane de l'un des codébiteurs d'une dette indivisible ; et la renonciation faite par le débiteur principal n'est pas non plus opposable à la caution.]

4 La renonciation faite par le débiteur est opposable à l'assureur et inversement, s'il existe un droit d'action direct contre ce dernier.

Les nouveaux alinéas appellent plusieurs observations.

- S'écartant de l'actuelle nullité de la renonciation à la prescription (art. 141 al. 1 CO), l'art. 141 al. 1 nCO permet au débiteur de renoncer à soulever l'**exception** de prescription, ce qui relève strictement de l'exercice de l'autonomie privée du débiteur et ne peut qu'être salué. Cette renonciation ne porte que sur la prescription qui a déjà commencé à courir ou est acquise, selon la décision de 2006 mentionnée ci-dessus[28]. Il ne s'ensuit donc pas que les délais eux-mêmes, voire leur durée, auraient été modifiés. L'actuel art. 129 CO excluant toute modification conventionnelle des « délais de prescription fixés dans le présent titre » reste en vigueur tel quel. On peut, malgré tout, regretter le maintien de cette limite au « présent titre » dont la raison d'être est loin d'être évidente : les délais du titre IIIe sont principalement en relation avec les obligations contractuelles par opposition aux autres délais, comme ceux des art. 60 ou 67 CO visant les obligations fondées sur un acte illicite ou

27 ATF 132 (2006) III 226 c. 3.3.7. L'arrêt a été abondamment commenté, notamment par PICHONNAZ (2006), p. 118, qui l'approuve, et GAUCH, p. 561 ss, qui le critique.

28 Message, Droit de la prescription (2013), p. 246 (cf. n. 27).

sur un enrichissement illégitime. On pourra donc modifier les délais des prétentions dont le fondement est étranger à la volonté des parties, justifiées par un acte illicite ou un déplacement patrimonial indu, alors que cela continuera de n'être pas permis s'agissant d'obligations fondées sur la volonté des parties. Même si le résultat n'est pas satisfaisant, il faudra s'en contenter pour l'avenir.

- Le Tribunal fédéral[29] traitait la renonciation à la prescription comme un cas d'interruption semblable aux cas visés par l'art. 135 CO, dont l'effet est de faire courir un nouveau délai de même durée. Vingt ans plus tard, l'arrêt fondamental déjà mentionné[30] privilégie l'autonomie des parties dans ce domaine (art. 19 CO)[31], tout en se montrant sensible aux critiques de Koller[32]. Le Tribunal fédéral semble ainsi – mais ce n'est qu'implicite – revenir sur sa jurisprudence antérieure. Dans le sens de ce revirement implicite, le législateur a choisi de ne pas ajouter un nouveau cas à l'art. 135 CO, à côté de la reconnaissance de la dette par le débiteur (art. 135 ch. 1 CO, inchangé). C'est un choix qu'il convient de saluer tant aurait été délicate la limite entre la reconnaissance de dette par le débiteur et la renonciation à soulever l'exception de prescription.
- Selon le nouveau droit, la conséquence de la renonciation n'est donc pas de faire courir un nouveau délai de même durée, mais de laisser la question à l'autonomie des parties, plus précisément au choix du débiteur qui peut renoncer à l'exception de prescription pour dix ans au plus[33]. La renonciation peut être renouvelée par période de dix ans au plus (art. 141 al. 1 nCO), ce qui, selon le Message, « constitue le pendant des actes interruptifs du créancier, qui peuvent également être répétés un nombre illimité de fois »[34]. Le législateur a renoncé à poser une règle par défaut pour le cas où aucun délai ne serait indiqué dans la renonciation du débiteur, considérant que la question devait être résolue par interprétation, au besoin comblement d'une lacune de la manifestation de volonté du débiteur[35]. On peut regretter ce choix. L'avant-projet de 2011 comportait la règle suivante à l'art. 134 al. 1 P-CO : « S'il [le débiteur] n'indique pas de délai, la renonciation est valable pour un an ». Une telle règle par défaut aurait amélioré la

---

29 ATF 112 (1986) II 231 c. 3e.bb, p. 233-234 : « La renonciation équivaut donc à une interruption, et un nouveau délai – de 10 ans selon l'art. 60 CO, en l'espèce – commence à courir à partir du moment où elle est formulée (…) ».

30 ATF 132 (2006) III 226 c. 3.3.2 ss, 3.3.8.

31 CR CO I-PICHONNAZ, CO 135 N 10e, considérait déjà que la « renonciation à la prescription n'est pas un acte interruptif de prescription, bien qu'un nouveau délai coure dès la renonciation ».

32 KOLLER, *passim*.

33 Cf. déjà ATF 132 (2006) III 226 c. 3.3.8.

34 Message, Droit de la prescription (2013), p. 247.

35 *Ibid*.

sécurité juridique pour le cas où, même après interprétation, la renonciation du débiteur ne comporte aucun délai. Face à une renonciation sans délai, le créancier a besoin de savoir à partir de quand il doit agir contre le débiteur, ou alors obtenir une nouvelle renonciation de la part de ce dernier.

- En revanche, la question du début de validité de la renonciation est désormais fixée au « début du délai de prescription » par l'art. 141 al. 1 nCO. Elle avait été laissée ouverte dans l'avant-projet de 2011[36]. La clarification est bienvenue.
- Sur le plan méthodologique, la jurisprudence s'était tout d'abord fondée sur l'abus de droit, opposé avec succès au débiteur qui invoque la prescription après y avoir renoncé[37]. Comme souvent, l'origine du raisonnement, perdue de vue par la suite, finit par une codification de la jurisprudence. Ce qui démontre, une fois de plus, le formidable laboratoire d'idées conduisant à un développement du droit que constitue l'abus de droit (art. 2 al. 2 CC).
- L'article 141 al. 1bis nCO pose l'exigence de la forme écrite (art. 13 CO), c'est-à-dire celle d'une signature écrite, en principe à la main, par celui qui renonce à l'exception de la prescription[38]. Cette exigence de forme est posée tant dans l'intérêt de la sécurité juridique que pour des questions de preuve[39]. La renonciation à invoquer la prescription sera donc nulle s'il manque la signature écrite à la main du renonçant (art. 11 al. 2 et 14 al. 1 CO). Une renonciation envoyée par courrier électronique n'y suffira pas.
- La même disposition envisage que la renonciation à l'exception puisse être prévue par des conditions générales. Dans cette hypothèse, la renonciation ne vaudra que pour l'« utilisateur » (« *Verwender* ») des conditions générales[40]. Cela signifie que seule la compagnie d'assurance utilisatrice des conditions générales, qui les soumet à l'assuré, pourra renoncer à l'exception de prescription dans le respect de la forme écrite, mais non l'autre partie, soit le consommateur assuré. Le Message relève

36 Le Message, Droit de la prescription (2013), p. 247, y consacre un paragraphe devenu sans objet.

37 CR CC I-CHAPPUIS, CC 2 N 44 n. 171.

38 Art. 13 al. 1 et 14 al. 1 CO.

39 Message, Droit de la prescription (2013), p. 247.

40 L'expression trouve son origine à l'art. 8 LCD (modifié le 16.6.2011, RO 2011 4909, FF 2009 5539) : « Utilisation de conditions commerciales abusives. Agit de façon déloyale celui qui, notamment, *utilise* des conditions générales qui, en contradiction avec les règles de la bonne foi prévoient, au détriment du consommateur, une disproportion notable et injustifiée entre les droits et les obligations découlant du contrat » (caractère italique ajouté). En allemand : « Verwendung missbräuchlicher Geschäftsbedingungen. Unlauter handelt insbesondere, wer allgemeine Geschäftsbedingungen *verwendet*, die in Treu und Glauben verletzender Weise zum Nachteil der Konsumentinnen und Konsumenten ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den vertraglichen Rechten und den vertraglichen Pflichten vorsehen » (caractère italique ajouté).

que la portée pratique de la protection est limitée puisqu'il n'est possible de renoncer à l'exception qu'une fois que le délai a commencé à courir, c'est-à-dire après le moment où les conditions générales sont acceptées[41], donc généralement pas sur la base de celles-ci. Il n'en demeure pas moins que l'attention est attirée sur le phénomène, courant en pratique dans ce domaine, des conditions générales dont le contrôle potentiel par le biais de l'art. 8 LCD nouveau ne doit pas être sous-estimé.

3. *Autres règles nouvelles ou modifiées*

A signaler encore deux dispositions qui joueront un rôle capital dans les litiges de responsabilité civile.

Effets de l'interruption envers les coobligés. L'art. 136 CO continue de viser les « effets de l'interruption envers des coobligés » selon son titre marginal inchangé[42]. L'alinéa 1er est enrichi d'une précision bienvenue : « si l'interruption découle d'un acte du créancier ». L'interruption ne produit effet contre les autres débiteurs solidaires (ou d'une dette indivisible) que si le créancier a fait valoir ses droits (art. 135 ch. 2 CO). L'acte du débiteur qui reconnaît la dette (art. 135 ch. 1 CO) ne suffit donc pas pour interrompre la prescription à l'égard les autres débiteurs solidaires. Le même ajout vaut pour le débiteur principal et la caution (art. 136 al. 2 nCO). L'alinéa 3 n'a pas été modifié. Un alinéa 4 nouveau précise les relations avec l'assureur. Il prévoit que l'interruption contre l'assureur vaudra aussi contre le responsable et inversement pour autant qu'il existe un droit d'action direct contre l'assureur. Il s'agit de la généralisation d'une règle existant en matière de circulation routière (art. 83 al. 2 LCR)[43], qui avait déjà été proposée par l'avant-projet de révision du droit de la responsabilité civile de 1999[44]. Il est heureux que le législateur ait intégré dans les règles générales sur la prescription cette règle clarifiant la situation juridique des assurés en matière d'assurances RC obligatoires.

Prescription de l'action récursoire. Le nouvel art. 139 nCO introduit une règle jusqu'ici manquante, celle de la prescription de l'action récursoire, qu'il fixe à trois ans à compter du jour où le codébiteur a indemnisé au-delà de sa part et connaît le codébiteur[45]. Cette règle ne figurait pas dans le projet soumis à

---

41 Message, Droit de la prescription (2013), p. 247.

42 La disposition ne vise que la solidarité parfaite : Message, Droit de la prescription (2013), p. 245 et réf. cit. n. 87.

43 Aussi prévue par l'art. 39 al. 2 LITC ; cf. Message, Droit de la prescription (2013), p. 246.

44 Art. 55b de l'avant-projet : <https://www.bj.admin.ch/bj/fr/home/wirtschaft/gesetzgebung/archiv/haftplicht.html> (consulté le 12.2.19).

45 L'avant-projet de 1999 contenait déjà un délai de prescription de trois ans (art. 55c).

consultation. Elle est en ligne avec le nouveau délai de l'action pour cause d'enrichissement illégitime (art. 67 al. 1 nCO). A nouveau, la précision est bienvenue. La règle n'était pas nécessaire dans le premier projet qui avait complètement modifié l'art. 127 CO, mais a été abandonné entretemps.

C. Appréciation de la réforme

Le communiqué du Conseil fédéral annonçant l'entrée en vigueur du nouveau droit de la prescription dès le 1er janvier 2020[46] met un terme à la saga de la révision totale du droit de la responsabilité civile transformée en une révision du droit de la prescription. Le nouveau droit mérite d'être salué, car il modifie l'un des pires chapitres du CO actuel en levant les incertitudes, et en tenant compte de bon nombre des critiques adressées au texte actuel.

Toutefois, le communiqué lui-même est contestable sur deux points : il donne l'impression que les victimes de dommages corporels différés seront désormais mieux protégées[47], et laisse entendre que la jurisprudence de la CourEDH sera respectée[48]. Sur le premier point, l'allongement du délai absolu de l'art. 60 al. 1bis CO de dix à vingt ans à compter du jour où le fait dommageable s'est produit ou a cessé continue de laisser sans protection les victimes de l'amiante ou d'un dommage corporel différé de plus de vingt ans. Pour des maladies, comme celles liées à l'amiante dont la période de latence se situe entre quinze et quarante-cinq ans après le début de l'exposition, un tel rallongement de la prescription est insuffisant. Sur le second point, le communiqué est encore plus trompeur. Dans son arrêt de 2014, la CourEDH, « constate que les prétentions des victimes de l'amiante, qui ont été exposées à cette substance jusqu'à son interdiction générale en Suisse, en 1989, sont toutes périmées ou prescrites au regard du droit en vigueur. **Elle observe également que le projet de révision du droit de la prescription suisse ne prévoit aucune solution équitable** – ne serait-ce qu'à titre transitoire, sous la forme d'un « délai de grâce » – au problème posé »[49]. Au moment où le projet examiné par la CourEDH comportait encore un délai absolu de trente ans, « aucune solution équitable » n'en découlait. Avec un délai absolu porté à « seulement » vingt ans, les dommages corporels différés, qu'ils soient dus à une exposition à

46 https://www.bj.admin.ch/bj/fr/home/aktuell/news/2018/ref_2018-11-07.html (consulté le 3.3.19).

47 « … le délai de prescription absolu sera de vingt ans en cas de dommage corporel. La prescription ne sera ainsi plus l'écueil qu'elle est aujourd'hui pour les victimes de dommages différés. » (*ibidem*).

48 « Le point de départ de cette amélioration est la motion 07.3763 "Délais de prescription en matière de responsabilité civile", qui se référait tout particulièrement aux victimes de l'amiante, dont les prétentions, selon le droit en vigueur, sont généralement prescrites avant même que se manifeste une pathologie éventuelle. Dans un arrêt de 2014 concernant une victime de l'amiante, la Cour européenne des droits de l'homme avait aussi jugé trop court le délai actuel de dix ans. » (*ibidem*).

49 Arrêt de la CourEDH, 11 mars 2014, affaire *Howald Moor et autres c. Suisse*, requête n° 52067/10 et 41072/11, par. 75, JdT 2014 II 165 (caractère gras ajouté).

l'amiante ou à une autre substance du même ordre, ne trouveront *a fortiori* pas de solution équitable pour les victimes. La jurisprudence de la CourEDH – qu'on l'approuve ou non – n'est toujours pas respectée.

Le communiqué obscurcit en réalité la situation juridique. Des propositions fondées sur le droit actuel permettraient de résoudre les cas de dommages corporels différés bien mieux qu'un allongement du délai à 20 ou 30 ans. Corinne Widmer Lüchinger[50] proposait en 2014 deux solutions parfaitement raisonnables fondées sur le droit actuel. Considérant que le problème tient moins à la durée qu'au point de départ de la prescription, elle proposait, d'une part, de fixer le point de départ de la prescription à l'apparition de la maladie, donc à la naissance de la créance en dommages-intérêts, et d'autre part d'appliquer l'art. 134 al. 1 ch. 6 CO à cette situation dans laquelle il est objectivement impossible de faire valoir la créance devant un tribunal suisse, ce qui aurait pour effet que la prescription serait suspendue jusqu'à l'apparition de la maladie. Le législateur n'a pas saisi la possibilité de modifier le *dies a quo* qu'il a maintenu au jour où le fait dommageable s'est produit ou a cessé (art. 60 al. 1 nCO). Rien n'empêche toutefois d'appliquer le cas d'empêchement de la prescription prévu par l'art. 134 ch. 6 CO à un cas où « il est scientifiquement prouvé qu'une personne est dans l'impossibilité de savoir qu'elle souffre d'une certaine maladie » comme le préconisait la CourEDH[51]. La prise en compte d'une telle circonstance pour le calcul du délai de péremption ou de prescription pourrait empêcher une autre condamnation de la Suisse dans un cas où une maladie professionnelle apparaîtrait alors que la prescription est déjà acquise. Il faudra, le cas échéant, y songer nonobstant la jurisprudence actuelle.

Pour en revenir au communiqué, doublement trompeur, il aurait mieux valu reconnaître ouvertement que la solution de problèmes tels que ceux posés par l'amiante ne passe exclusivement ni par les règles de la responsabilité civile ni par celles de la prescription. En tout cas la prolongation du délai de dix à vingt ans ne résout rien – ou presque – s'agissant de l'amiante et des dommages corporels différés en général. Si l'on considère que, à l'heure actuelle déjà, des solutions auraient pu être trouvées sur la base d'une interprétation novatrice des textes existants, l'enthousiasme pour cette révision nécessaire du droit de la prescription retombe quelque peu.

---

50 WIDMER LÜCHINGER, p. 472, considérait, alors que la prescription pour les dommages corporels était encore proposée à 30 ans, que le projet « präsentiert sich […] letztlich als **völlig untauglicher Versuch**, die Ansprüche von Asbestopfern zum Durchbruch zu verhelfen » (caractère gras ajouté).

51 Arrêt de la CourEDH, 11 mars 2014, affaire *Howald Moor et autres c. Suisse*, requête n° 52067/10 et 41072/11, par. 78, JdT 2014 II 165.

III. La remise du gain suite à une campagne médiatique attentatoire à l'honneur

Apparemment moins brûlant, le thème de la remise du gain est de première importance pour le système général des prétentions compensatoires. Il est au centre de deux affaires, l'une récente, l'autre moins, qui méritent quelques lignes.

A. Deux affaires à considérer

La remise du gain est au centre de l'affaire *Tamedia & Espace Media* qui a échauffé les esprits en 2017[52]. Le demandeur avait fait l'objet d'une campagne attentatoire à l'honneur de la part d'une série d'organes de presse (*Medienhype*). Il demandait à *Tamedia AG* et *Espace Media AG*, la remise du gain réalisé par ces entreprises grâce à ladite campagne médiatique, ainsi que les informations nécessaires au calcul du gain, et, enfin, une indemnité pour tort moral. Deux passages au Tribunal fédéral plus tard, l'affaire est de nouveau devant les juges zurichois pour décision dans le sens des considérants. Même si elle a déjà fait l'objet de nombreux commentaires[53], elle mérite une analyse qui va au-delà du domaine du droit de la personnalité, le premier dans lequel pareille clarification de la prétention en remise du gain est intervenue. Il convient également d'attirer l'attention des francophones sur une décision d'une longueur peu usuelle en droit privé, et qui n'est pas traduite.

La décision *Tamedia & Espace Media* se réfère à une autre affaire qui avait déjà opposé les juges zurichois au Tribunal fédéral sur des questions similaires en 2006 : l'affaire *Schnyder* contre *Ringier AG* et *Kraushaar*[54]. La remise du gain réalisé par *Ringier AG* avait été ordonnée au père de la joueuse de tennis *Patty Schnyder* pour divers articles attentatoires à l'honneur parus dans le *Sonntagsblick*. Le Tribunal fédéral avait condamné *Ringier* à la remise du gain sur la base de l'art. 423 CO, par renvoi de l'art. 28a al. 3 CC, et retourné l'affaire à l'instance cantonale sur le calcul du gain.

Les deux affaires présentent plusieurs points communs. D'abord, toutes deux ont défrayé la chronique et conduit à des articles de presse attentatoires à la personnalité des victimes. La presse a fait ses choux gras des déboires

---

52 ATF 143 (2017) III 297, *A. et B. AG contre Tamedia AG et Espace Media AG*, 9 juin 2017 ; fait suite à une première décision non publiée du TF : 5A_658/2014 du 6 mai 2015. Le nom de la victime, *Carl Hirschmann*, est mentionné dans un commentaire de PICHONNAZ (RSJ 2018), p. 192.

53 AEBI-MÜLLER, p. 399 ss ; CHAPPUIS (2018), p. 153 s. ; HRUBESCH-MILLAUER/FUHRER, p. 648 s. ; LING, p. 104 s. ; PICHONNAZ (RSJ 2018), p. 192 ; SCHMID/BUSSMANN, p. 787 ss.

54 ATF 133 (2006) III 153. Commentaires : WERRO (2008) ; CHAPPUIS (2008).

amoureux de la joueuse de tennis *Patty Schnyder*[55] avec ses amants, l'un entraîneur et l'autre détective, de ses démêlés avec son père (demandeur), comme de ses victoires et défaites en tennis de haute compétition. Quant à *Carl Hirschmann*, présenté comme un playboy richissime, acteur des chaudes nuits zurichoises, il est interpellé un matin de 2010 à l'hôtel Dolder à Zurich, où il réside, suite à deux plaintes pour contrainte sexuelle et acte sexuel avec une mineure[56]. Là encore, tous les ingrédients d'un bon scandale sont donnés (luxe, sexe et notoriété). Les deux personnages sont devenus des cibles de choix de la presse (sérieuse, comme à scandales)[57].

Ensuite, les deux affaires ont opposé les autorités judiciaires zurichoises au Tribunal fédéral sur la question de la remise du gain réalisé par des organes de presse (*Ringier AG* et *Krausharr* – auteur de l'article – pour la première affaire, *Tamedia AG* et *Espace Media AG* pour la seconde) au moyen de publications attentatoires à l'honneur. C'est la question qui nous intéresse ici. Dans ces affaires[58], les autorités zurichoises refusent de donner droit à la prétention en remise du gain élevée par les victimes (art. 28a al. 3 CC et art. 423 CO). Le Tribunal fédéral a renvoyé les deux cas aux autorités zurichoises pour nouvelle décision sur la remise du gain qui avait été refusée à tort.

Et, pour finir, dans les deux cas, le litige se termine par un arrangement entre les parties[59]. De là à en déduire que les organes de presse ne veulent surtout pas d'une décision de justice sur la remise du gain, il n'y a qu'un pas. Quoi qu'il en soit, le calcul concret de la remise du gain en matière d'atteintes à la personnalité par la voie de la presse sur la base de l'art. 42 al. 2 CO restera dans l'ombre[60].

---

55 Voir l'état de fait de l'ATF 133 (2006) III 153 (A et B.).

56 RTS, 28 juin 2010, https://www.rts.ch/info/suisse/1736985-le-jet-setteur-carl-Tamedia & Espace Media-a-ete-arrete-a-zurich.html (consulté le 5.6.2019).

57 Sources « sérieuses » : NZZ ou RTS ; à scandales : 20 Minutes (cf. n. 59).

58 Dans l'ATF 143 (2017) III 297 c. 6.2, l'autorité cantonale avait nié l'existence d'une atteinte à la personnalité du fait de la campagne de presse subie par la victime, ce que corrige le Tribunal fédéral (c. 6.4-6.8) : « Im Ergebnis stellt das Bundesgericht fest, dass die Beschwerdegegnerinnen die Persönlichkeit des Beschwerdeführers widerrechtlich verletzt haben, indem sie ab 4. November 2009 im beschriebenen Sinn (E. 6.5 und 6.7.3) an einer eigentlichen Medienkampagne rund um die Verhaftung des Beschwerdeführers mitwirkten. Die Beschwerde ist in diesem Punkt gutzuheissen. Zur Prüfung der Frage, ob sich die Beschwerdegegnerinnen auch ab dem 9. September 2011 an einer persönlichkeitsverletzenden Medienkampagne gegen den Beschwerdeführer beteiligten, ist die Sache an die Vorinstanz zurückzuweisen » (c. 6.8, p. 316-317).

59 Pour l'affaire *Tamedia & Espace Media* : la NZZ du 23.5.2019, https://www.nzz.ch/feuilleton/medien/tamedia-entschuldigt-sich-bei-carl-hirschmann-ld.1484089 (2.6.2019), fait état des excuses de *Tamedia* publiées dans 20 Minutes le 23 mai 2019 en français [https://www.20min.ch/people/schweiz/story/Tamedia-s-excuse-aupres-de-Carl-Hirschmann-17450566 (consulté le 2.6.2019)] et en allemand. Pour l'affaire *Schnyder*, la NZZ du 26.4.2007 rapporte que le litige s'est également terminé par un arrangement entre les parties [https://www.nzz.ch/newzzF0Z2UDYX-12-1.149482 (consulté le 2.6.2019)].

60 Pour un exemple de calcul du gain en matière de brevets, voir ATF 134 (2008) III 306 c. 4, JdT 2008 I 386.

B. Quelles leçons pour la remise du gain ?

L'on ne reviendra pas sur la condition première de la remise du gain, l'acte d'immixtion dans les affaires du maître, qui est admise lorsqu'une atteinte aux droits de la personnalité est réalisée[61]. Le renvoi de l'art. 28a al. 3 CC permet à la victime de l'atteinte d'obtenir la remise du gain selon les règles sur la gestion d'affaires (art. 423 CO) et de s'en prendre à l'accroissement du patrimoine de l'auteur de l'acte (gain) sans être limitée par la diminution du sien propre (dommage). La portée du renvoi de l'art. 28a al. 3 CC qui « réserve » les actions en dommages-intérêts et en réparation du tort moral, ainsi que la remise du gain selon les dispositions sur la gestion d'affaires, ne pose plus problème dans l'affaire *Tamedia & Espace Media*[62]. Une fois l'atteinte à la personnalité admise, le moyen de la remise du gain est ouvert. Reste alors à déterminer quel est concrètement le gain qui fait l'objet de l'obligation de remise, une question largement débattue dans les deux arrêts.

L'une des critiques adressées à l'arrêt *Schnyder* était que cette décision revenait à accorder une « remise du gain sans gain »[63]. Le Tribunal fédéral avait commencé par rappeler que le thème de la preuve d'une prétention en remise du gain fondée sur les art. 423 al. 1 CO et 28a al. 3 CC était une atteinte illicite à la personnalité, la réalisation d'un gain et un lien de causalité entre ces deux éléments. Puis, il avait précisé qu'un degré de vraisemblance prépondérante suffisait pour la causalité. Quant au gain, l'art. 42 al. 2 CO (par analogie) permettait au tribunal de le déterminer équitablement lorsque son montant ne pouvait pas strictement être prouvé. Le Tribunal fédéral avait encore relevé que des exigences trop strictes de preuve ne devaient pas rendre illusoires les prétentions auxquelles renvoie l'art. 28a al. 3 CC[64]. Toutes constatations à approuver sans réserve.

La même année, l'arrêt de la cafetière[65], rendant responsable un fabricant à l'égard d'une consommatrice blessée par l'explosion du produit défectueux, montrait une approche semblablement généreuse de la preuve du défaut. La preuve du défaut n'est pas moins délicate que celle du gain, mais ne bénéficie pas de l'aide de l'art. 42 al. 2 CO. Son traitement est fluctuant puisque, dans l'arrêt de la prothèse de hanche[66], le Tribunal fédéral en est revenu à une application plus stricte des règles de preuve et a rejeté la demande. La prothèse de hanche dont le défaut était allégué ayant été jetée (tout comme la

---

61 Sur cette condition, cf. CR CO I-HERITIER LACHAT, CO 423 N 5 s., 12 ; BSK OR I-WEBER, OR 423 N 2, 5-6, 16 ; TERCIER/BIERI/CARRON, N 5397, 5404 ss.

62 Cf. CHAPPUIS (2008), p. 155, pour une analyse de cette condition dans l'arrêt *Schnyder*.

63 WERRO, p. 495 ss (et titre de la contribution).

64 ATF 133 (2006) III 153, 161-162, c. 3.3.

65 ATF 133 (2006) III 81.

66 ATF 137 (2011) III 226 c. 3.2.

cafetière quelques années auparavant), il n'avait pas été possible de la « verser » au dossier pour l'expertiser et apporter la preuve directe du défaut[67]. Une application stricte de la preuve dans ce deuxième cas exclut toute application de la LRFP. Abordés par le prisme de la preuve, deux cas de responsabilité du fait des produits, sont tranchés de manière diamétralement opposée selon la sévérité avec laquelle la preuve est examinée. Il en va de même de tous les cas de responsabilité civile, qu'il s'agisse d'une faute médicale[68] ou, de manière générale, des conditions de la responsabilité[69].

Dans l'affaire *Schnyder*, le Tribunal fédéral ne s'était pas laissé prendre au piège de telles exigences trop strictes de preuve[70]. On ne peut que saluer cette position, qui permet d'éviter que la remise du gain ne demeure un moyen illusoire de réparer les atteintes à la personnalité en dépit du renvoi de l'art. 28a al. 3 CC à l'art. 423 CO.

La décision *Tamedia & Espace Media* (2017) représente une ferme confirmation de l'affaire *Schnyder* (2006), sur les questions de la preuve et de l'allégation des faits pertinents. En effet, le problème de la preuve du gain réalisé grâce à la campagne de presse incriminée paraît sans issue, sauf à reconnaître au tribunal le droit de procéder à une détermination équitable du montant exact du gain en application par analogie de l'art. 42 al. 2 CO, aujourd'hui largement admise[71]. Comme le relèvent les juges fédéraux, la victime de l'atteinte à la personnalité, soit le maître en termes de gestion d'affaires sans mandat, ignore le montant du gain réalisé par l'autre partie et ce, sans aucune faute de sa part[72].

Toutefois, la preuve facilitée du gain sur la base de l'art. 42 al. 2 CO par analogie ne suffit pas pour que la victime obtienne gain de cause. C'est sans

---

67 « Dans le cas particulier, l'examen de la prothèse litigieuse aurait permis d'établir s'il y avait ou non défaut de fabrication, à savoir une erreur intervenue dans le processus de fabrication d'un produit en soi bien conçu (ATF 133 (2006) III 81 consid. 3.2 p. 85) ; selon toute probabilité, la lésée aurait alors été en mesure d'apporter une preuve stricte. Or, une telle démarche s'est révélée impossible parce que la recourante, respectivement le médecin qui a pratiqué l'intervention, n'ont pas conservé la prothèse retirée lors de l'opération du 9 avril 2002 ; la prothèse litigieuse n'a ainsi pas été produite dans la procédure du fait de la recourante. Toute possibilité de contre-preuve était pratiquement exclue pour l'intimée » (ATF 137 (2011) III 226, 232 c. 3.2).

68 Par ex., ATF 141 (2015) III 363 (déchirure périnéale). Critiques quant à la sévérité de cette décision pour la patiente incapable de satisfaire aux exigences ici posées quant à la preuve du défaut de diligence du médecin : WERRO/TOLOU, p. 386 ; KINZL, p. 133 : « […] keiner andern Berufsgruppe werden – soweit ersichtlich – derartig weitgehende Privilegien eingeräumt. Stattdessen erschwert das Bundesgericht nun die ohnehin schon schwierige Beweislage für den Patienten noch zusätzlich, sodass dieser die ihm auferlegte Beweislast kaum noch zu erfüllen vermag ».

69 Sur le thème de la preuve en responsabilité civile, voir les contributions publiées in CHAPPUIS Christine/WINIGER Bénédict, Journée de la responsabilité civile 2010, La preuve en droit de la responsabilité civile, Genève, etc. (Schulthess) 2011.

70 Cf. *supra*, n. 62.

71 CR CO I-HÉRITIER LACHAT, CO 423 N 22 et réf. cit ; ZK-SCHMIDT, CO 423 N 43 ; BSK OR I-WEBER, OR 423 N 15.

72 ATF 143 II 297, 324 s. c. 8.2.5.2.

doute la raison pour laquelle le demandeur dans l'affaire *Tamedia & Espace Media* a pris soin de formuler une requête en production de documents, elle aussi, rejetée par l'autorité cantonale comme n'étant pas assez précise[73]. L'arrêt cite les nombreux auteurs admettant une prétention en information et en reddition de comptes (fondée sur l'art. 2 al. 1 CC) et la possibilité pour la partie demanderesse de procéder par une action échelonnée selon l'art. 85 CPC (*Stufenklage*)[74]. Dans la mesure cependant où la partie demanderesse bénéficie de la possibilité de faire fixer le gain selon l'appréciation du tribunal en application par analogie de l'art. 42 al. 2 CO, l'obligation pour la partie demanderesse de chiffrer la demande une fois les preuves administrées ou les informations requises fournies par le défendeur n'est, selon l'arrêt, pas applicable (art. 85 al. 2 CPC)[75]. Cela ne signifie toutefois pas que la partie demanderesse ne puisse pas faire valoir sa prétention en information et en reddition de comptes, car l'action échelonnée prévue par l'art. 85 al. 2 CPC ne doit pas la restreindre dans ses possibilités d'agir en justice.

Le Tribunal fédéral poursuit son examen du raisonnement de l'autorité cantonale, auquel il reproche d'avoir confondu la prétention principale (remise du gain) et la prétention accessoire (information et reddition de comptes) du point de vue des exigences différenciées posées à l'allégation des faits pertinents[76], et d'avoir été exagérément strict sur le caractère suffisamment déterminé de l'action en information et reddition de comptes[77]. Les juges fédéraux[78] concluent que l'autorité cantonale doit commencer par clarifier quels sont les articles de presse contraires à la personnalité de la victime donnant lieu à remise du gain, et si les défenderesses en répondent de par leur participation à la campagne de presse incriminée ; cela fait, procédant en deux étapes, l'autorité cantonale doit examiner les prétentions en information et reddition de comptes servant de base à la prétention de fond en remise du gain ; en fonction du résultat de cette première étape, l'autorité cantonale devra, dans une seconde étape, examiner la prétention principale en remise du gain et procéder à l'appréciation de celui-ci en application par analogie de l'art. 42 al. 2 CO. L'affaire est renvoyée à l'autorité cantonale sur ces points.

Les étapes ainsi prescrites par le Tribunal fédéral peuvent servir de base à toute demande en remise du gain fondée sur l'art. 423 CO en matière d'atteintes à la personnalité, comme, *mutatis mutandis*, à toute demande en remise du gain.

---

73 ATF 143 (2017) III 297, 324 s. c. 8.1.

74 ATF 143 (2017) III 297, 322 ss c. 8.2.5.2.

75 ATF 143 (2017) III 297, 324 c. 8.2.5.2. Sur la relation entre ces deux moyens relevant l'un du droit de fond (art. 42 al. 2 CO) et l'autre du droit de procédure (art. 85 al. 2 CPC), voir PASQUIER, p. 238 s ; SCHÖBI, p. 455 s.

76 ATF 143 (2017) III 297, 325-327 c. 8.2.5.3.

77 ATF 143 (2017) III 297, 327-330 c. 8.2.5.4-5.

78 ATF 143 (2017) III 297, 330 c. 8.2.6.

C. Perspectives d'avenir et élargissements possibles

Les possibilités de réclamer la remise du gain, à côté de la réparation du dommage, sont larges, ainsi que la loi, la jurisprudence et la doctrine l'admettent aujourd'hui.

Les renvois légaux[79] à la « remise du gain selon les dispositions sur la gestion d'affaires » se sont multipliés depuis le premier renvoi introduit à l'art. 28a al. 3 CC en 1983 en matière d'atteintes à la personnalité. Le dernier renvoi en date est prévu par l'art. 20 al. 2 de la Loi sur la protection des armoiries (LPAP) du 21 juin 2013. Il est formulé ainsi : « Sont réservées les actions intentées en vertu du code des obligations qui tendent notamment au paiement de dommages-intérêts, à la réparation du tort moral ainsi qu'à la remise du gain selon les dispositions sur la gestion d'affaires. ». On observe que la formulation du renvoi à l'art. 423 CO est demeurée quasiment inchangée en 30 ans[80].

La jurisprudence a poursuivi son œuvre comme le démontrent les deux décisions examinées ici. À ce titre, on peut mentionner diverses autres décisions rendues en application de l'art. 423 CO. Une décision de 2000 rappelle le but de la remise du gain fondée sur l'art. 423 al. 1 CO, qui est d'empêcher qu'un acte illicite (ici, une violation du droit d'auteur) ne soit rentable, et règle la prescription de cette action selon les art. 60 et 67 CO[81]. La même année, le Tribunal fédéral examine le calcul du gain obtenu par la violation d'un brevet après soustraction des frais déductibles sur la base de l'art. 423 al. 2 CO[82]. Plus récemment, le Tribunal fédéral a admis qu'un fondé de procuration violant la prohibition de concurrence prévue à l'art. 464 al. 1 CO devait remettre au chef de la maison le gain ainsi réalisé[83].

La doctrine[84] a porté une attention constante à la remise du gain selon les règles sur la gestion d'affaires et systématisé la jurisprudence rendue sur le fondement de l'art. 423 CO, un fondement plutôt faible et mal placé dans la partie spéciale du CO après les règles sur le mandat. Bien qu'il subsiste quelques controverses sur la définition des actes donnant lieu à la remise du gain et sur l'exigence d'une condition subjective, la remise du gain trouve

---

79 Voir art. 28a al. 3 CC, art. 9 al. 3 LCD, art. 55 al. 2 LPM, art. 62 al. 2 LDA, art. 15 al. 1 LPD, art. 10 al. 1 LTo, art. 12 al. 1 lit. c Lcart, art. 35 al. 2 LDes, art. 20 al. 2 LPAP.

80 L'art. 20 al. 2 LPAP est entré en vigueur le 1er janvier 2017, en même temps que la dernière modification de la loi sur la protection des marques (LPM).

81 ATF 126 (2000) III 382, JdT 2000 I 520 (violation de l'ancienne LDA).

82 ATF 134 (2008) III 306, JdT 2008 I 386 : le gérant ne peut déduire que les frais servant exclusivement à la production de contrefaçon (renvoi de la cause à l'autorité inférieure).

83 ATF 137 (2011) III 607, et commentaire de SCHMID/RÜEGG approuvant cette décision.

84 Cf., parmi beaucoup, CHAPPUIS (2011), p. 144 ss ; CHAPPUIS (2002), p. 52 ss ; CR CO I-HÉRITIER LACHAT, CO 423 N 5 s., 11 ss ; BSK OR I-WEBER, CO 423 N 3 et 16 ; ZK-SCHMIDT, CO 423 N 13 ss, 21 ss ; SCHMIDT, Rechtsentwicklung, p. 426, 428 ss.

clairement sa place parmi les prétentions compensatoires, alors même que sa fonction n'est pas de réparer un dommage, mais d'éviter que l'usurpateur ne conserve le profit réalisé au moyen du patrimoine d'autrui. L'auteur de ces lignes avait d'ailleurs suggéré que le moment était venu de rapatrier le fondement de la remise du gain dans la partie générale du CO à l'occasion de la révision totale du droit de la responsabilité civile. Les temps étaient mûrs en 2002 déjà[85]. L'occasion a été manquée avec la renonciation définitive à ce projet de révision[86].

La jurisprudence, avec l'aide de la doctrine, doit donc poursuivre son œuvre créatrice fondée sur l'art. 1 al. 3 CC, en relation avec les difficultés de calcul du gain dans les diverses hypothèses envisageables. En effet, ce calcul pose toujours le même problème. La victime (c.-à-d., le maître) se trouve dans une difficulté de preuve (*Beweisnot*) évidente due au fait que les moyens de prouver le gain sont en mains du gérant d'affaires et non en celles du maître, victime des agissements du gérant d'affaires qui viole les droits de la personnalité, d'autres droits (absolus ou relatifs) du maître.

Prenant acte de ces développements législatifs, doctrinaux et jurisprudentiels, le projet CO 2020[87] a généralisé les principes développés ci-dessus en quatre dispositions fixant les conditions de la remise du gain et proposant des règles sur la preuve du gain (art. 69-72 CO 2020)[88] :

Art. 69 CO 2020 (I. Principe)

Celui qui s'immisce dans les intérêts juridiquement protégés d'autrui doit remettre tout ou partie du gain en résultant à l'ayant droit, à moins qu'il ne prouve qu'il ne savait ni n'aurait dû savoir qu'il s'immisçait dans les intérêts d'autrui.

Art. 70 CO 2020 (II. Calcul du gain, 1. Preuve)

1 Il incombe au demandeur de rendre vraisemblable la réalisation d'un gain.

2 Lorsque le montant exact du gain ne peut être établi, le tribunal l'évalue en considération du cours ordinaire des choses.

Art. 71 (2. Déductions)

Les frais d'acquisition du gain sont déduits, pour autant qu'ils soient raisonnables et susceptibles d'être prouvés.

---

85 CHAPPUIS (2002), titre de la contribution.

86 Cf. *supra*, n. 7.

87 Dirigé par Claire Huguenin et Reto Hilty, un groupe de professeures et de professeurs provenant de toutes les facultés de droit de Suisse, a procédé à un réexamen des art. 1 à 183 CO à la lumière de cent ans de développements en Suisse et en Europe. Ces travaux ont débouché sur une proposition d'un « Code des obligations suisse 2020, Projet relatif à une nouvelle partie générale » en 220 articles rédigés en allemand, français et italien, puis traduits en anglais (http://or2020.ch/, consulté le 21.6.19). Les articles sont suivis d'une indication des sources d'inspiration législatives (suisses, européennes et de droit uniforme) et d'un commentaire explicatif de la situation actuelle et de ses défauts, ainsi que de la règle proposée et de son but.

88 OR CO 2020-CHAPPUIS/DE WERRA, art. 69-72 OR 2020 et commentaires.

Art. 72 (III. Fixation de la remise)

1 Le tribunal fixe l'étendue de la remise en fonction de l'ensemble des circonstances.

2 Il examine en particulier si et dans quelle mesure :

a. la remise du gain est nécessaire pour assurer la protection des intérêts particuliers de l'ayant droit ;

b. celui qui a réalisé le gain l'a obtenu grâce à ses propres prestations.

Le projet CO 2020 propose ainsi le rapatriement de la remise du gain dans la partie générale au sein du chapitre intitulé « De l'enrichissement illégitime » en quelques dispositions limitées au strict nécessaire. Ces dispositions tranchent les questions controversées. La définition de l'acte d'immixtion est large, englobant la violation d'un droit absolu (droits de la personnalité, propriété, etc.) comme relatif (fondé sur un contrat), ainsi que les autres comportements interdits par l'ordre juridique (LCD, etc.)[89]. La faute est exigée, mais présumée[90]. La preuve du gain est facilitée[91]. Une déduction des frais d'acquisition du gain est permise dans certaines limites pour éviter que le demandeur ne puisse obtenir davantage que le résultat concret de l'acte d'immixtion[92]. Si le législateur suisse revenait sur son attitude attentiste et reprenait l'idée d'adapter (enfin) le CO aux besoins du 21e siècle, il y aurait là un modèle intéressant permettant de systématiser les développements de la doctrine et de la jurisprudence en relation avec la remise d'un gain obtenu au moyen d'une immixtion dans les intérêts juridiquement protégés d'autrui.

IV. Conclusion

La période sous revue s'est révélée riche en développements. D'une part, la révision du droit de la prescription a trouvé son épilogue et entrera en vigueur au 1er janvier 2020. D'autre part, la remise du gain – un moyen à ne plus ignorer désormais – a bénéficié d'une clarification salutaire quant aux exigences de preuve, qui ne doivent pas être sévères au point de rendre le moyen inopérant.

89 OR CO 2020-Chappuis/de Werra, art. 69 OR 2020 N 7.

90 OR CO 2020-Chappuis/de Werra, art. 69 OR 2020 N 9.

91 OR CO 2020-Chappuis/de Werra, art. 70 OR 2020 N 2.

92 OR CO 2020-Chappuis/de Werra, art. 71 OR 2020 N 2.

V. Ouvrages cités

AEBI-MÜLLER Regina E., Die privatrechtliche Rechtsprechung des Bundesgerichts im Jahr 2017, *in* RJB 2018 397 ss.

CHAPPUIS Christine, Droit de la responsabilité civile, Les *essentialia* 2018-2019 [recte: 2017-2018], in Fuhrer (édit.), Annales SGHVR 2018, Zurich, etc. (Schulthess) 2018, p. 145 ss (cité : 2018) ; La restitution des profits issus de la corruption : quels moyens en droit privé ? *in* Cassani Ursula (édit.), Lutte contre la corruption internationale : "the never ending story", Genève (Schulthess) 2011, p. 139 ss (cité : 2011) ; Violation contractuelle et remise du gain, *in* Mélanges en l'honneur de Pierre Tercier, Genève, etc. (Schulthess) 2008, p. 153 ss (cité : 2008) ; L'harmonisation internationale du droit des obligations, muse du législateur Suisse ? *in* Le législateur et le droit privé : Colloque en l'honneur du professeur Gilles Petitpierre (Chappuis/Foëx/Thévenoz, édit.), Genève, etc., (Schulthess) 2006, p. 177 ss (cité : 2006) ; La remise du gain : les temps sont mûrs, *in* Werro (édit.), Quelques questions fondamentales du droit de la responsabilité civile : actualités et perspectives, Berne (Stämpfli) 2002, p. 51 ss (cité : 2002).

CHAPPUIS Christine/DE WERRA Jacques, art. 64-72 CO 2020, *in* Huguenin/Hilty, Schweizer Obligationenrecht 2020, Entwurf für einen neuen allgemeinen Teil, Code des obligations suisse 2020, Projet relatif à une nouvelle partie générale, Zurich, etc. (Schulthess) 2013 (cité : OR CO 2020-Chappuis/de Werra).

CHAPPUIS Christine/WINIGER Bénédict, Journée de la responsabilité civile 2010, La preuve en droit de la responsabilité civile, Genève, etc. (Schulthess) 2011 (cité : Preuve 2011).

CONSEIL FÉDÉRAL, Message relatif à la modification du code des obligations (Droit de la prescription) du 29 novembre 2013, FF 2014 221 (cité : Droit de la prescription (2013)).

GAUCH Peter, Verjährungsverzicht : Ein Entscheid des Bundesgerichts (BGE 132 III 226) und was davon zu halten ist, *in* RSJ 102/2008 533 ss.

HÉRITIER LACHAT Anne, art. 419-424 CO, *in* Thévenoz/Werro (édit.), Commentaire romand, Code des obligations I, art. 1-529 CO, 2e éd., Bâle (Helbing) 2012 (cité : CR CO I-Héritier Lachat).

HONSELL/VOGT/WIEGAND (édit.), Basler Kommentar, Obligationenrecht I, Art. 1-529 CO, 6e éd., Bâle (Helbing) 2015 (cité : BSK OR I-Auteur).

HRUBESCH-MILLAUER Stephanie/FUHRER Olivia, Rechtsprechungspanorama Einleitungsartikel und Personenrecht, *in* PJA 2018 634 ss.

HUGUENIN Claire/HILTY Reto, Schweizer Obligationenrecht 2020, Entwurf für einen neuen allgemeinen Teil, Code des obligations suisse 2020, Projet

relatif à une nouvelle partie générale, Zurich, etc. (Schulthess) 2013 (cité : OR CO 2020-Auteur).

KINZL Stephan, BGE 141 III 363 und die neue Praxis zur ärztlichen Dokumentationspflicht, *in* REAS 2016 131 ss.

KOLLER Alfred, Die Tragweite eines zeitlich begrenzten Verjährungsverzichts, *in* RSJ 92/1996 369 ss.

LING Peter, Life Science Recht, 2/2018 102.

LOSER-KROGH Peter, Kritische Überlegungen zur Reform des privaten Haftpflichtrechts – Haftung aus Treu und Glauben, Verursachung und Verjährung, *in* RDS 102/2006, p. 127 ss.

PASQUIER Bruno, Die Schätzung nach gerichtlichem Ermessen – Kritik an Art. 42 Abs. 2 OR, *in* REAS 2015 235 ss.

PICHONNAZ Pascal, art. 127-142 CO, *in* Thévenoz/Werro (édit.), Commentaire romand, Code des obligations I, art. 1-529 CO, 2e éd., Bâle (Helbing) 2012 (cité : CR CO I-Pichonnaz) ; Le point sur la partie générale du droit des obligations, *in* RSJ 115/2019 248 ss (cité : RSJ 2019) ; Le point sur la partie générale du droit des obligations, *in* RSJ 114/2018 191 ss (cité : RSJ 2018) ; La prescription de l'action en dommages-intérêts : Un besoin de réforme, *in* Werro (édit.), Le temps dans la responsabilité civile, Berne (Stämpfli) 2007, p. 71 ss (cité : 2007) ; Du nouveau sur la renonciation à la prescription, *in* DC 2006 118 ss (cité : 2006).

SCHMID Jörg, Die Geschäftsführung ohne Auftrag, *in* Gauch/Schmidt (édit.), Die Rechtsentwicklung an der Schwelle zum 21. Jahrhundert, Symposium zum Schweizerischen Privatrecht, Zurich (Schulthess) 2001, p. 421 ss ; Kommentar zum Schweizerischen Zivilgesetzbuch, Die Geschäftsführung ohne Auftrag (Art. 419-424 OR), Zurich (Schulthess) 1993.

SCHMID Jörg/BUSSMANN Céline, Die privatrechtliche Rechtsprechung des Bundesgerichts im Jahr 2017 (2/2), *in* RJB 154/2018 764 ss.

SCHMID Jörg/RÜEGG Jonas, Die privatrechtliche Rechtsprechung des Bundesgerichts im Jahr 2011, *in* RJB 149/2013 492 ss.

SCHÖBI Christian, Art. 42 Abs. 2 OR : Substanziieren vs Schätzen – eine Annäherung an die Rechtsfigur der „perte d'une chance" ?, *in* Ohne jegliche Haftung, Festschrift für Willi Fischer zum 65. Geburtstag, Zurich, etc. (Schulthess) 2016, p. 447 ss.

TERCIER Pierre/BIERI Laurent/Carron Blaise, Les contrats spéciaux, 5e éd., Genève, etc. (Schulthess) 2016.

THÉVENOZ/WERRO (édit.), Commentaire romand, Code des obligations I, art. 1-529 CO, 2e éd., Bâle (Helbing) 2012 (cité : CR CO I-Auteur).

THOUVENIN Florent/PURTSCHERT Tina, Art. 148-162 OR 2020, *in* Huguenin/Hilty, Schweizer Obligationenrecht 2020, Entwurf für einen neuen allgemeinen Teil, Code des obligations suisse 2020, Projet relatif à une nouvelle partie générale, Zurich, etc. (Schulthess) 2013 (cité : OR CO 2020-Thouvenin/Purtschert).

WERRO Franz, Une remise du gain sans gain ?, *in* Mélanges en l'honneur de Pierre Tercier, Genève, etc. (Schulthess) 2008, p. 495 ss.

WERRO Franz/TOLOU Alborz, L'obligation de documenter du médecin, *in* REAS 2015 382 ss.

WIDMER LÜCHINGER Corinne, Die Verjährung bei Asbestschäden, *in* RJB 150/2014 460 ss.

Derniers ouvrages parus

Collection Genevoise

http://www.unige.ch/droit/CG.html

Droit de la responsabilité

Chappuis, Christine / Winiger, Bénédict (éds) *2019*
Responsabilité civile et nouvelles technologies
(Journée de la responsabilité civile 2018)

Chappuis, Christine / Winiger, Bénédict (éds) *2018*
La responsabilité du fait des produits
(Journée de la responsabilité civile 2016)

Chappuis, Christine / Winiger, Bénédict (éds) *2015*
Responsabilité civile – Responsabilité pénale
(Journée de la responsabilité civile 2014)

Chappuis, Christine / Winiger, Bénédict (éds) *2013*
Le tort moral en question
(Journée de la responsabilité civile 2012)

Chappuis, Christine / Winiger, Bénédict (éds) *2011*
La preuve en droit de la responsabilité civile
(Journée de la responsabilité civile 2010)

Chappuis, Christine / Winiger, Bénédict (éds) *2009*
La responsabilité pour l'information fournie à titre professionnel
(Journée de la responsabilité civile 2008)

Droit international

Graf-Brugère, Anne-Laurence *2019*
La « menace contre la paix » dans la pratique du Conseil de sécurité des Nations Unies – Réflexions sur un concept de droit international

Fardel, Mélissa *2019*
La participation des victimes aux procédures pénales internationales et les droits de l'accusé

Le Fort, Olivia *2018*
La preuve et le principe de non-refoulement
Entre droit international des réfugiés, protection des droits humains et droit suisse des migrations

Thalmann, Vanessa *2018*
Reasonable and effective universality
Conditions to the exercice by national courts of universal jurisdiction over international crimes

Sangbana, Komlan *2017*
La protection des eaux douces transfrontières contre la pollution : dimensions normatives et institutionnelles

Marquis, Julien *2017*
La qualité pour agir devant la Cour européenne des droits de l'homme

Riondel, Ghislaine *2016*
La prise en charge des soins de santé dans un contexte transfrontalier européen – Problématique générale en Europe et propositions pour la Région franco-valdo-genevoise

Rodriguez Ellwanger, Maria *2016*
Les instruments juridiques de la planification territoriale transfrontalière dans le bassin de vie franco-valdo-genevois

Herren, Pascal *2016*
L'intervention internationale au nom des droits de l'homme – L'autorité de l'approche finaliste

Christófolo, João Ernesto *2016*
Solving Antinomies Between Peremptory Norms in Public International Law

Carron, Djemila *2016*
L'acte déclencheur d'un conflit armé international

Sossou Biadja, Cassius Jean *2015*
L'acte uniforme OHADA relatif à l'arbitrage à l'épreuve des standards transnationaux de la justice arbitrale
Approche comparée de droit international privé

McGregor, Eleanor *2015*
L'arbitrage en droit public suisse
Une comparaison avec la France, les États-Unis et l'arbitrage d'investissement

Reymond, Michel *2015*
La compétence internationale en cas d'atteinte à la personnalité par Internet

de María Palaco Caballero, Flor *2015*
La Cour internationale de justice et la protection de l'individu

Romano, Gian Paolo *2014*
Le dilemme du renvoi en droit international privé
La thèse, l'antithèse et la recherche d'une synthèse

Granges, Mathieu *2014*
Les intérêts moratoires en arbitrage international

Grignon, Julia *2014*
L'applicabilité temporelle du droit international humanitaire

Bulak, Begüm *2014*
La liberté d'expression face à la présomption d'innocence
Justice et médias en droit italien et suisse à l'aune de la convention et de la jurisprudence de la cour européenne des droits de l'homme

Johannot-Gradis, Christiane *2013*
Le patrimoine culturel matériel et immatériel : quelle protection en cas de conflit armé ?

Chatton, Gregor T. *2013*
Vers la pleine reconnaissance des droits économiques, sociaux et culturels

Ludwiczka, Maria *2013*
La délégation internationale de la compétence pénale

Petry, Roswitha *2013*
La situation juridique des migrants sans statut légal
Entre droit international des droits de l'homme et droit suisse des migrations

Redalié, Lorenzo *2013*
La conduite des hostilités dans les conflicts armés asymétriques : un défi au droit humanitaire

Tran, Laurent *2013*
Le régime uniforme de responsabilité du transporteur aérien de personnes

Recueils de textes

Trigo Trindade, Rita / Bahar, Rashid / Neri-Castracane Giulia (éds) *2019*
Vers les sommets du droit
Liber amicorum pour Henry Peter

Hottelier, Michel / Hertig Randall, Maya / Flückiger, Alexandre (éds) *2019*
Études en l'honneur du Professeur Thierry Tanquerel
Entre droit constitutionnel et droit administratif : questions autour du droit de l'action publique

Bernard, Frédéric / McGregor, Eleanor / Vallée-Grisel, Diane (éds) *2017*
Études en l'honneur de Tristan Zimmermann
Constitution et religion
Les droits de l'homme en mémoire

Wyler, Rémy / Meier, Anne / Marchand, Sylvain (éds) *2015*
Regards croisés en droit du travail :
Liber Amicorum pour Gabriel Aubert

Bellanger, François / de Werra, Jacques (éds) *2012*
Genève au confluent du droit interne et du droit international
Mélanges offerts par la Faculté de droit de l'Université de Genève
à la Société Suisse des Juristes à l'occasion du Congrès 2012

Hottelier, Michel (éd.) *2011*
Albert Cohen
L'écrivain au service de l'Etat de droit
Actes du colloque organisé le 18 février 2011 par la Faculté de droit et la Fondation Mémoire Albert Cohen

Flückiger, Alexandre (éd.) *2010*
Emouvoir et persuader pour promouvoir le don d'organes ?
L'efficacité entre éthique et droit

Trigo Trindade, Rita / Peter, Henry / Bovet, Christian (éds) *2009*
Economie Environnement Ethique
De la responsabilité sociale et sociétale.
Liber amicorum Anne Petitpierre-Sauvain

Collection générale

Schmidt, Tanja *2019*
Les clauses pour solde de tout compte
Ou la renonciation définitive à se prévaloir de prétentions ultérieures

Liégeois, Fabien *2018*
La disponibilité du revenu : le moment de l'acquisition en droit fiscal suisse

Avramov, Philippe *2018*
L'omission fautive : la violation d'un devoir juridique ou moral.
Une analyse historique et dogmatique

Villard, Katia *2017*
La compétence du juge pénal suisse à l'égard de l'infraction reprochée à l'entreprise
Avec un regard particulier sur les groupes de sociétés

Jubin, Oriana *2017*
Les effets de l'union libre
Comparaison des différents modes de conjugalités et propositions normatives

Neri-Castracane, Giulia *2016*
Les règles de gouvernance d'entreprise comme moyen de promotion de la responsabilité sociale de l'entreprise – Réflexions sur le droit suisse dans une perspective internationale

Hohl-Chirazi, Catherine *2016*
La privation de liberté en procédure pénale suisse : but et limites

Dan, Adrian *2015*
Le délit de commission par omission – éléments de droit suisse et comparé

Mirfakhraei, Kaveh *2014*
Les indemnités de fin de contrat dans le contrat d'agence et le contrat de distribution exclusive

Sigrist, Alexandra *2013*
Les pouvoirs de la police : le cas de la délinquance juvénile

Pavlidis, Georgios *2012*
Confiscation internationale : instruments internationaux, droit de l'Union européenne, droit suisse

Rubido, José-Miguel *2012*
L'exercice du droit de préemption immobilier au regard du droit privé

Gonin, Luc *2011*
L'obsolescence de l'Etat moderne
Analyse diachronique et contextuelle à l'exemple de l'Etat français

Marti, Ursula *2011*
Das Vorsorgeprinzip im Umweltrecht
Am Beispiel der internationalen, europäischen und schweizerischen Rechtsordnung

Alberini, Adrien *2010*
Le transfert de technologie en droit communautaire de la concurrence
Mise en perspective avec les règles applicables aux accords de recherche et développement, de production et de distribution

Bernard, Frédéric *2010*
L'Etat de droit face au terrorisme

Donatiello, Giuseppe *2010*
Responsabilité du débiteur : de la délégation à l'organisation de l'exécution des obligations
Codifications supranationales récentes (CVIM, Principes d'UNIDROIT, Principes européens) et Code des obligations suisse

Droit de la propriété

Foëx, Bénédict / Hottelier, Michel (éds) *2018*
Imprescriptibilité, contrôle et responsabilité
Les effets du droit de propriété dans le temps

Foëx, Bénédict / Hottelier, Michel (éds) *2016*
La propriété immobilière face aux défis énergétiques
Du statut juridique de l'énergie au contrôle des loyers

Foëx, Bénédict (éd.) *2016*
La propriété par étages aujourd'hui
Une alerte cinquantenaire

Foëx, Bénédict (éd.) *2013*
Planification territoriale
Droit fédéral et spécificités cantonales

Foëx, Bénédict (éd.) *2012*
Les rénovations d'immeubles

Foëx, Bénédict (éd.) *2012*
La réforme des droits réels immobiliers
Les modifications du Code civil entrées en vigueur le 1er janvier 2012

Foëx, Bénédict (éd.) *2011*
Droit de superficie et leasing immobilier
Deux alternatives au transfert de propriété

Foëx, Bénédict / Hottelier, Michel *2009*
La garantie de la propriété à l'aube du XXIe siècle
Expropriation, responsabilité de l'Etat, gestion des grands projets et protection du patrimoine

Droit civil

Leuba, Audrey / Papaux van Delden, Marie-Laure (Foëx, Bénédict / (éds) *2017*
Le droit en question
Mélanges en l'honneur de la Professeure Margareta Baddeley

Geissbühler, Grégoire *2016*
Le recouvrement privé de créances
Aspects contractuels et protection du débiteur

Baddeley, Margareta / Foëx, Bénédict / Leuba, Audrey / Papaux van Delden, Marie-Laure (éds) *2014*
Facettes du droit de la personnalité
Journée de droit civil 2013 en l'honneur de la Professeure Dominique Manaï

Marchand, Sylvain *2012*
Droit de la consommation

Baddeley, Margareta / Foëx, Bénédict / Leuba, Audrey / Papaux Van Delden, Marie-Laure (éds) *2012*
Le droit civil dans le contexte international
Journée de droit civil 2011

Baddeley, Margareta / Foëx, Bénédict (éds) *2009*
La planification du patrimoine
Journée de droit civil 2008 en l'honneur du Professeur Andreas Bucher

Perrin, Jean-François / Chappuis, Christine *2008*
Droit de l'association
3e édition

Baddeley, Margareta (éd.) *2007*
La protection de la personne par le droit
Journée de droit civil 2006 en l'honneur du Professeur Martin Stettler

Droit et histoire

Mettral Dubois, Véronique *2015*
L'œuvre politique de James Fazy (1794-1878) et son apport à l'avènement des droits fondamentaux à Genève
Sources doctrinales et contexte historique

Dufour, Alfred / Quastana, François / Monnier, Victor (éds) *2013*
Rousseau, le droit et l'histoire des institutions
Actes du colloque international pour le tricentenaire de la naissance de Jean-Jacques Rousseau (1712-1778) organisé à Genève, les 12, 13 et 14 septembre 2012

Dufour, Alfred / Monnier, Victor (éds) *2011*
La Savoie, ses relations avec Genève et la Suisse
Actes des journées d'étude à l'occasion du 150e anniversaire de l'Annexion de la Savoie à la France organisées à Genève, les 4 et 5 novembre 2010

Schmidlin, Bruno *2011*
Der Vertrag im europäischen Zivilrecht / Le contrat en droit civil européen

Hottelier, Michel (éd.) *2010*
James Fazy
De l'intelligence collective des sociétés
Cours de législation constitutionnelle