

Le droit à l'intégrité numérique

Réelle innovation ou simple évolution du droit ?

Edité par Florence Guillaume et Pascal Mahon

LE DROIT A L'INTÉGRITÉ NUMÉRIQUE

LE DROIT A L'INTÉGRITÉ NUMÉRIQUE

Edité par
Florence Guillaume et Pascal Mahon

Faculté de droit de l'Université de Neuchâtel
Helbing Lichtenhahn



FACULTÉ DE DROIT

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>.

Tous droits réservés pour tous pays. L'œuvre et ses parties sont protégées par la loi. Toute utilisation en dehors des limites de la loi est strictement interdite et requiert l'accord préalable écrit des éditeurs.

ISBN 978-3-7190-4456-5

© 2021 Helbing Lichtenhahn, Bâle, Faculté de droit de l'Université de Neuchâtel, Neuchâtel

www.helbing.ch

www.unine.ch/droit

Préface

Cet ouvrage réunit les contributions écrites des intervenantes et intervenants au colloque qui s'est tenu à l'Université de Neuchâtel, en date du 21 février 2020, sur le thème « Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? ». L'idée de cette manifestation est née d'une discussion à bâtons rompus entre les deux organisateurs du colloque, soussignés, et Alexis Roussel, qui est un spécialiste reconnu de l'environnement numérique. Nous avons débattu longuement de la question de savoir si notre identité numérique doit ou peut être protégée de la même manière que notre personnalité en confrontant nos points de vue de constitutionnaliste et de civiliste aux préoccupations concrètes des utilisatrices et utilisateurs du numérique.

Cette discussion a suscité l'envie d'élargir le débat et d'examiner comment le droit à l'intégrité numérique pourrait être appréhendé dans sa globalité. C'est ainsi que nous avons réuni des spécialistes des principaux domaines du droit concernés pour analyser de façon transversale si la protection de l'intégrité physique et psychique peut être étendue à l'intégrité numérique, par une simple interprétation évolutive des normes juridiques existantes, ou s'il est nécessaire, au contraire, de créer de nouvelles règles de droit pour protéger les données numériques à caractère personnel. Si les personnalités invitées ont été surprises, dans un premier temps, par ce thème novateur, toutes ont accepté avec enthousiasme d'approfondir la réflexion dans leurs domaines de spécialité (droit civil, droit pénal, droit international privé, droit des médias, protection des données, droit constitutionnel et droit de la Convention européenne des droits de l'homme, notamment).

Le colloque a permis de dessiner les premiers contours des divergences existant entre les domaines du droit quand il s'agit d'appréhender la protection des données numériques. Dans certaines matières, le droit à l'intégrité numérique peut être protégé en procédant à une simple interprétation des règles existantes. En droit civil, par exemple, le droit à l'intégrité numérique peut être envisagé comme une simple extension du droit de la personnalité protégé par l'art. 28 CC. Dans d'autres matières, en revanche, la protection du droit à l'intégrité numérique ne peut exister sans base légale expresse. Tel est le cas en droit pénal en raison du principe de la légalité (*nulla poena sine lege*).

Les oratrices et orateurs ont pu affiner leur réflexion dans le cadre de la contribution écrite. Il ressort des textes, pris dans leur ensemble, une tendance à considérer que les données personnelles sont des éléments constitutifs de l'être humain ou de la personnalité. Sur cette base, une différence d'approche conceptuelle peut être constatée dans les disciplines où la protection du droit à l'intégrité numérique peut être considérée. Si certains auteurs estiment que le droit à l'intégrité numérique est un droit distinct du droit à l'intégrité physique et psychique, d'autres appréhendent la protection des données numériques à travers la protection de la personne elle-même. La première approche conceptuelle fait ressortir un besoin de protection propre du « moi numérique », lequel est envisagé comme une extension numérique de la personne s'épanouissant dans l'espace numérique, alors que la seconde rattache le « moi numérique » à l'esprit et au corps de l'individu, lesquels sont impactés, le cas échéant, dans le monde physique. Le débat entre les deux doctrines se situe donc fondamentalement au niveau de la reconnaissance de l'existence d'un ou de plusieurs espaces ou « moi » numériques distincts du monde physique. La question revient ainsi à se demander s'il est souhaitable ou nécessaire de différencier l'atteinte subie dans l'espace numérique de celle subie dans le monde physique.

Toutes et tous se rejoignent néanmoins sur un point : la protection du droit de chaque personne de contrôler et maîtriser ses propres données numériques et le traitement qui en est fait implique de déterminer préalablement ce que l'on veut – et peut – protéger. La difficulté consistant à identifier les données personnelles est, à ce titre, une entrave importante à leur protection. En outre, la dimension internationale de l'atteinte à l'intégrité numérique complique encore davantage l'intervention des législateurs nationaux et des tribunaux pour protéger les utilisatrices et utilisateurs du numérique.

A notre connaissance, il s'agit du premier ouvrage présentant une analyse transversale du droit à l'intégrité numérique. Au moment où les autorités publiques de différents niveaux envisagent ou adoptent une « stratégie numérique » ou un positionnement vis-à-vis du monde numérique, nous espérons que ces premiers éléments de réflexion juridique transversale pourront servir d'inspiration aux législateurs et autres instances normatives dans un contexte où les premiers signes d'un intérêt à introduire un droit à l'intégrité numérique dans le catalogue des droits

Préface

fondamentaux commencent à se manifester. En Suisse, le débat est déjà ouvert au niveau cantonal. Les Cantons du Valais et de Genève jouent un rôle précurseur à cet égard en ayant entamé des démarches et travaux législatifs en vue d'examiner l'opportunité d'inscrire le droit à l'intégrité numérique dans leur Constitution.

Florence Guillaume et Pascal Mahon
Neuchâtel, novembre 2020

Sommaire

ALEXIS ROUSSEL

Cofondateur de Bity, Neuchâtel

Le droit à l'intégrité numérique de la personne 1

JOHAN ROCHEL

Chercheur à l'Université de Zurich

L'intégrité numérique dans la Constitution :

Entre liberté et technologies numériques 13

PASCAL MAHON

Professeur à l'Université de Neuchâtel

Le droit à l'intégrité numérique : réelle innovation
ou simple évolution du droit ? Le point de vue du

droit constitutionnel 43

MARIE-LAURE PAPAUX VAN DELDEN

Professeure à l'Université de Genève

Le « droit à l'intégrité numérique » du point de vue de la

protection de droit civil de la personnalité 65

ANDRÉ KUHN

Professeur à l'Université de Neuchâtel

Le droit à l'intégrité numérique est-il une innovation ou une

extension de l'intégrité physique ? 87

Sommaire

JEAN-PHILIPPE WALTER

Commissaire à la protection des données du Conseil de l'Europe

L'intégrité numérique : une nécessité du point de vue du

droit à la protection des données ? 95

BERTIL COTTIER

Professeur associé à la Faculté de droit de l'Université de Lausanne

Professeur invité à l'Académie de journalisme de l'Université de
Neuchâtel

Membre de la Commission fédérale des médias

L'intégrité numérique : un obstacle au journalisme

d'investigation ? 103

FLORENCE GUILLAUME et SVEN RIVA

Professeure à l'Université de Neuchâtel

Assistant-doctorant à l'Université de Neuchâtel

L'atteinte à l'intégrité numérique appréhendée par le droit

international privé..... 117

Abréviations

ACEDH	Arrêt de le Cour européenne des droits de l'homme
ACJC	Arrêt de la Cour de justice du canton de Genève
AFAPDP	Association francophone des autorités de protection des données personnelles
Aff.	Affaire
Affaire phare	Liste des affaires phares de la Cour européenne des droits de l'homme recommandées par le Jurisconsulte et approuvées par le Bureau
al.	alinéa(s)
art.	article(s)
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
BSK	<i>Basler Kommentar</i>
c.	considérant(s)
c.	contre
CC	Code civil du 10 décembre 1907 (RS 210)
CE	Communauté européenne
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (RS 0.101)
CF	Conseil fédéral
cf.	<i>confer</i> (comparez)
ch.	chapitre
ch.	chiffre(s)

Abréviations

Charte	Charte des droits fondamentaux de l'Union Européenne
CJCE	Cour de justice des Communautés européennes
CJUE	Cour de justice de l'Union européenne
CL	Convention de Lugano concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale du 30 octobre 2007 (RS 0.275.12)
CO	Loi fédérale complétant le Code civil suisse (Livre cinquième : Droit des obligations) du 30 mars 1911 (RS 220)
cons.	considérant(s)
consid.	considérant(s)
Convention 108	Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (RS 0.235.1)
CourEDH	Cour européenne des droits de l'homme
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0)
CPC	Code de procédure civile suisse du 19 décembre 2008 (RS 272)
CR	Commentaire romand
Cst.	Constitution fédérale de la Confédération Suisse du 18 avril 1999 (RS 101)
Cst. féd.	Constitution fédérale de la Confédération Suisse du 18 avril 1999 (RS 101)
DAO	<i>Decentralized Autonomous Organization</i>
DUDH	Déclaration universelle des droits de l'homme du 10 décembre 1948

Abréviations

éd.	éditeur(s)
éd.	édition
édit.	éditeur(s)
et al.	<i>et alii</i> (et d'autres)
etc.	<i>et cetera</i> (et le reste)
ex.	exemple
FF	Feuille fédérale
GC	Grande chambre
ICIJ	<i>International Consortium of Investigative Journalism</i>
ICL Journal	Vienna Journal on International Constitutional Law
IA	Intelligence artificielle
i.e.	<i>id est</i> (c'est-à-dire)
JdT	Journal des Tribunaux
JOUE	Journal officiel de l'Union européenne
LDIP	Loi fédérale sur le droit international privé du 18 décembre 1987 (RS 291)
let.	lettre(s)
lit.	<i>littera</i> (lettre)
litt.	<i>littera</i> (lettre)
LPD	Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1)
LRH	Loi fédérale relative à la recherche sur l'être humain du 30 septembre 2011 (RS 810.30)
LS	Loi genevoise sur la santé du 7 avril 2006 (RS.GE K 1 03)

Abréviations

MM.	Messieurs
n.	note(s)
n°	numéro
no	numéro
N	numéro marginal
OCDE	Organisation de coopération et de développement économiques
ONU	Organisation des Nations unies
OSCE	Organisation pour la sécurité et la coopération en Europe
p.	page(s)
Pacte ONU II	Pacte international relatif aux droits civils et politiques du 16 décembre 1966 (RS. 0.103.2)
par.	paragraphe(s)
p.ex.	par exemple
PJA	Pratique Juridique Actuelle
PLR	Parti libéral-radical
pp.	pages
PS	Parti socialiste
RDS	Revue de droit suisse
Rec.	Recueil des arrêts et décisions de la Cour européenne des droits de l'homme
Rec.	Recueil de la jurisprudence de la Cour de justice de l'Union européenne
réf.	référence

Abréviations

RGPD	Règlement (UE) 2016/679 du Parlement et du Conseil, 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)
RO	Recueil officiel du droit fédéral
RS	Recueil systématique du droit fédéral
RS.GE	Recueil systématique genevois
s.	et suivant(e)
SJ	La Semaine judiciaire
SKMR	<i>Schweizerisches Kompetenzzentrum für Menschenrechte</i>
spéc.	spécialement
ss	(et) suivant(e)s
TF	Tribunal fédéral suisse
UE	Union européenne
Vol.	volume
ZGB	<i>Schweizerisches Zivilgesetzbuch</i> (= CC)

Le droit à l'intégrité numérique de la personne

par

Alexis Roussel

Cofondateur de Bity, Neuchâtel

I. Introduction.....	2
II. Un contexte politique et économique.....	2
III. A la recherche de nouveaux droits liés au numérique.....	3
IV. Le droit à la vie comme fondement.....	4
V. L'espace numérique, une nouvelle réalité immatérielle	5
VI. La reconnaissance de la vie numérique	6
VII. Les données, des éléments de notre personne.....	6
VIII. L'étendue insaisissable de notre existence numérique	8
IX. La mise en œuvre de la protection de l'intégrité numérique	8
X. Conclusion.....	10
Bibliographie	11

I. Introduction

1. Le concept de droit à l'intégrité numérique de la personne émerge depuis une dizaine d'années. Il entre en 2020 dans une phase plus active avec les premières propositions de mise en œuvre dans des ordres juridiques. L'introduction du droit à l'intégrité numérique est dorénavant envisagée au niveau de lois nationales et supranationales. Nous sommes d'avis que ce droit doit être intégré dans la Constitution fédérale de la Confédération suisse. En ajoutant le droit à l'intégrité numérique à celui de l'intégrité physique et mentale (ou psychique) au sein du droit à la vie, nous permettrions aux droits fondamentaux de faire leur transition tant attendue dans le numérique.

II. Un contexte politique et économique

2. Le procès du site Internet « the Pirate Bay », qui s'est déroulé en Suède en 2009, conservera une portée hautement symbolique dans l'Histoire de nos sociétés numériques. The Pirate Bay était le plus grand site de partage culturel de l'époque. Lorsque le juge demanda à son concepteur Peter Sunde¹, « vous vous rencontriez IRL ? » (In Real Life, Dans la Vraie Vie), celui-ci répondit : « Nous n'utilisons pas l'expression IRL. Nous disons AFK (Away From Keyboard, Loin du Clavier). Nous pensons qu'Internet est réel. » Peter Sunde voulait souligner la différence fondamentale de conception de ce qu'est le numérique. Pour le juge, à l'instar d'Angela Merkel et son « Neuland »², le numérique était un espace distinct de la vie. Si dès le début de l'ère d'Internet, les juristes se sont toujours mis d'accord qu'Internet n'est pas une zone de non-droit, il paraît bien moins évident que les droits humains s'y appliquent. Pour Peter Sunde,

¹ TPB AFK : The Pirate Bay Away From Keyboard, film documentaire de SIMON KLOSE 2013, https://www.youtube.com/watch?v=eTOKXCEwo_8, 9:40.

² « Das Internet ist für uns alle Neuland, und es ermöglicht auch Feinden und Gegnern unserer demokratischen Grundordnung natürlich, mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen », discours d'ANGELA MERKEL, la Chancelière fédérale de la République d'Allemagne, lors d'une conférence de presse avec Barack Obama, le Président des Etats-Unis, 19 juin 2013, <https://archiv.bundesregierung.de/archiv-de/dokumente/pressekonferenz-von-bundeskanzlerin-merkel-und-us-praesident-obama-844776>.

Internet est une extension de l'espace de vie et de notre monde. Le débat au sujet du Pair à Pair (Peer-to-Peer), suscité par le procès du site the Pirate Bay, n'était pas qu'une simple question de violation des droits d'auteur. Ce procès a été perçu par les utilisateurs du site comme une tentative de détruire un nouvel espace public où les individus pouvaient vivre et s'exprimer notamment par le partage altruiste de leur Culture. Le procès « the Pirate Bay » a marqué l'avènement d'un nouvel espace de vie, qui a d'ailleurs survécu à ce procès.

3. Pendant ce temps, au cœur de la Silicon Valley, la société numérique est en construction. Des milliers d'entreprises hautement performantes produisent l'ensemble de logiciels et services que nous utilisons quotidiennement. Elles fournissent notamment aux Etats les outils de gouvernance, elles influencent les politiques publiques dans leurs intérêts. Leur force repose sur une hypothèse puissante : les données personnelles sont le pétrole du XXI^e siècle³. Les données personnelles sont un concentré d'énergie à haute valeur dont on peut extraire de nombreux sous-produits. Cette notion est régulièrement évoquée pour concevoir les politiques publiques. Pourtant il est particulièrement dérangeant de parler de pétrole quand il s'agit en réalité d'humains dont on parle. Les données personnelles ne sont pas un simple produit mais des éléments de la personne humaine.

III. A la recherche de nouveaux droits liés au numérique

4. En Europe et en Amérique du Nord, on peut observer que les mouvements de protection des droits humains poussent à l'émergence de nouveaux droits cherchant à répondre aux problématiques de notre société numérique. Le droit à l'accès aux données, le droit à l'oubli, font partie des nouveaux droits émergents. Mais ces mouvements sont encore à la recherche d'un

³ « Data is the new oil », expression rendue célèbre en 2006 par CLIVE HUMBY, un mathématicien américain, lors du ANA Senior marketer's summit, Kellog School ; voir PALMER MICHAEL, Data is the New Oil, 3 novembre 2006, in : [ana.blogs.com](https://ana.blogs.com/maestros/2006/11/data_is_the_new/comments/page/2/#comments), https://ana.blogs.com/maestros/2006/11/data_is_the_new/comments/page/2/#comments.

droit humain fondamental, qui serait la justification pour l'ensemble des droits numériques.

5. Les révolutions et évolutions humanistes ont un lien étroit avec les technologies. C'est l'avènement de l'imprimerie qui a permis d'accélérer la diffusion des idées mais a aussi permis d'initier un changement profond dans l'organisation de la société. De la même manière, Internet et le numérique ont apporté un changement sociétal d'ampleur comparable, voire même supérieur, à celui induit par l'apparition de l'imprimerie. Ces changements touchent notamment la manière dont les individus communiquent et échangent entre eux. Cela induit des changements des règles de la société. Avec un contrat social en évolution, des nouveaux droits humains apparaissent. Nous le constatons déjà.

IV. Le droit à la vie comme fondement

6. En observant la construction des droits fondamentaux dans différentes juridictions, on peut constater qu'ils s'organisent autour du droit à la vie. Ainsi, si chaque individu a le droit d'exister, ses autres droits sont une déclinaison du droit à la vie. Sans le droit à la vie, nous n'aurions simplement aucun autre droit. La notion de droit à la vie émerge avec le Christianisme et le Judaïsme selon la formule biblique : « tu ne tueras point ». Ce concept a évolué jusqu'à être inclus plus récemment dans des déclarations de droits humains ainsi que dans des Constitutions.
7. Le droit à la vie inclut à la fois le droit de naître et celui de mourir dignement. Il s'agit d'un concept hautement symbolique d'application extrêmement large. Dans les textes qui le consacrent, il n'apparaît que peu d'éléments qui permettent sa mise en œuvre directe. C'est au travers de l'ensemble du dispositif normatif que l'on va donner forme à ce droit à la vie.
8. Si chaque humain se voit attribuer le droit à la vie, le droit ne propose pas de définition de ce qu'est un humain. Même avec une jambe en moins ou un chromosome en plus, on reste humain. Le droit à la vie est construit sur une hypothèse : l'existence des humains. A aucun moment, savons-nous de quoi est composé l'être humain titulaire du droit à la vie. Certains textes, comme la

Constitution fédérale, proposent des droits annexes qui ont une nature symbolique supplémentaire mais aussi une portée pédagogique. Ainsi, dans le prolongement de nos croyances selon lesquelles l'humain est un corps et un esprit, la Constitution fédérale garantit à ses citoyens, dans son article 10, le droit à l'intégrité physique et l'intégrité psychique. Il s'agit encore une fois de concepts extrêmement larges mais qui s'imposent dans toutes les relations de l'Etat, par ses institutions ou ses représentants, avec le citoyen. Une relation qui ne respecterait pas ces droits serait considérée comme abusive. L'Etat cherche également à garantir l'application de ces droits dans les relations entre les citoyens.

9. Si certains abus peuvent être facilement identifiables, comme l'esclavagisme ou les violences corporelles, d'autres abus peuvent être soumis à interprétation. Ainsi le domaine de la publicité, dont le but est clairement de modifier l'état mental de l'individu, est soumis à une réglementation importante. Le droit acceptera une publicité informative, mais refusera l'utilisation de messages subliminaux, car ils constitueraient une atteinte à l'intégrité psychique de la personne en altérant sa capacité de juger librement.

V. L'espace numérique, une nouvelle réalité immatérielle

10. Lorsque Peter Sunde nous dit : « Nous pensons qu'Internet est réel », il exprime une évolution fondamentale dans notre vie. Nous voyons apparaître l'espace numérique comme une extension de notre espace de vie. L'espace numérique est simplement perçu comme une réalité immatérielle par les individus. Avant même notre naissance, nous y apparaissions au travers de données médicales ou d'une simple échographie partagée sur un réseau social. Au moment de notre naissance, de par la quantité de données personnelles, nous existons déjà numériquement.
11. Le droit à la vie s'applique avant la naissance. C'est tout l'enjeu du débat profond sur l'avortement qui a lieu dans nos sociétés. Par analogie, notre existence numérique précédant notre naissance, une forme de protection devrait déjà être consacrée avant la naissance. De la même manière, il existe un droit de mourir dignement. Dès lors que la mort survient également dans le numérique, notre société devrait également apprivoiser le concept de mort numérique.

VI. La reconnaissance de la vie numérique

12. Notre postulat est donc le suivant : le droit à la vie comprend notre existence numérique. La vie numérique a étendu les contours de notre personnalité juridique. Nous devons le reconnaître et en déduire des conséquences juridiques.
13. En reconnaissant la vie numérique, nous pouvons alors affirmer que, en sus de la nécessaire protection de notre intégrité physique et psychique, nous avons un droit à la protection de notre intégrité numérique.
14. Il existe un lien entre notre autonomie, donc notre capacité de faire nos propres choix, et notre liberté individuelle. Une personne dont l'intégrité est en danger n'est pas en mesure de faire ses propres choix en pleine autonomie. Certaines jurisprudences⁴ reconnaissent déjà notre droit à l'autodétermination informationnelle qui est l'extension de notre volonté d'être autonome également dans l'espace numérique. Donc, par analogie avec la nécessaire protection de l'intégrité physique garante de notre autonomie et de notre liberté, c'est le droit à la protection de l'intégrité numérique qui permettra de garantir à l'individu de rester autonome dans ses choix et donc libre, également, dans l'espace numérique.

VII. Les données, des éléments de notre personne

15. Ce sont principalement les données personnelles qui constituent notre existence numérique. Contrairement à notre corps physique dont on croit comprendre aisément les limites, notre existence numérique paraît floue, enregistrée dans de multiples endroits. Nos données sont multiples et comprennent celles que nous créons consciemment, nos traces que nous laissons sur Internet, et celles qui sont créées indépendamment de notre volonté sur la base de

⁴ CÉLIAN HIRSCH, La condamnation d'un automobiliste grâce à la recherche automatisée de véhicule, 15 novembre 2019, in : *LawInside.ch*, www.lawinside.ch/839/.

l'analyse de nos données primaires⁵. L'ensemble de ces données constituent notre « corps » numérique.

16. Les données personnelles sont des éléments constitutifs de notre personne. Cette position a déjà été exprimée par l'AFAPDP (l'Association Francophone des Autorités de Protection des Données Personnelles) dont le Préposé suisse à la protection des données ou encore la CNIL française sont membres. Dans la Résolution sur la propriété sur les données personnelles du 18 octobre 2018⁶, l'AFAPDP a affirmé que « les données à caractère personnel sont des éléments constitutifs de la personne humaine, qui dispose, dès lors, de droits inaliénables sur celles-ci ». Cela revient à assimiler les données personnelles à des organes du corps humain. Par principe, l'individu ne peut pas renoncer à ses droits sur ses données. Les données personnelles ne peuvent donc pas être cédées, leur propriété ne peut être transférée.
17. Aujourd'hui, la collecte de données personnelles paraît admise par la société même si cette collecte est effectuée par une personne, entreprise ou institution qui n'entretient aucune relation avec l'individu concerné. Cette collecte est autorisée en raison de l'absence de protection juridique de la donnée personnelle que l'on considère comme une chose abandonnée dont on peut se saisir librement. La reconnaissance de la vie numérique permettrait de considérer une telle collecte comme une atteinte à l'intégrité numérique de la personne que seul un consentement éclairé autoriserait. Cette reconnaissance enclencherait un processus de réappropriation des données. Ni l'innovation ni la raison économique ne devraient pouvoir justifier des collectes de données personnelles.

⁵ PANOPTYKON FOUNDATION, Three layers of your digital profile, 18 mars 2019, in : *panoptikon.org*, <https://en.panoptikon.org/articles/three-layers-your-digital-profile>.

⁶ ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES, Résolution sur la propriété sur les données personnelles, 18 octobre 2018, <https://www.edoeb.admin.ch/edoeb/fr/home/le-pfpdt/cooperation-internationale/association-francophone-des-autorites-de-protection-des-donnees-.html>.

VIII. L'étendue insaisissable de notre existence numérique

18. Nous devons également enfin admettre qu'il est impossible pour un individu de connaître l'étendue de son existence numérique. Même pour des experts en informatique⁷, il est impossible d'apprécier la quantité de données numériques qui nous constituent, ni même le nombre et le lieu des bases de données numériques dans lesquelles les informations nous concernant sont enregistrées. Nos lois actuelles de protection des données ont été établies en partant du principe qu'il est de la responsabilité de l'individu de connaître l'existence des données qui le concernent, cette connaissance étant un prérequis pour qu'il puisse se défendre contre d'éventuels abus. Ce mécanisme est tout simplement irréaliste pour assurer la protection des données numériques d'individus qui ignorent tout de l'étendue de leur existence numérique. La mise en œuvre d'un droit à l'intégrité numérique permettrait de garantir que la protection contre les abus puisse être assurée même si l'on ignore l'étendue exacte des données numériques concernant un individu et le lieu exact où elles sont enregistrées. Cela permettrait de renverser enfin le fardeau de la preuve et d'offrir aux individus une réelle protection de leurs données numériques.

IX. La mise en œuvre de la protection de l'intégrité numérique

19. Le droit à l'intégrité numérique doit trouver son chemin vers le texte fondamental du droit suisse. Ajouter le droit à l'intégrité numérique à l'article 10 de la Constitution fédérale permettrait d'imposer à l'Etat, ses institutions et ses représentants d'interagir avec les citoyens en garantissant leur sécurité numérique. L'Etat doit déjà s'assurer de traiter les citoyens avec dignité dans le respect de leur intégrité physique et psychique. L'utilisation de GovWares, la mise en place de surveillance des communications, l'utilisation de bases de données centralisées, la mise en place de surveillances financières nous montrent que de nombreuses institutions étatiques n'agissent

⁷ BERNARD MARR, How Much Data Do We Create Every Day ? The Mind-Blowing Stats Everyone Should Read, 21 mai 2018, in : *Forbes.com*, <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#3b3dd38b60ba>.

pas dans le respect de l'intégrité numérique des citoyens en participant activement à la propagation des données personnelles ou à l'insécurité de l'espace numérique dans lequel nous vivons. Les institutions étatiques ne doivent pas pouvoir être autorisées à utiliser, pour leur propre confort, des outils numériques contenant des données personnelles des individus en se contentant de respecter un cadre légal qui ne fait que proscrire les abus. L'Etat doit promouvoir la construction d'un espace numérique sûr et ouvert, utilisable par tous. La mise en œuvre du droit à l'intégrité numérique en Europe imposera une modification de l'article 2 du Règlement général sur la protection des données⁸ de l'Union européenne afin de réduire drastiquement les larges exclusions prévues pour des motifs sécuritaires dans l'article 2 alinéa 2d du Règlement.

20. De même, l'introduction de la protection constitutionnelle de l'intégrité numérique doit inciter l'Etat à fournir aux citoyens les outils et l'éducation nécessaires à la protection de leur intégrité numérique. Par exemple, un droit d'utiliser la cryptographie sans aucune restriction devrait exister. La cryptographie est un des outils fondamentaux nécessaires à la protection des données personnelles. La maîtrise d'un tel outil est essentielle dans une société numérique afin que chaque individu puisse protéger son autonomie. Le rôle de l'Etat est d'éduquer les citoyens et de les inciter à maîtriser cet outil qui permet notamment un usage responsable de la signature électronique. Pourtant la tentation est grande pour certains Etats ou institutions étatiques, à l'instar du législateur australien⁹, de vouloir forcer l'utilisation d'outils cryptographiques ayant des portes dérobées utilisables par les forces de l'ordre. Cela va à l'encontre d'une application démocratique de la cryptographie. De plus, la simple utilisation d'outils non conformes mais réellement protecteurs est considérée, dans certaines situations, comme suspecte. Se protéger devient alors synonyme de vouloir cacher un comportement répréhensible. Malheureusement, une telle politique

⁸ Règlement (UE) 2016/679 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 ; JOUE L 119/1).

⁹ Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Australie), https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

a pour seul résultat de mettre en péril la sécurité des citoyens dans leur espace de vie numérique.

21. Enfin, l'introduction d'un droit à l'intégrité numérique dans un texte comme celui de l'article 3 de la Charte des droits fondamentaux de l'Union européenne permettrait à l'Etat, ses institutions et ses représentants de promouvoir le respect de l'intégrité numérique dans les relations entre les citoyens, ou entre un citoyen et une entreprise. Il existe actuellement un dangereux développement de formes d'esclavagisme numérique reposant sur une exploitation abusive des données personnelles sans réelle contre-prestation. Les Etats sont également incités à utiliser des outils de « big data » qui puisent, par commodité, dans les données personnelles numériques des citoyens. Les services publics devraient être exemplaires et devraient respecter l'intégrité numérique des citoyens en limitant la collecte des données au strict minimum et en n'utilisant que des standards ouverts et libres.

X. Conclusion

22. En plus de notre intégrité physique et psychique, notre intégrité numérique fait partie de notre droit à la vie. Nous devons reconnaître que notre vie numérique a étendu les contours de notre personnalité juridique. Le droit à l'intégrité numérique doit devenir la justification de l'ensemble des droits numériques, notamment ceux dont l'objectif est d'assurer la protection des données personnelles. Le droit à l'intégrité numérique nous permet de revendiquer notre droit à l'autodétermination informationnelle, car nous ne pourrions être autonomes et libres dans nos choix si notre intégrité est menacée. Les hypothèses sous-tendant les règles juridiques censées protéger les données doivent être inversées pour tenir compte de l'impossibilité intrinsèque à connaître l'étendue exacte de nos données numériques. Un changement de perspective est nécessaire, car ce ne sont pas simplement les données qui doivent être protégées, mais les individus.

Bibliographie

ASSOCIATION FRANCOPHONE DES AUTORITES DE PROTECTION DES DONNEES PERSONNELLES, Résolution sur la propriété sur les données personnelles, 18 octobre 2018, <https://www.edoeb.admin.ch/edoeb/fr/home/le-pfpdt/cooperation-internationale/association-francophone-des-autorites-de-protection-des-donnees-.html>

HIRSCH CÉLIAN, La condamnation d'un automobiliste grâce à la recherche automatisée de véhicule, 15 novembre 2019, in : *LawInside.ch*, www.lawinside.ch/839/

MARR BERNARD, How Much Data Do We Create Every Day ? The Mind-Blowing Stats Everyone Should Read, 21 mai 2018, in : *Forbes.com*, <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#3b3dd38b60ba>

PALMER MICHAEL, Data is the New Oil, 3 novembre 2006, in : *ana.blogs.com*, https://ana.blogs.com/maestros/2006/11/data_is_the_new/comments/page/2/#comments

PANOPTYKON FOUNDATION, Three layers of your digital profile, 18 mars 2019, in : *panoptikon.org*, <https://en.panoptikon.org/articles/three-layers-your-digital-profile>

L'intégrité numérique dans la Constitution : Entre liberté et technologies numériques

par

Johan Rochel

Chercheur à l'Université de Zurich

I. L'actualité de l'intégrité numérique	14
II. Jalons conceptuels de l'intégrité numérique	16
A. L'intégrité numérique comme extension fonctionnelle de l'intégrité	16
B. L'intégrité numérique comme intermédiaire vers l'intégrité physique et psychique	18
C. L'intégrité numérique comme outil d'identification de dangers et d'intérêts à protéger	22
D. Conclusion intermédiaire	25
III. L'intégrité numérique comme norme « courroie »	26
A. La cristallisation d'une conception de la liberté	27
B. Impact sur les droits connexes	29
IV. Critiques	33
V. Conclusion	36
Bibliographie	37

I. L'actualité de l'intégrité numérique

1. On l'appelle encore parfois le « Vieux pays » en référence à l'image d'Epinal d'un Valais fantasmé entre majestueuses montagnes et habitants à fort caractère. Le canton est moins souvent associé aux défis numériques, et ce alors qu'il pourrait devenir le premier canton à introduire dans sa Constitution cantonale un droit fondamental portant sur la protection de l'intégrité numérique. En effet, la Constituante actuellement au travail pour réviser entièrement la Constitution cantonale de 1907 a formulé une première série de propositions dont l'une porte sur l'opportunité d'introduire une protection de l'intégrité numérique¹. La commission qui traite des droits fondamentaux propose ainsi à une très large majorité d'inscrire un article stipulant que « Tout être humain a droit à son intégrité numérique »². L'article est proposé à la suite d'un article protégeant l'intégrité physique et psychique (« Tout être humain a droit à son intégrité physique et psychique »).
2. Cette actualité cantonale fait écho à un projet d'initiative populaire actuellement en phase de préparation. L'association « pour la reconnaissance et la protection de la vie numérique » s'engage en faveur d'un changement constitutionnel en proposant de modifier l'article 10 al. 2 de la Cst. féd. : « Tout être humain a droit à la liberté personnelle, notamment à l'intégrité physique, psychique *et numérique* et à la liberté de mouvement ». Deux des personnes à l'origine de ce projet, MM. Barbey et Roussel, ont présenté les éléments principaux de leur argumentaire lors de la Conférence 2019 de l'Association francophone des autorités de protection des données, organisée à Dakar³.
3. Cette actualité politico-juridique autour d'un droit fondamental portant sur l'intégrité numérique nous offre une excellente occasion

¹ L'auteur de cette contribution est membre élu de la Constituante, sous les couleurs du mouvement non partisan « Appel citoyen ». Il est membre de la Commission 2 qui traite des droits fondamentaux.

² Voir le document résumant les propositions de la Commission, <https://www.vs.ch/web/constituante/rapports-preliminaires>.

³ « Plaidoyer pour l'intégrité numérique », Conférence de l'Association francophone des autorités de protection des données (AFAPDP), (Dakar, 2019) (<http://vienumerique.ch/discours-sur-lintegrite-numerique-prononce-a-dakar/>).

de poser les bases d'une réflexion systématique à son propos. En effet, ce nouveau droit fondamental se trouve à la jonction d'un intérêt croissant pour la manière dont les droits de l'homme peuvent répondre aux défis de la numérisation⁴. Cette courte contribution vise donc à proposer une lecture de l'intégrité numérique comme nouveau droit fondamental⁵. Outre sa pertinence politique comme réponse constitutionnelle aux défis du numérique, cette approche va enrichir une réflexion juridique pour l'heure quasiment inexistante sur l'intégrité numérique⁶.

4. Dans une première partie, la contribution pose des jalons conceptuels pour tenter de définir ce que recouvre l'intégrité numérique. Dans une deuxième partie, elle traite de la fonction générale que pourrait remplir le droit à l'intégrité numérique. L'hypothèse défendue ici consiste à voir l'intégrité numérique comme remplissant une fonction de courroie de transmission. Ce nouveau droit permettrait ainsi de préciser la protection générale accordée à la dignité humaine et, dans le même temps, de donner plus de substance à l'autodétermination informationnelle et, plus largement, à la protection de la vie privée. C'est dans cette fonction de courroie que l'intégrité numérique pourrait déployer un effet particulièrement intéressant sur l'ensemble des droits fondamentaux touchant aux défis numériques.
5. Au vu de la polysémie du terme intégrité, il est utile de préciser ce dont la présente contribution ne traite pas. L'usage du terme intégrité comme droit fondamental diffère de l'intégrité au sens

⁴ Sur la question des droits de l'homme et des technologies numériques, VIOLA DE AZEVEDO CUNHA et al. (2013) ; MURPHY et CUINN (2010) ; LAND et ARONSON (2018) ; RISSE (2019). Sur l'actualité du concept d'intégrité, voir les références proposées par ADDIS (2020).

⁵ Pour une structure argumentative similaire sur la question de l'intelligence artificielle, PFEIL (2020).

⁶ Une version plus étoffée de cet article, axée sur la Charte de l'Union européenne et construit sur une interprétation de l'intégrité numérique à l'aune de la philosophie politique républicaine de P. Pettit, sera publiée dans la *Human Rights Law Review*. Dans un article de 1998 portant sur les données et les défis de l'archivage, Rudin mentionne un concept proche (« intégrité informationnelle »), RUDIN (1998). Bondallaz parle de droit « à la vie privée numérique », BONDALLAZ (2007), pp. 231 ss.

technique (intégrité des réseaux ou des systèmes d'information par exemple)⁷. De même, la question du droit à l'intégrité en matière de protection de la propriété intellectuelle (art. 6bis de la Convention de Berne) n'est pas traitée ici⁸. Il est également important de distinguer l'approche proposée par Nissenbaum pour traiter de l'intégrité contextuelle en matière de flux d'informations⁹. Pour elle, l'intégrité contextuelle vise à identifier les contextes sociaux de certains types d'informations et les normes spécifiques qui s'appliquent à chacun des contextes. Cette approche par l'intégrité contextuelle se joue à un autre niveau et, en ce sens, elle peut être compatible avec l'intégrité numérique.

II. Jalons conceptuels de l'intégrité numérique

6. Cette section veut donner une première réponse à la question de la définition de l'intégrité numérique. Cette définition se construit sur la base de trois hypothèses qui vont permettre de délimiter de manière toujours plus précise les contours de ce nouveau droit fondamental. Cette définition de travail sera l'occasion de mobiliser la jurisprudence et la doctrine sur l'intégrité physique et psychique afin de faire ressortir certains points de convergence.

A. L'intégrité numérique comme extension fonctionnelle de l'intégrité

7. De manière intuitive, l'intégrité numérique pourrait être comprise comme l'intégrité dont une personne jouit dans la sphère numérique. Cette nouvelle intégrité serait donc l'extension spatiale de l'intégrité physique et psychique tel que prévu dans la Cst. féd.
8. Cette compréhension intuitive est erronée, mais comprendre d'où elle vient est presque aussi intéressant que sa réfutation. L'idée d'une extension spatiale prend naissance dans une appréhension faussée du « monde » numérique, du « cyberspace », de l'« online ». Les concepts que nous utilisons pour donner du sens aux réalités numériques utilisent systématiquement une composante spatiale,

⁷ Pour cet usage, National Academies of Sciences (2019).

⁸ Sur ce sujet, DE WERRA (2013).

⁹ Voir par exemple NISSENBAUM (2009).

presque géographique. Pour une approche par les droits fondamentaux, cette vision spatiale rattache immédiatement l'intégrité numérique avec des questionnements autour de la notion de juridiction. Pour savoir quels droits fondamentaux s'appliquent au cyberspace, il nous faut déterminer où se trouve cet espace. Mais la piste nous emmène dans un cul-de-sac conceptuel. GRAHAM a raison de souligner que les métaphores spatiales pour appréhender le numérique sont « imprécises et ne permettent pas au débat d'avancer »¹⁰.

9. Les technologies numériques ne doivent pas être pensées comme constituant un monde parallèle. Le défi consiste plutôt à déterminer quels éléments de ces technologies numériques peuvent et doivent être appréhendés de manière spatiale. Premièrement, les technologies numériques ont une existence spatiale très claire par l'intermédiaire des infrastructures physiques nécessaires à leur fonctionnement et à leur utilisation (par exemple centre de données, infrastructure de communication, outils d'utilisation). Deuxièmement, les technologies numériques sont conçues, développées et vendues par des personnes et des entreprises ayant une existence physique. Troisièmement, et de manière centrale pour cette contribution, les technologies numériques se concrétisent à travers les activités qu'elles permettent. D'une part, il s'agit de se concentrer sur les utilisateurs d'une technologie numérique. A ce titre, nous sommes tous utilisateurs de nombreux outils numériques. D'autre part, il s'agit de mettre en lumière que les individus ne sont pas toujours utilisateurs de ces technologies, ils peuvent en être l'objet. Les différents outils numériques de surveillance illustrent qu'une personne, sans utiliser de technologie, peut être soumise à une technologie, comme dans le cas des outils de surveillance déployés dans les « smart city ».

¹⁰ GRAHAM (2019), p. 24. Le texte « Déclaration d'indépendance du cyberspace » de John P. Barlow, rendu public à Davos en 1996, illustre parfaitement ces problèmes conceptuels. Il écrit sans frémir que « le Cyberspace ne se situe pas dans vos frontières. [...] Le Cyberspace est fait de transactions, de relations, et de la pensée elle-même, formant comme une onde stationnaire dans la toile de nos communications. Notre monde est à la fois partout et nulle part, mais il n'est pas où vivent les corps » (traduction française « Editions Hache » disponible <http://editions-hache.com/essais/barlow/barlow2.html>).

10. Dans ce troisième sens, il apparaît clairement que la spatialité des technologies numériques est liée à des activités très concrètes soit en tant qu'utilisateur, soit en tant qu'objet des technologies. Cela n'empêche pas de reconnaître qu'il faut travailler avec un concept de territorialité capable de prendre en compte des situations plus complexes¹¹. A titre d'exemple, le lieu où les données sont sauvegardées (le data center) n'est pas similaire au lieu où l'activité numérique (réception d'un mail) se déroule. Mais tous deux ont une réalité spatiale déterminable.
11. L'intégrité numérique n'est donc pas une extension spatiale du concept d'intégrité. Il ne s'agit pas d'amener l'intégrité dans un monde parallèle, mais bien plutôt de se focaliser sur des activités rendues possibles par des technologies numériques. C'est une extension *fonctionnelle* : l'intégrité numérique porte sur des activités spécifiques aux technologies numériques. Quand une personne utilise une technologie numérique ou qu'elle en est l'objet, son intégrité numérique est potentiellement mise en jeu.

B. L'intégrité numérique comme intermédiaire vers l'intégrité physique et psychique

12. Si l'intégrité numérique est une extension fonctionnelle de l'intégrité, nous devons préciser quelle relation elle entretient avec l'intégrité physique et psychique. De manière fondamentale, l'intégrité numérique n'apparaît pas au même niveau que l'intégrité physique et psychique. Cette dernière vise à protéger un support d'expériences humaines. Elle possède une dimension fondamentale en ce sens qu'elle porte et qu'elle protège les systèmes physiologiques et mentaux dont l'humain a besoin pour établir une relation au monde. A l'inverse, l'intégrité numérique n'est pas un support d'expériences humaines comparable. Elle devrait être appréhendée comme un intermédiaire vers l'intégrité physique et psychique.
13. L'intégrité physique et psychique est protégée par l'art. 10 de la Cst. féd. Au sein de l'UE, l'art. 3 de la Charte protège l'intégrité physique

¹¹ Sur ces défis, DASKAL (2015).

et psychique, spécifiquement dans le domaine de la médecine et de la biologie, notamment sous l'angle de l'importance du consentement¹². La Cour européenne des droits de l'homme a également développé une riche jurisprudence en matière de protection de l'intégrité en lien avec les questions médicales¹³.

14. De manière générale, l'intégrité physique protège le corps physique de la personne. La jurisprudence suisse a clarifié quelles atteintes au corps étaient couvertes par cette protection¹⁴. Elle a notamment traité des atteintes qui ne provoquaient ni douleur ni dommage au corps humain (par exemple du bruit ou des radiations invisibles)¹⁵. De même, il est établi que l'obligation de se couper les cheveux en milieu carcéral¹⁶ ou l'obligation de fournir du matériel biologique à des fins de test¹⁷ touchent l'intégrité physique. L'intégrité physique possède une dimension procédurale essentielle en ce qu'elle fonde le droit d'une personne capable de discernement de choisir comment utiliser son corps. L'intégrité est ici directement liée à l'autonomie¹⁸.
15. L'intégrité psychique protège l'esprit humain dans ses différentes fonctions. La protection porte notamment sur la faculté humaine d'apprécier une situation et de se déterminer sur la base de cette appréciation¹⁹. Il s'agit donc de protéger tout à la fois la capacité de percevoir, la capacité de comprendre et la capacité de décider. De plus, cette intégrité psychique protège la santé mentale (notamment l'absence de douleur ou de souffrance) et le sentiment de valeur de la personne²⁰.

¹² Pour un commentaire général, MICHALOWSKI (2014), N 03.20.

¹³ Pour une analyse générale, MARSHALL (2009), pp. 163 ss. Voir notamment les arrêts *Pretty c. Royaume-Uni* [2002], no 2346/02, *Peck c. Royaume-Uni* [2003], no 44647/98, et *Jalloh c. Allemagne* [2006], no 54810/00.

¹⁴ De manière générale, DUBEY (2017), § 16 ; KIENER, KÄLIN et WYTTEBACH (2018), § 12.

¹⁵ ATF 133 I 110 c. 5.2.3, 120 s. ; 118 Ia 427 c. 4b, 434

¹⁶ ATF 1P.528/1995 c. 2b.

¹⁷ ATF 128 II 259 c. 3.3, 269 s.

¹⁸ DUBEY (2017), § 16, N 1280 ; KIENER, KÄLIN et WYTTEBACH (2018), § 12.

¹⁹ ATF 133 I 110 c. 5.2, 119 ; 127 I 6 c. 5a, 11.

²⁰ DUBEY (2017), § 16, N 1287 ; SCHWEIZER (2014), art. 10 Cst., N 25.

16. Dans les deux cas, l'intégrité protège un ensemble de capacités humaines fondamentales liées au fonctionnement du corps et de l'esprit. En ce sens, elle protège les supports de l'expérience humaine, expérience étant ici définie de la manière la plus fondamentale possible comme relation au monde extérieur. Il apparaît clairement que l'intégrité numérique ne doit pas être conçue au même niveau. Elle ne protège pas un support d'expériences humaines comparable.
17. Sur ce point également, la manière dont nous parlons du numérique peut nous emmener sur des pistes conceptuellement hasardeuses. Parler de vie numérique peut laisser entendre que nous aurions une sorte de « moi » dédoublé avec une vie numérique propre, une sorte d'avatar « Second life ». Mais les expériences négatives que nous faisons par le biais d'activités numériques n'impactent pas un moi numérique, elles impactent un esprit et un corps, ceux-là mêmes qui sont protégés par l'intégrité physique et psychique. L'intégrité numérique joue un rôle d'intermédiaire entre les activités numériques et d'éventuelles menaces sur le corps et l'esprit : via des activités numériques et ce qui s'y déroule, l'intégrité psychique et/ou physique d'une personne peut être menacée.
18. Il existe deux manières additionnelles d'illustrer cette différence de niveau. Premièrement, il est utile de rappeler que la distinction entre le corps et l'esprit est elle-même au cœur d'une controverse millénaire parmi les philosophes. De manière plus générale, les liens entre corps et esprit sont le lieu d'influences religieuses et sociétales. L'esprit n'est-il pas « ardent », tandis que la chair est « faible »²¹ ? Le corps est souvent assimilé à une machine (dont le fonctionnement peut être amélioré de multiples façons), tandis que l'esprit est comparé au pilote, le point d'entrée vers des sphères plus élevées. A ce titre, certains philosophes de l'esprit estiment que toutes les activités psychiques pourraient être réduites à des phénomènes physiques, tels que des connexions électriques dans le cerveau²². A suivre cette piste, l'intégrité psychique serait donc une sous-catégorie de l'intégrité physique. Il est inutile de chercher ici à défendre à tout prix cette conclusion, celle-ci ne sert qu'à illustrer le

²¹ Marc 14, 38 - Matthieu 26, 41.

²² Sur ce débat, MASLIN (2007), ch. 1.

fait que l'intégrité physique pourrait déployer une ambition encore plus fondamentale, visant à rassembler sous sa protection l'ensemble de nos expériences humaines. Cette discussion est intéressante pour nous car elle souligne d'une perspective différente pourquoi l'intégrité numérique doit être placée à un autre niveau.

19. Deuxièmement, la même conclusion peut être défendue en posant la question des conditions d'une intégrité numérique comme support d'expériences. Pour ce faire, nous pourrions imaginer une entité numérique capable d'expérimenter des états comparables aux états mentaux et physiques humains. Le philosophe Luciano Floridi a par exemple développé une approche centrée autour d'un écosystème informationnel comprenant des entités numériques complexes et autonomes²³. Si ces entités étaient déjà réalité, nous pourrions envisager une réflexion sur leur intégrité numérique comme support d'expériences, non humaines, mais fondamentales. Cette intégrité serait la bonne approche pour appréhender ces expériences, étant donné l'absence d'existence physique (à part une existence sous forme de données sauvegardées sur un serveur) et d'existence mentale. Cette analogie, marquée (encore) par une approche de science-fiction, clarifie que les activités numériques de l'être humain ne peuvent pas être appréhendées par le biais d'une intégrité numérique comprise comme support d'expériences.
20. L'intégrité numérique est utilisée comme vecteur pour signifier la spécificité des dangers liés aux technologies numériques, dangers qui pèsent sur l'intégrité physique et psychique des personnes²⁴. L'intégrité numérique est donc utilisée comme un outil pour mettre en lumière de nouveaux dangers pour la personne humaine dans un contexte marqué par l'omniprésence de technologies numériques.

²³ FLORIDI (2013), ch. 7. Il se posera d'ailleurs peut-être une fois la question de savoir comment il faut protéger les droits de ces entités. Voir par exemple au sujet des robots et des IA, VAN DEN HOVEN VAN GENDEREN (2018).

²⁴ Afin d'illustrer cette idée d'intermédiaire, il est intéressant de rappeler un cas où le Tribunal fédéral mentionne que la prise d'empreinte digitale d'un suspect et le fait de le prendre en photo touchent « sans conteste la sphère intime de l'individu et [constituent], partant, une atteinte à la liberté personnelle », ATF 109 Ia 146, 155. La technologie apparaît comme pouvant mettre en jeu la protection due à la personne humaine. La référence doit être appréciée avant tout à titre d'illustration de l'idée générale d'intermédiaire.

***C. L'intégrité numérique comme outil d'identification
de dangers et d'intérêts à protéger***

21. La troisième hypothèse porte sur l'utilité fonctionnelle de l'intégrité numérique comme outil d'identification des dangers spécifiques liés aux technologies numériques, tant pour la personne qui utilise ces technologies que pour celle qui en est l'objet. Par effet miroir, cette mise en lumière des dangers va permettre de mettre en exergue les intérêts que l'intégrité numérique permettrait de protéger. Il s'agit des deux faces d'une même médaille.
22. Pour la personne utilisatrice de technologies numériques, trois types de dangers peuvent être identifiés. Premièrement, les activités numériques peuvent être documentées, suivies et mesurées – en un mot, surveillées. Différents acteurs peuvent être impliqués dans cet effort de surveillance : les entreprises privées qui développent ces technologies, mais également des institutions publiques cherchant à documenter les activités numériques des citoyens²⁵. Mais ces interférences peuvent aller plus loin qu'une logique de surveillance. Les situations de cyber-harcèlement illustrent comment l'utilisation d'outils numériques peut créer de nouvelles sources de dangers²⁶. Comme expliqué avec la deuxième hypothèse, ce n'est pas l'avatar numérique de la personne qui est menacé, c'est bel et bien la personne elle-même par l'intermédiaire des outils numériques qu'elle utilise.
23. Exprimée de manière positive, cette première catégorie de dangers révèle un ensemble d'intérêts qui devraient être protégés lors d'activités numériques. De manière générale, il s'agit de protéger la capacité de la personne utilisant des outils numériques à agir comme une personne libre. L'intégrité numérique protège les éléments nécessaires afin que la personne agisse librement dans et par le biais de ses activités numériques. Comme nous l'avons vu, cette demande de liberté semble inclure à tout le moins un besoin de sécurité (face, par exemple, au cyber-harcèlement) et un besoin d'anonymat afin

²⁵ Pour une analyse des droits de l'homme du pouvoir des grandes entreprises du numérique, JØRGENSEN (2018).

²⁶ Dans le contexte de l'école ou du travail, voir par exemple GREENE (2006) ; CARBO et HUGHES (2010).

de prévenir une surveillance permanente²⁷. Nous verrons plus loin que l'intégrité numérique joue un rôle clef de courroie de transmission assurant la cohérence entre différents droits. Nous apercevons ici l'un de ces chantiers de cohérence entre une protection générale accordée à la capacité d'être libre et l'utilisation spécifique d'outils numériques.

24. Deuxièmement, les technologies numériques peuvent menacer directement l'identité d'une personne. Cette deuxième catégorie est plus fondamentale que la première : il ne s'agit plus des activités elles-mêmes, mais de la condition nécessaire à ces activités. Si l'identité de la personne est détournée, usurpée, volée, celle-ci se retrouve dans l'impossibilité d'utiliser des outils numériques²⁸. Exprimée positivement, cette catégorie se reflète dans l'intérêt de la personne d'avoir le contrôle sur son identité numérique, c'est-à-dire l'ensemble des éléments nécessaires à la réalisation de ses activités numériques.
25. Troisièmement, une menace sur cette capacité d'action encore plus fondamentale porte sur l'opportunité d'accéder aux technologies numériques, principalement l'accès à Internet. L'impossibilité d'accéder à Internet peut avoir de multiples raisons (technologiques, économiques, politiques, liées aux compétences). Au-delà de cet accès général, il est possible de constater des exclusions plus circonstanciées, mais tout aussi pertinentes du point de vue de la capacité d'action des individus. L'accès à certaines plateformes peut être nécessaire pour profiter d'opportunités économiques, d'interactions sociales ou même afin de participer pleinement à la vie politique²⁹. Ce danger est particulièrement marqué dans les situations de quasi-monopole de certaines plateformes.
26. Ces trois catégories de risques (et d'intérêts) portent sur la personne comme utilisatrice de technologies numériques. Pour la situation où la personne est l'objet de ces technologies, c'est la première catégorie de dangers qui est la plus pertinente, à savoir toutes les

²⁷ Bondallaz traite le droit à l'anonymat comme un point essentiel du respect de la vie privée, BONDALLAZ (2007), pp. 259 ss.

²⁸ Sur l'idée d'identité, SULLIVAN (2011).

²⁹ Pour une analyse droits de l'homme de l'accès aux réseaux sociaux, JONES (2014).

formes de surveillance qui peuvent s'exercer sur les individus³⁰. Dans ce contexte, l'intégrité numérique vise à mettre en lumière l'impact important que peuvent déployer les technologies numériques sur la vie des individus, notamment sur leur capacité à agir librement. Différents acteurs peuvent menacer la liberté : les autorités publiques, un employeur, ou simplement un voisin. Le degré de menace est bien sûr différent, mais les trois cas de figure peuvent être pertinents au titre de menace pour l'individu³¹.

27. Dans cette catégorie de la personne comme objet, il est important de distinguer entre des types de menaces bien connues, réactualisées par de nouvelles technologies, ou de nouvelles menaces, apparues avec certaines technologies. Dans la première catégorie, on trouve toutes les mesures de surveillance. Celles-ci ne sont pas apparues avec le numérique, mais cette technologie a décuplé leur capacité d'action. Dans ce cas, l'intégrité numérique met en exergue le phénomène de réactualisation d'une menace par le biais d'une technologie. Souvent, cette menace peut être appréhendée à l'aune d'autres droits fondamentaux (par exemple la protection générale de la liberté, de la vie privée, de l'autodétermination informationnelle). L'intégrité numérique vient en complément, afin de souligner la spécificité de l'outil numérique comme source de menace.
28. Dans la deuxième catégorie, nous trouvons des nouvelles menaces créées par les technologies numériques. Cette situation est pertinente dans tous les cas où la technologie crée un intérêt digne de protection qui n'existe pas sans cette technologie ou que la technologie crée un véritable nouveau danger. Un premier exemple pourrait être la technologie de l'« Internet des objets » (IoT), connectant à terme l'ensemble de nos appareils quotidiens. De manière plausible, la collecte de données deviendra alors permanente, à travers toutes nos activités privées et professionnelles. L'idée que le consentement est l'instrument fondamental pour justifier ces nouveaux types de récolte de

³⁰ Pour des références générales sur l'idée de surveillance numérique à l'aune des droits de l'homme, LIGHT et OBAR (2019).

³¹ Sur la vidéosurveillance, FLÜCKIGER et AUER (2006). Sur la surveillance informatique dans le milieu professionnel, FANTI (2017).

données ne sera peut-être plus suffisante dans cette existence ultra-connectée³². De même, cette masse de données à disposition sur chacun permettra des pratiques de profilage encore inconnues à ce jour, augmentant l'importance d'une protection contre d'éventuelles discriminations indirectes³³. Un deuxième exemple de nouvelles menaces porte sur l'importance essentielle d'avoir la capacité de réaliser des activités en ligne. A ce titre, il importe d'investiguer si l'accès à Internet ne devrait pas être garanti en tant que droit fondamental³⁴. Il va de soi que ce droit n'avait aucune pertinence avant qu'Internet, ou plus globalement nos activités numériques ne prennent autant d'importance.

D. Conclusion intermédiaire

29. En résumé, l'intégrité numérique en tant que droit fondamental est une extension fonctionnelle de l'intégrité physique et psychique qui porte sur la capacité d'une personne d'utiliser des technologies numériques ou sur la capacité à prévenir d'en être l'objet. A ce titre, l'intégrité numérique vient compléter la protection accordée à l'intégrité physique et psychique en tant que protection du corps et de l'esprit, deux supports d'expériences humaines. L'intégrité numérique agit comme un intermédiaire entre les activités numériques et la protection de l'intégrité physique et psychique. Finalement, l'intégrité numérique permet de mettre en lumière trois catégories principales de menaces. A ce titre, elle souligne un mouvement bien connu pour les droits fondamentaux : de nouvelles technologies apportent de nouvelles menaces dont il faut tenir compte, soit en réactualisant l'interprétation des droits fondamentaux existants, soit en intégrant de nouveaux droits. L'intégrité numérique n'a pas l'ambition de remplacer d'autres droits fondamentaux, mais plutôt de s'inscrire en complément des droits fondamentaux ayant fait leurs preuves dans la protection

³² Sur cette question, ALLHOFF et HENSCHKE (2018), pp. 74 ss ; PEPPET (2014).

³³ Voir l'exemple de l'idée de discrimination « par association » développée par WACHTER (2020).

³⁴ Dans la jurisprudence de la Cour européenne des droits de l'homme, voir l'arrêt *Jankovskis c. Lituanie* [2017], no 21575/08, § 62. Pour la situation européenne, JASMONTAITE et DE HERT (2019). Pour une vue d'ensemble du droit international sur la question, TULLY (2014).

accordée à la personne et sa capacité d'agir librement. L'intégrité numérique souligne l'importance de cette capacité d'action dans un contexte marqué par l'omniprésence des technologies numériques.

III. L'intégrité numérique comme norme « courroie »

30. Sur la base de ces jalons conceptuels, cette troisième section veut préciser la fonction que pourrait remplir l'intégrité numérique comme partie intégrante d'un catalogue de droits fondamentaux. L'hypothèse principale consiste à avancer que l'intégrité numérique remplit une fonction de courroie normative entre la protection générale accordée à la dignité humaine et les droits plus spécifiquement liés à l'autodétermination informationnelle et à la protection de la vie privée. L'intégrité numérique déploie et promeut un effet de cohérence entre ces droits car cette norme exige d'explicitement une conception de la liberté pour une société marquée par les technologies numériques.
31. A titre liminaire, il est intéressant de souligner que cette fonction peut être remplie grâce à l'introduction d'un nouveau droit fondamental (comme le propose la Constituante valaisanne, mais également l'initiative populaire au niveau national). Mais elle pourrait également l'être sur la base de droits existants. A ce titre, le développement jurisprudentiel d'un droit à l'intégrité numérique pourrait ressembler au développement du droit à l'autodétermination informationnelle. La Suisse a peu à peu reconnu et renforcé ce droit, sans qu'il ne soit explicitement contenu dans la Cst. féd. de 1999³⁵. Par contraste, le Conseil d'Etat français écrit au sujet du droit à l'autodétermination qu'il ne souhaite pas le reconnaître comme un nouveau droit. Néanmoins, il reconnaît son importance en lui donnant un statut de principe général d'interprétation. Il écrit que « ce droit ne devrait pas être défini comme un droit supplémentaire s'ajoutant aux autres droits (droit d'information, droit d'accès...) mais comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et interprétés et

³⁵ Pour une vue d'ensemble du développement de ce droit en Europe et en Suisse, FLÜCKIGER (2013) ; WALDMEIER (2015).

mis en œuvre à la lumière de cette finalité »³⁶. Par analogie, l'hypothèse présentée ici veut capter cet effet de cohérence par la finalité de protection de la liberté que porte en elle l'intégrité numérique. Cette remarque liminaire permet de souligner l'intérêt de conceptualiser l'intégrité numérique, qu'elle soit ensuite reconnue à travers un droit fondamental explicite ou qu'elle soit peu à peu reconnue par la voie jurisprudentielle.

A. La cristallisation d'une conception de la liberté

32. L'intégrité numérique est un article « courroie » jouant un rôle d'intermédiaire. D'une part, il précise et opérationnalise la protection générale accordée à la dignité humaine. En admettant que la protection de la dignité humaine soit la base conceptuelle et normative d'un catalogue de droits fondamentaux, à tout le moins dans le droit constitutionnel suisse³⁷, l'intégrité numérique joue un premier rôle similaire à celui de l'intégrité physique et psychique. Protéger la dignité humaine, c'est s'engager, *entre autres*, à protéger l'intégrité physique et psychique de la personne. Interpréter cette intégrité suppose une certaine vision de l'importance du corps et de l'esprit humain en vertu de la protection accordée à la dignité humaine. Suivant une même structure argumentative, protéger la dignité humaine justifie la protection de l'intégrité numérique telle que définie dans la deuxième section.
33. D'autre part, cet article « courroie » va fonctionner comme fondation pour les droits plus spécifiques qui sont directement en lien avec l'usage et l'impact des technologies numériques. Cela concerne notamment les droits liés à la protection des données, de l'autodétermination informationnelle, de la vie privée ou, plus généralement, de la liberté individuelle³⁸. Cela ne signifie bien sûr pas que ces droits sont inopérants sans l'intégrité numérique. Comme l'a écrit le Conseil d'Etat français au sujet de

³⁶ Rapport du Conseil d'Etat, le numérique et les droits fondamentaux, 2014, p. 26, <https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000541.pdf>.

³⁷ BELSER et MOLINARI (2015).

³⁸ Brunner note que la protection de la vie privée est liée à la protection de la dignité humaine, BRUNNER (2018), p. 218. La présente contribution précise cette intuition en introduisant l'intégrité numérique comme courroie de transmission.

l'autodétermination informationnelle, l'intégrité numérique pourrait jouer le rôle de finalité à la lumière de laquelle les autres droits seraient interprétés. Pour utiliser une image, un nouveau droit ou principe d'interprétation « intégrité numérique » serait semblable à un aimant qui modifierait la compréhension et les rapports des différents droits entre eux. Par son effet sur ces droits, l'aimant provoquerait un nouvel ordonnancement.

34. Pour approfondir cette hypothèse de l'article « courroie », il faut spécifier deux éléments. L'intégrité numérique est le *lieu* d'une cristallisation juridique autour d'une protection spécifique face aux technologies numériques (l'aimant). De plus, l'intégrité numérique comme lieu appelle un débat de substance sur le *type* de protection à conférer (le type de force magnétique déployée par l'aimant). En couplant ces deux éléments, l'intégrité numérique représente la cristallisation juridique d'une certaine vision où la capacité d'agir librement de la personne est garantie, tant dans la situation de l'utilisateur que dans celle de l'objet des technologies numériques.
35. Cette approche nous force à spécifier les relations entre l'intégrité numérique et l'idée de liberté. L'intégrité numérique n'a pas exactement le même rapport à la liberté individuelle que l'intégrité physique et psychique. L'intégrité physique et psychique protège le support d'expériences humaines. Elle protège les systèmes physiologiques et mentaux qui rendent possible la liberté humaine. Comme expliqué plus haut, l'intégrité numérique n'a pas prétention à être aussi fondamentale, elle se déploie à un autre niveau. Elle vise à protéger une qualité normative, un certain standard de liberté, dans la manière dont une personne peut agir en société. Sa relation avec la liberté n'est donc pas celle d'une condition préalable (comme le corps et l'esprit), mais celle d'une modalité d'exercice (quelle liberté dans une société marquée par les technologies numériques ?). Cette dimension de modalité d'exercice de la liberté porte en elle une réelle substance normative. Définir l'intégrité numérique, c'est tenter de définir le type et le degré de liberté, respectivement de protection, qui doit être garanti dans un contexte marqué par l'omniprésence des technologies numériques. L'intégrité numérique représente la norme qui va cristalliser cette substance.
36. Cette dimension substantielle explique pourquoi l'intégrité numérique joue un rôle de courroie avec des droits plus

procéduraux. En effet, la protection accordée à l'autodétermination informationnelle possède une dimension avant tout procédurale. Pour le Tribunal fédéral, cette autodétermination garantit à chacun la maîtrise de ses données personnelles³⁹. En d'autres mots, la personne doit avoir le droit de décider si elle souhaite ou non, et si oui à quelles conditions, communiquer des données à son sujet⁴⁰. Cette approche donne un rôle essentiel à l'idée de consentement exprimé par la personne. Le droit à l'autodétermination informationnelle, mais plus généralement la protection de la vie privée, reste passablement neutre sur le plan du contenu de la protection⁴¹. Le travail normatif est fait avant tout par le mécanisme de consentement de la personne. Comme l'explique Solove, l'approche par consentement permet, si elle est poussée à l'extrême, de légitimer toutes sortes de menaces pour la vie privée : « the privacy self-management model attempts to be neutral about substance – whether certain forms of collecting, using, or disclosing of personal data are good or bad – and instead focuses on whether people consent to the collection, use, or disclosure of their data. Consent legitimizes nearly any form of collection, use, and disclosure of personal data »⁴².

37. Le trait est volontairement forcé pour bien faire apparaître l'espace normatif que peut occuper l'intégrité numérique. La présence de cette norme force un débat sur la définition substantielle de la liberté et sa pertinence face aux technologies numériques.

B. Impact sur les droits connexes

38. Cette définition substantielle de la liberté et sa cristallisation par l'intermédiaire de l'intégrité numérique vont impacter une série de droits connexes. Cette connexion s'établit sur la base d'un lien entre l'usage d'une technologie numérique et la protection de la liberté individuelle. La présente contribution doit se borner à mettre en

³⁹ TF 2P.165/2004 c. 7.1.

⁴⁰ Pour une vue d'ensemble, FLÜCKIGER (2013), pp. 852 ss.

⁴¹ Sur le droit des personnes de renoncer à cette protection de leur consentement, SINHA (2018).

⁴² SOLOVE (2013), p. 1880.

lumière ces liens, elle ne peut les exemplifier à la lumière d'une conception concrète de la liberté. Pour ce faire, il faudrait esquisser une conception de la liberté et l'appliquer ensuite à l'intégrité numérique et à ses effets sur les droits connexes⁴³.

39. Premièrement, l'intégrité numérique impacte les droits qui protègent la vie privée. De manière fondamentale, la protection de cette intégrité pose la question de l'importance donnée au consentement. À l'aune de la capacité d'une personne à agir librement en lien avec les technologies numériques, la question du consentement apparaît comme un mécanisme fondamental de protection de l'autonomie individuelle⁴⁴. L'intégrité numérique aurait certainement un impact sur les qualités requises pour ce consentement, à titre d'utilisateur comme à titre d'objet des technologies. L'idée générale qui pourrait guider l'interprétation renouvelée du consentement consisterait à donner à la personne qui consent de véritables moyens d'identifier, de comprendre, et de contrôler les opérations qui découlent de son consentement⁴⁵. Des questions portant sur le processus de consentement, sur les parties en présence et leurs rapports de force respectifs, sur la forme du consentement et sur son objet gagneraient ainsi en visibilité et en importance dans l'évaluation de la légitimité d'un consentement. Il ne s'agit pas d'arguer que ces considérations sont totalement absentes du débat actuel. Sous l'effet d'un nouveau droit, leur interprétation serait amenée à évoluer.
40. En matière de vie privée, l'intégrité numérique aurait également un impact important sur les questions d'autodétermination informationnelle. Afin de ne pas provoquer de fausses attentes, il est crucial de rappeler que le droit à l'intégrité numérique est avant tout le lieu d'un débat sur les contours de la liberté. Il n'est pas la

⁴³ Pour une tentative en ce sens, voir ma proposition d'adopter une approche néo-républicaine de la liberté (définie comme absence de domination) et son impact sur certains droits (article à venir dans la *Human Rights Law Review*). Pour une approche de la vie privée avec une conception républicaine de la liberté, ROBERTS (2015), p. 327.

⁴⁴ Parmi une abondante littérature, HAASE (2019).

⁴⁵ Pour l'argument néo-républicain derrière cette approche, LAOGHAIRE (2018), p. 232.

solution miracle, comme tombée du ciel constitutionnel, qui permettrait de régler d'un seul coup toutes les controverses. C'est plutôt sa présence – et l'effet qu'il provoque sur les droits connexes – qui va forcer le débat et faire bouger les lignes. A l'exemple de la question de savoir si le sujet possède, au sens de la propriété, ou seulement contrôle ses données⁴⁶, l'intégrité numérique ne fournit pas de réponses toutes faites, mais elle offre le lieu où les différentes approches pourront clarifier leur vision de la liberté. Par la substance qu'elle amène dans le débat (par contraste avec des normes essentiellement procédurales), l'intégrité numérique force à expliciter des divergences en matière de conceptions de la liberté. Par analogie, la question du don/vente d'organes ne peut pas être réglée par un recours exclusif au concept d'intégrité physique. Par contre, cette norme est le lieu du débat (notamment la disponibilité de certains biens juridiques) et l'interprétation de son contenu normatif sera la réponse donnée à ce débat à un moment X, dans un contexte spécifique.

41. Deuxièmement, l'intégrité numérique pourrait avoir un impact important sur l'interprétation des droits pertinents pour conceptualiser et prévenir la surveillance des individus. C'est particulièrement important pour les situations où la personne est l'objet de technologies numériques⁴⁷. Dans ces situations, le défi est de sauvegarder la liberté de la personne. L'argument par l'intégrité numérique vient ici s'adosser à la protection générale de la liberté individuelle et aux arguments classiques contre la surveillance (concentration dangereuse du pouvoir, situation de vulnérabilités pour les individus, menaces sur les libertés politiques et civiques).
42. L'intégrité numérique est ici utile en complément pour appréhender les spécificités des dangers découlant des technologies numériques. Imaginons deux cas de surveillance par l'Etat, distincts seulement dans la méthode utilisée. Dans le premier cas, un policier surveille à la jumelle le passage sur la voie publique. Dans le deuxième cas, une caméra « intelligente » (dotée d'outils de reconnaissance faciale) réalise le même travail. Il apparaît que les deux scénarios sont

⁴⁶ Sur ce débat, FLÜCKIGER (2013), pp. 858 ss. Voir également THOUVENIN, FRÜH et LOMBARD (2017).

⁴⁷ Pour des références sur la littérature consacrée à la surveillance, HOYE et MONAGHAN (2018), pp. 347 ss.

porteurs de dangers comparables quant à la menace sur la liberté individuelle (surveillance), mais que le scénario de la caméra amène en plus une nouvelle série de risques. A titre d'exemples, le matériel vidéo peut être sauvegardé, puis analysé de manière automatisée et relié à une banque de données. Le fait de repérer une certaine personne sur la voie publique pourrait même être lié à une suite d'actions automatisées (déclenchement d'une alarme, blocage d'un compte, etc.). Ces actions sont rendues possibles par la technologie. Cette technologie porte en elle un potentiel de surveillance décuplée. Dans ce scénario, l'approche enrichie par l'intégrité numérique permet de mettre en lumière ces dangers directement liés à la technologie. L'intégrité numérique de la personne, définie comme sa capacité à agir librement dans le contexte des technologies numériques, est ici menacée⁴⁸.

43. Troisièmement, cette discussion sur l'impact de l'intégrité numérique sur des droits connexes inclut les questions d'accès aux technologies numériques et de capacité à les utiliser. L'intégrité numérique protège la capacité de la personne à utiliser certaines technologies. Cela comprend l'accès à Internet comme réseau qui va permettre l'utilisation de nombreux outils numériques. Exprimé négativement, cela signifie que l'intégrité numérique n'est pas respectée si la personne n'a pas accès à Internet, soit pour des raisons techniques (le réseau n'est pas disponible là où elle se trouve), soit pour des raisons politico-juridiques (l'accès à Internet est restreint). De manière plus spécifique, cette question de l'accès se pose aussi dans le cas de plateformes ou autres ressources spécialement importantes pour la liberté des individus. Il en va notamment ainsi de plateformes à vocation professionnelle ou de plateformes ayant atteint une telle importance que la vie politique semble exiger de pouvoir y participer. En matière professionnelle, le développement de l'économie de plateforme donne parfois un pouvoir immense à certaines entreprises privées jouant le rôle de « gate-keeper ». Pour un chauffeur indépendant, une exclusion de la

⁴⁸ En cherchant à justifier le droit d'avoir un humain dans un processus de décisions automatisé (« human in the loop »), Jones utilise l'idée de dignité comme valeur de référence. Elle parle également de l'« intégrité de la personnalité ». Son argument pourrait être reformulé sur la base de l'idée d'intégrité numérique. Cette intégrité serait alors la protection accordée à la dignité humaine dans le contexte d'un processus de décisions automatisé. JONES (2017), p. 238.

plateforme Uber signifie un risque économique majeur. Son intégrité numérique, qui protège sa liberté, est mise en jeu, en complément d'autres droits fondamentaux. De manière plus large, cette réflexion s'intègre dans l'ambition de donner un cadre normatif basé sur les droits de l'homme à cette économie de plateforme⁴⁹.

44. Outre l'accès, l'intégrité numérique protège également les conditions d'utilisation de ces technologies numériques. A titre d'exemple, elle protège notamment la personne utilisant ces technologies. Comme mentionné plus haut, les situations de cyber-harcèlement représentent un risque majeur, directement lié aux technologies numériques. La personne n'est plus en capacité d'agir librement car elle est menacée. Ce n'est pas le « double numérique » de la personne qui est touché par le cyber-harcèlement, c'est la personne elle-même, dans son corps et dans son esprit. L'intégrité numérique sert ici d'intermédiaire entre les activités numériques de la personne (ses contacts sociaux sur une plateforme par exemple) et les menaces qui pèsent sur son intégrité physique et psychique.

IV. Critiques

45. Cette vision de l'intégrité numérique se heurte à plusieurs critiques qu'il importe d'évoquer et de discuter⁵⁰. Premièrement, on peut argumenter que l'intégrité numérique est superflue car d'autres droits déjà existants réalisent le même travail normatif. Cette ligne de critique peut être avancée en utilisant le droit à l'autodétermination informationnelle ou l'intégrité informationnelle⁵¹. De manière générale, il faut souligner que l'intégrité numérique prend une place spécifique. Elle crée le lien entre des technologies numériques rendant possibles de nouvelles menaces pour les individus et la protection de la liberté de ces mêmes individus. A ce titre, elle a un champ d'action plus grand que les données (ou l'information). Elle englobe les questions de données dans la mesure où celles-ci sont liées aux technologies

⁴⁹ Voir par exemple NATOUR (2016).

⁵⁰ Pour des critiques similaires dans le cadre de l'autodétermination informationnelle, WALDMEIER (2015), pp. 44 ss.

⁵¹ Pour ce concept, RUDIN (1998).

numériques. Mais elle va plus loin que ces seules données. Par contraste, l'autodétermination informationnelle n'a pas pour objet principal les questions d'accès aux technologies numériques ou la protection à garantir pour les personnes utilisant/étant utilisées par des technologies numériques. Dans le même temps, l'intégrité numérique n'a rien à dire sur les questions de données non liées aux technologies numériques. Nonobstant ces spécificités, il est clair que les deux concepts ont une thématique largement commune. La contribution de l'intégrité numérique consiste à mettre en lien ces droits de nature procédurale avec une vision plus substantielle de la protection de la liberté. A l'aune de cette hypothèse, les deux concepts ne sont pas concurrents, mais plutôt complémentaires. L'intégrité numérique exige, de par son existence au sein d'une Constitution, de clarifier la conception de la liberté dans un contexte marqué par les technologies numériques.

46. Cette approche possède des similarités avec ceux qui veulent utiliser directement la dignité humaine dans le contexte des technologies numériques. C'est au final la même critique selon laquelle l'intégrité numérique serait superflue. L'approche par la dignité vise également à donner plus de substance aux droits de protection des données. Le problème porte alors plutôt sur la difficulté de définir la dignité humaine de manière à la rendre opérationnelle⁵². Sans pouvoir clairement définir ce que signifie la dignité humaine dans le contexte de technologies numériques, il est difficile de l'utiliser pour interpréter les droits connexes⁵³. L'approche par l'intégrité numérique doit relever un défi similaire, mais elle peut le faire en utilisant un concept à la fois moins chargé et moins difficile à appréhender. L'intégrité numérique relie ces différents droits en proposant une norme médiane apportant de la substance, sans être chargée de controverses presque millénaires.
47. Deuxièmement, le concept d'intégrité numérique peut être critiqué pour son manque de clarté. Derrière une formulation attrayante, son contenu reste trop évasif. Ce point n'est pas directement contesté. Comme nombre d'autres droits fondamentaux et principes constitutionnels, l'intégrité numérique est une norme générale,

⁵² Sur cette difficulté à interpréter la dignité humaine, DE HINGH (2019). Pour des références en droit suisse, MAHLMANN (2013).

⁵³ FLORIDI (2016), p. 308.

abstraite et nécessitant un important effort d'interprétation. A ce titre, elle n'est pas différente de l'intégrité physique ou psychique. Cet article défend l'idée que cette généralité n'est pas un défaut, mais une qualité de la norme. Elle est assez ouverte pour remplir ce rôle fonctionnel qui veut qu'elle soit le lieu de la définition d'une conception de la liberté dans un contexte de technologies numériques. Les autorités administratives et judiciaires utilisant cette norme vont devoir préciser leur vision de la personne libre et donc définir peu à peu sa substance normative par voie d'interprétation.

48. Troisièmement, l'intégrité numérique peut être critiquée à cause de son impact négatif sur d'autres droits fondamentaux ou, plus généralement, sur l'équilibre lentement construit entre différents droits fondamentaux⁵⁴. Par exemple, l'équilibre entre les droits protégeant la vie privée d'un individu et le droit des médias d'investiguer et de divulguer certaines informations pourrait être remis en jeu par l'arrivée de l'intégrité numérique. A titre d'exemple, cette norme pourrait avoir un impact sur le niveau d'attention portée à la protection face aux méthodes de data-journalisme. En guise de réponse à cette critique, il faut avant tout souligner que le droit à l'intégrité numérique, comme les autres droits fondamentaux, peut être restreint. De plus, il importe de souligner le caractère nécessairement dynamique de l'interprétation de chacun des droits fondamentaux et de leurs équilibres mutuels. La jurisprudence évolue et les équilibres sont transformés. Il serait faux de vouloir sanctuariser un état de la jurisprudence à un moment X. L'arrivée de nouvelles technologies oblige les autorités administratives et judiciaires à adapter leur interprétation de certains principes et droits fondamentaux. L'intégrité numérique, comme l'autodétermination informationnelle, sont apparues à la suite de nouvelles technologies ayant créé de nouvelles sources de dangers pour les libertés humaines. Le caractère dynamique de leur interprétation et de leur application est crucial.

⁵⁴ Merci au Prof. BERTIL COTTIER d'avoir soulevé cette critique. Voir FLÜCKIGER (2013), p. 853.

V. Conclusion

49. Cette contribution souhaite poser les bases conceptuelles d'un droit à l'intégrité numérique. De manière générale, l'argument pour cette intégrité numérique procède d'une logique simple, presque banale : l'apparition de nouvelles technologies, numériques en l'espèce, provoque de nouveaux dangers pour la personne et sa capacité à vivre librement en société. Ces nouveaux dangers peuvent et doivent être abordés grâce aux droits fondamentaux existants. Néanmoins, ils peuvent également être l'occasion de réfléchir à l'introduction de nouveaux droits. C'est dans cet esprit de dialogue constructif que la présente contribution a présenté les contours possibles d'un droit à l'intégrité numérique.
50. Ce droit à l'intégrité numérique est une norme « courroie » qui doit être appréhendée de manière fonctionnelle entre la protection générale de la dignité humaine et les droits plus spécifiques liés à la protection face aux technologies numériques, notamment la protection des données et la protection de la vie privée. L'intégrité numérique joue ce rôle de courroie normative en se proposant comme norme qui va cristalliser une conception de la liberté en contexte de technologies numériques. Que veut dire être libre, à la fois comme utilisateurs et comme objets de ces technologies ? La réponse à cette question donne la substance de l'intégrité numérique, substance qui va à son tour être impactée par l'interprétation des droits connexes.
51. L'intégration de l'intégrité numérique dans un catalogue de droits fondamentaux déploie donc une dynamique normative. Ce nouveau droit aurait le premier mérite de forcer un débat longtemps repoussé sur cette conception de la liberté en matière numérique, tant par les spécialistes de droit constitutionnel que par les décideurs politiques. Il aurait ensuite le second mérite de créer une forme de cohérence autour de cette conception en irradiant vers les droits directement mobilisés pour répondre aux défis du numérique. L'intégrité numérique n'a pas réponse à toutes les questions actuellement ouvertes, mais elle est le lieu et le vecteur d'un débat aussi important que nécessaire.

Bibliographie

- Cour EDH, affaire Pretty c. Royaume-Uni, requête no 2346/02 [2002]
- Cour EDH, affaire Peck c. Royaume-Uni, requête no 44647/98 [2003]
- Cour EDH, affaire Jalloh c. Allemagne, requête no 54810/00 [2006]
- Cour EDH, affaire Jankovskis c. Lituanie, requête no 21575/08 [2017]
- ADDIS A., Dignity, Integrity, and the Concept of a Person, ICL Journal 4/2019, pp. 323-372
- ALLHOFF F./HENSCHKE A., The Internet of Things : Foundational Ethical Issues, Internet of Things 1-2/2018, p. 5566
- BELSER E. M./MOLINARI E. M., ad art. 7, in : Belser/Epiney/Waldmann (édit.), Basler Kommentar, Bundesverfassung, Bâle 2015
- BONDALLAZ S., La protection des personnes et de leurs données dans les télécommunications, Analyse critique et plaidoyer pour un système en droit suisse, Zurich 2007
- BRUNNER L., Digital Communications and the Evolving Right to Privacy, in : Aronson/Land (édit.), New Technologies for Human Rights Law and Practice, Cambridge 2018
- CARBO J./HUGHES A., Workplace Bullying : Developing a Human Rights Definition from the Perspective and Experiences of Targets, Journal of Labour and Society 3/2010, pp. 387-403
- DASKAL J. C., The Un-Territoriality of Data, Yale Law Journal 2/2015, pp. 326-398
- DE HINGH A., Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation, German Law Journal 5/2019, pp. 1269-1290
- DE WERRA J., Le droit moral en Suisse, Les cahiers de propriété intellectuelle 1/2013, pp. 527-547
- DUBEY C., Droits fondamentaux, Volume II : Libertés, garanties de l'Etat de droit, droits sociaux et politiques, Bâle 2017

FANTI S., Protection des données informatiques, in : Dunand/Mahon (édit.), La protection des données dans les relations de travail, Genève/Zurich 2017

FLORIDI L., On Human Dignity as a Foundation for the Right to Privacy, *Philosophy & Technology* 4/2016, pp. 307-312

FLORIDI L., *The Ethics of Information*, Oxford 2013

FLÜCKIGER A., L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, *Pratique juridique actuelle* 6/2013, pp. 837-864

FLÜCKIGER A./AUER A., La vidéosurveillance dans l'œil de la constitution, *Pratique juridique actuelle* 8/2006, pp. 924-942

GRAHAM M., There are no rights "in" cyberspace, in : Wagner/Kettemann/Vieth (édit.), *Research Handbook on Human Rights and Digital Technology*, Global politics, Law and International Relations, Cheltenham 2019, pp. 24-32

GREENE M. B., Bullying in Schools : A Plea for Measure of Human Rights, *Journal of Social Issues* 1/2006, pp. 63-79

HAASE M., Die Einwilligung im Datenschutzrecht – Einschränkung der Freiheit des Einzelnen durch die überzogene Forderung nach Freiwilligkeit, *Zeitschrift zum Innovations- und Technikrecht* 3/2019, pp. 113-118

HOYE J. M./MONAGHAN J., Surveillance, Freedom and the Republic, *European Journal of Political Theory* 3/2018, pp. 343-363

JASMONTAITE L./DE HERT P., Access to the Internet in the EU : a policy priority, a fundamental, a human Right, or a concern of eGovernment ?, in : Wagner/Kettemann/Vieth (édit.), *Research Handbook on Human Rights and Digital Technology*, Global politics, Law and International Relations, Cheltenham 2019, pp. 157-179

JONES B. C., Is Social Media a Human Right ? Exploring the Scope of Internet Rights, *International Journal of Constitutional Law Blog* 2014, disponible sur <http://www.icconnectblog.com/2014/12/is-social-media-a-human-right-exploring-the-scope-of-internet-rights/>

JONES M. L., *The Right to a Human in the Loop : Political Constructions of Computer Automation and Personhood*, *Social Studies of Science* 2/2017, pp. 216-239

JØRGENSEN R. F., *Human Rights and Private Actors in the Online Domain*, in : Land/Aronson (édit.), *New Technologies for Human Rights Law and Practice*, Cambridge 2018

KIENER R./KÄLIN W./WYTTENBACH J., *Grundrechte*, 3^e éd., Berne 2018

LAND M. K./ARONSON J. D. (édit.), *New Technologies for Human Rights Law and Practice*, Cambridge 2018

LAOGHAIRE T. Ó., *Making Offers They Can't Refuse : Consensus and Domination in the WTO*, *Moral Philosophy and Politics* 2/2018, pp. 227-256

LIGHT E./OBAR J. A., *Surveillance reform : revealing surveillance harms and engaging reform tactics*, in : Wagner/Kettemann/Vieth (édit.), *Research Handbook on Human Rights and Digital Technology*, Cheltenham 2019, pp. 195-222

MAHLMANN M., *Die Garantie der Menschenwürde in der Schweizerischen Bundesverfassung*, *Pratique juridique actuelle* 9/2013, pp. 1307-1320

MARSHALL J., *Personal Freedom through Human Rights Law ? Autonomy, Identity and Integrity under the European Convention on Human Rights*, Leiden 2009

MASLIN K. T., *An Introduction to the Philosophy of Mind*, 2^e éd., Cambridge 2007

MICHALOWSKI S., ad art. 3, in : Peers/Hervey/Kenner/Ward (édit.), *The EU Charter of Fundamental Rights, A Commentary*, Oxford 2014, pp. 82-103

MURPHY T./CUINN G. Ó., *Works in Progress : New Technologies and the European Court of Human Rights*, *Human Rights Law Review* 4/2010, pp. 601-638

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING AND MEDICINE, *Authenticity, Integrity, and Security in a Digital World*, *Proceedings of a Workshop – in Brief*, Washington 2019

NATOUR F., Respecting Human Rights in the On-Demand Economy : Closing the New Governance Gap, *Business and Human Rights Journal* 2/2016, pp. 315-320

NISSENBAUM H., Privacy in Context, Technology, Policy, and the Integrity of Social Life, Stanford 2010

PEPPET S. R., Regulating the Internet of Things : First Steps Toward Managing Discrimination, Privacy, Security, and Consent, *Texas Law Review* 1/2014, pp. 85-176

PFEIL W., “Der Mensch steht höher als Technik und Maschine” – Benötigen wir ein Grundrecht zum Schutz vor Künstlicher Intelligenz ?, *Zeitschrift zum Innovations- und Technikrecht* 2/2020, pp. 82-89

RISSE M., Human Rights and Artificial Intelligence : An Urgently Needed Agenda, *Human Rights Quarterly* 1/2019, pp. 1-16

ROBERTS A., A republican account of the value of privacy, *European Journal of Political Theory* 3/2015, pp. 320-344

RUDIN B., Kollektives Gedächtnis und informationelle Integrität : Zum Datenschutz im öffentlichen Archivwesen, *Pratique juridique actuelle* 3/1998, pp. 247-260

SCHWEIZER R., ad art. 10, in : Ehrenzeller B. et al. (édit.), *Die schweizerische Bundesverfassung, St. Galler Kommentar*, 3^e éd., Zurich 2014

SINHA G. A., Technology, Self-Inflicted Vulnerability, and Human Rights, in : Aronson/Land (édit.), *New Technologies for Human Rights Law and Practice*, Cambridge 2018, pp. 270-28

SOLOVE D. J., Privacy Self-Management and the Consent Dilemma, *Harvard Law Review* 2013, pp. 1880-1903

SULLIVAN C., Digital Identity : An Emergent Legal Concept, The role and legal nature of digital identity in commercial transactions, Adelaide 2011

THOUVENIN F./FRÜH A./LOMBARD A., Eigentum an Sachdaten : Eine Standortbestimmung, *Revue suisse de droit des affaires et du marché financier* 1/2017, pp. 25-34

TULLY S., A Human Right to Access the Internet? Problems and Prospects, *Human Rights Law Review* 2/2014, pp. 175-195

VAN DEN HOVEN VAN GENDEREN R., Do We Need New Legal Personhood in the Age of Robots and AI ?, in : Corrales/Fenwick/Forgó (édit.), Robotics, AI and the Future of Law, Singapore 2018, pp. 15-50

VIOLA DE AZEVEDO CUNHA M. et al. (édit.), New Technologies and Human Rights, Challenges to Regulation, Londres 2013

WACHTER S., Affinity Profiling and Discrimination by Association in Online Behavioural Advertising, Berkeley Technology Law Journal 2/2020, pp. 1-74

WALDMEIER S.-D., Informationelle Selbstbestimmung – ein Grundrecht im Wandel ?, Zurich 2015

Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? Le point de vue du droit constitutionnel

par

Pascal Mahon

Professeur à l'Université de Neuchâtel

I. Introduction.....	44
II. Les protections existantes et leur application au numérique	45
III. La signification et le contenu d'un éventuel « droit à l'intégrité numérique ».....	53
A. L'« intégrité numérique » et ses caractéristiques.....	53
B. Le contenu (encore) incertain d'un éventuel « droit à l'intégrité numérique ».....	55
IV. Conclusion	60
Bibliographie	62

I. Introduction

1. Le concept de « droit à l'intégrité numérique » semble avoir le vent en poupe. L'expression, en tous les cas, est à la mode – en témoigne le titre du colloque dont le présent ouvrage rassemble les contributions – et l'idée paraît même faire des émules chez les constituants, du moins les constituants cantonaux. Ainsi, l'Assemblée constituante valaisanne est ou sera tout prochainement confrontée à une proposition de sa commission relative aux droits fondamentaux visant à intégrer un tel « droit à l'intégrité numérique » dans le catalogue des droits fondamentaux de la future Constitution valaisanne¹. Dans la foulée, à Genève, on envisage aussi l'inscription d'une disposition semblable dans la Constitution cantonale entièrement révisée en 2012².

De même, dans la doctrine³ ou sur un plan plus politique⁴, des voix s'élèvent pour réclamer l'inscription ou la reconnaissance d'un « droit à l'intégrité numérique » soit explicitement dans la Constitution, fédérale ou cantonale, soit comme extension de la garantie de la liberté personnelle et/ou de la protection de la sphère privée.

¹ Voir à ce propos le rapport de la Commission 2 *Droits fondamentaux et sociaux, société civile*, du 17 février 2020, pp. 5-6, https://www.vs.ch/documents/3914032/7264038/2020-02-17_Principes_Rapport+de+la+COMMISSION+2.pdf/31115896-4628-a57e-773f-36b392a8d811?t=1589533364598 ; voir aussi, et surtout, dans cet ouvrage, la contribution de JOHAN ROCHEL, membre de ladite commission, *supra*, pp. 13 et ss.

² Voir à ce propos *Le Temps* du 26 juin 2020, p. 6 : « Le PLR genevois veut protéger l'intégrité numérique », où il est question d'une initiative populaire cantonale qui devrait être lancée fin août 2020.

³ Voir, dans cet ouvrage, la contribution de ROCHEL, déjà citée (note 1).

⁴ Voir SCHWAAB, *Projet socialiste*, pp. 23 et ss, où il est plutôt question d'adapter les droits fondamentaux existants à la révolution numérique, mais où les termes de droit à l'« intégrité numérique » apparaissent aussi (pp. 29 et 31, entre autres), à côté notamment de ceux de droit à l'« éducation numérique » (p. 30) ou à la « formation numérique » (pp. 36-37), etc. Cf. aussi, dans cet ouvrage, la contribution d'ALEXIS ROUSSEL, *supra*, pp. 1 et ss, N 1, qui estime que ce droit « doit être intégré dans la Constitution fédérale », ce qui permettrait « aux droits fondamentaux de faire leur transition tant attendue dans le numérique ».

2. Face à cette revendication, et avant même de déterminer si l'inscription ou la reconnaissance d'un tel « droit à l'intégrité numérique » est souhaitable ou non, on peut et on doit se demander, du point de vue du droit constitutionnel, si l'expression même (« droit à l'intégrité numérique ») recouvre une réelle innovation – de fond – ou si elle manifeste – sous une autre appellation – une simple évolution du droit, un élargissement de ce qui existe. Telle était du moins l'interrogation, qui peut être pertinente dans d'autres branches du droit, à l'origine du colloque organisé en février 2020 à l'Université de Neuchâtel par la professeure Florence Guillaume et le soussigné. L'objet de la présente contribution est donc de répondre – ou, plus modestement, vu la brièveté du propos, de tenter de répondre – à cette interrogation, sous l'angle du droit constitutionnel en général, étant entendu que d'autres contributions y répondront sous des angles plus pointus, relevant aussi, pour partie au moins, du droit constitutionnel⁵.
3. Pour ce faire, la présente contribution commencera par chercher à recenser ce qui existe déjà, aujourd'hui, en droit constitutionnel, et en matière de droits fondamentaux en particulier, et à déterminer dans quelle mesure cet arsenal existant s'applique (aussi) au numérique (II). Elle tentera ensuite de voir ce que signifie et ce qu'apporterait (de plus) – selon ses défenseurs – un éventuel « droit à l'intégrité numérique » (III), avant de revenir à la question posée et d'y répondre, puis de conclure (IV).

II. Les protections existantes et leur application au numérique

4. Si l'on cherche à recenser ce qui existe en termes de dispositions juridiques protectrices susceptibles de se rapprocher d'un « droit à l'intégrité numérique », on se trouve en effet face à un arsenal imposant de normes les plus diverses. À côté des dispositions de droit civil destinées à la protection de la personnalité (art. 28 et ss

⁵ Voir notamment, sous l'angle du droit de la protection des données, la contribution de JEAN-PHILIPPE WALTER, et sous l'angle du droit des médias et de la liberté des médias, celle de BERTIL COTTIER, toutes deux *infra*, dans cet ouvrage, pp. 95 et ss et 103 et ss.

du Code civil⁶), ainsi que des dispositions pénales ayant un but analogue (notamment art. 111 et ss ainsi que 179 et ss du Code pénal⁷), dont on ne traitera pas ici⁸, le droit constitutionnel général offre lui aussi une protection large et diversifiée des droits de la personnalité, en particulier à travers les articles 10 et 13 de la Constitution fédérale⁹. La première de ces dispositions, l'article 10, qui garantit la liberté personnelle (« Droit à la vie et liberté personnelle »), protège en particulier, au titre de cette liberté, « l'intégrité physique et psychique » de toute personne, utilisant ainsi une terminologie à laquelle l'idée d'un « droit à l'*intégrité* numérique » fait écho. C'est du reste ainsi que semble le concevoir le constituant valaisan, qui estime que la « vie numérique doit être prise en compte dans le contexte de la protection des libertés individuelles, au même titre qu'une vie physique ou psychique »¹⁰.

Pour sa part, l'article 13, qui traite de la « Protection de la sphère privée », garantit tout d'abord le droit de toute personne « au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications » (art. 13 al. 1). S'y ajoute le droit de toute personne « d'être protégée contre l'emploi abusif des données qui la concernent » (art. 13 al. 2), disposition qui implique le droit à la protection des données (personnelles) et qui est concrétisée notamment par la loi fédérale du même nom¹¹.

⁶ Code civil suisse, du 10 décembre 1907 (RS 210).

⁷ Code pénal suisse, du 21 décembre 1937 (RS 311.0).

⁸ Voir, pour ce qui est du droit civil, la contribution de MARIE-LAURE PAPAUX VAN DELDEN, et, pour le droit pénal, celle d'ANDRÉ KUHN, toutes deux *infra*, dans cet ouvrage, pp. 65 et ss et 87 et ss.

⁹ Constitution fédérale de la Confédération suisse, du 18 avril 1999 (RS 101). On rappellera que les diverses garanties qu'instituent ces deux dispositions n'étaient, sous l'empire de l'ancienne Constitution fédérale et de la jurisprudence du Tribunal fédéral qui les avaient progressivement reconnues comme droits fondamentaux non écrits, pas séparées, mais au contraire regroupées sous l'égide de la « liberté personnelle » ; voir à ce propos MAHON, *Petit commentaire*, N 3 ad art. 10 et N 1 et 2 ad art. 13.

¹⁰ Voir le rapport, précité (note 1), de la Commission 2 *Droits fondamentaux et sociaux, société civile*, p. 5.

¹¹ Loi fédérale sur la protection des données, du 19 juin 1992 (RS 235.1).

5. On rappellera par ailleurs sans trop s'y arrêter que ces dispositions constitutionnelles « nationales » sont complétées par – ou plutôt complètent, devrait-on dire – plusieurs normes du droit international des droits fondamentaux, comme les articles 12 DUDH et 17 du Pacte ONU II, ainsi que 8 CEDH, dispositions dont la nouvelle Constitution fédérale s'est du reste, en partie au moins, largement inspirée¹².
6. Toutes ces dispositions garantissent, en fin de compte – au-delà des appellations et formulations diverses – un « droit à la protection de la sphère privée », à la « protection de l'intégrité physique et psychique » et, plus largement, à la « protection de la personnalité ». Ce droit implique notamment que nul ne peut faire l'objet d'immixtions arbitraires ou illégales dans sa vie privée, d'une part. Mais il signifie aussi que toute personne possède un « droit à l'autodétermination en matière informationnelle » (*informationelle Selbstbestimmung*)¹³, droit qui confère à l'individu une forme de maîtrise sur ses propres données personnelles¹⁴ : ou, pour reprendre une autre formulation du Tribunal fédéral, un droit qui permet à

¹² Pour un panorama très complet de ces normes de droit international, et des activités auxquelles elles ont donné lieu au sein des diverses organisations internationales (ONU, Conseil de l'Europe, OCDE, OSCE et Union européenne), cf. KAUFMANN et al., *Studie*, pp. 7-62.

¹³ Pour l'article 8 CEDH, selon la jurisprudence de la Cour européenne des droits de l'homme (ci-après Cour EDH), voir l'arrêt de la Grande Chambre du 27 juin 2017, en la cause *Affaire Satakunnan Markkainpörssi Oy et Satamedia Oy c. Finlande*, requête no 931/13, par. 137 : « L'article 8 de la Convention consacre donc le droit à une forme d'auto-détermination informationnelle, qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne des données qui, bien que neutres, sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits au titre de l'article 8 peuvent être mis en jeu ».

¹⁴ ATF 138 II 346 (Google Street View), c. 8.2, pp. 359-360 : « garantiert das verfassungsmässige Recht auf informationelle Selbstbestimmung [...], dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, dem Einzelnen die Herrschaft über seine personenbezogenen Daten zusteht ». Voir aussi ATF 140 I 381 (loi sur la police du canton de Genève), c. 4.1, p. 384 : « Dans le domaine de la protection des données, le droit à l'autodétermination en matière d'informations personnelles, consacré par la Constitution (art. 13 al. 2 Cst. et art. 8 CEDH), garantit que l'individu demeure en principe maître des données le concernant, indépendamment du degré de sensibilité effectif des informations en cause ».

toute personne de pouvoir déterminer elle-même, à l'égard de tout traitement de données qui la concerne (données personnelles) de la part de tiers, qu'ils soient publics ou privés, et en principe indépendamment de la question de savoir si les données en question sont effectivement sensibles, si et dans quels buts de telles données sont traitées¹⁵.

7. Il résulte de toutes ces dispositions une obligation pour l'Etat de protéger la sphère et la vie privées des individus, obligation qui porte sur le stockage, le traitement et la transmission des données personnelles, que ce soit par l'Etat lui-même ou par des entreprises privées. Ces dispositions constitutionnelles et internationales ont donc, dans une certaine mesure, un « effet horizontal », au moins indirect, en ce sens qu'elles obligent les pouvoirs publics à intervenir et à prendre des mesures, en particulier législatives, pour protéger les droits fondamentaux en question même contre les atteintes que pourraient leur porter d'autres particuliers¹⁶. En Suisse, la législation fédérale évoquée de protection des données concrétise cet effet horizontal (indirect) dans la mesure où elle s'applique non seulement aux traitements de données par des organes de

¹⁵ ATF 144 I 126 (Dienst Überwachung Post- und Fernmeldeverkehr), c. 4.1, p. 131 : « garantiert das verfassungsmässige Recht auf informationelle Selbstbestimmung, dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden ». Cf. aussi ATF 144 II 77 (Neuen Ereignisdatenbank), c. 5.2, p. 84 : « das Recht auf informationelle Selbstbestimmung [...] impliziert, dass jede Person gegenüber fremder, staatlicher oder privater Bearbeitung von sie betreffenden Informationen bestimmen können muss, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden ». Cf. encore, pour (pratiquement) la même formule, ATF 142 II 340 (Swissmedic), c. 4.2, pp. 346-347, ATF 140 I 2 (Konkordat über Massnahmen gegen Gewalt), c. 9.1, pp. 22-23, ATF 129 I 232 (Volksinitiative « Einbürgerungen vors Volk ! »), c. 4.3.1, p. 245. Sur l'émergence progressive de ce droit, au plan international comme au plan national, ainsi que sur les discussions relatives à son contenu, voir en particulier FLÜCKIGER, pp. 843-851.

¹⁶ Dans ce sens, par exemple, KAUFMANN et al., *Studie*, p. 70.

l'administration (fédérale¹⁷), mais aussi à ceux qu'effectuent des personnes privées¹⁸. Quoi qu'il en soit, la protection en question vaut, en principe, aussi bien pour le numérique que pour l'analogique, on ne fait à cet égard pas de différence *a priori*¹⁹.

8. Cette obligation « constitutionnelle » pour l'Etat de protéger la sphère et la vie privées des individus a du reste entraîné une grande activité régulatrice ou « législative », mais aussi jurisprudentielle, en la matière, et ce au plan international comme au plan national. Pour ce qui est de l'action régulatrice ou du moins promotrice, on peut mentionner, pour ne citer que quelques exemples – et sans prétention aucune à l'exhaustivité – divers règlements et directives de l'Union européenne, dont le fameux « RGPD », soit le *Règlement (UE) 2016/679 du Parlement européen et du Conseil, 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)*, du 27 avril 2016 (RGPD)²⁰, entré en vigueur en mai 2018, sur lequel on reviendra. On peut citer aussi diverses conventions et recommandations, notamment du Conseil de l'Europe, dont la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, du 28 janvier 1981²¹, qui ne fait, elle non plus, pas

¹⁷ On rappellera que la législation *fédérale* sur la protection des données ne s'applique pas aux traitements des données par des organes publics cantonaux, les cantons ayant leurs propres législations en la matière (cf. art. 2 al. 1 let. a LPD).

¹⁸ Art. 2 al. 1 let. a et b LPD, ainsi que 12 et ss, pour les personnes privées, 16 et ss, pour les organes fédéraux.

¹⁹ Voir par exemple, à ce propos, l'arrêt de la Cour EDH, déjà cité (note 13), en la cause *Affaire Satakunnan Markkiapörssi Oy et Satamedia Oy c. Finlande*, notamment par. 117 ; la Cour ne fait aucune différence entre « médias numériques » et médias traditionnels. De même, KAUFMANN et al., *Update*, p. 2.

²⁰ Journal officiel de l'Union européenne, L 119/1, 4.5.2016, <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679>.

²¹ Que la Suisse a ratifiée avec effet au 1^{er} février 1998 (RS 0.235.1), avec son Protocole additionnel, du 8 novembre 2001, ratifié avec effet au 1^{er} avril 2008 (RS 0.235.11) ; sur cette convention, voir notamment la contribution de JEAN-PHILIPPE WALTER, *infra*, dans cet ouvrage, pp. 95 et ss, N 6 et ss.

de différence entre le numérique et les traitements traditionnels, ainsi que des rapports spéciaux des Nations Unies²².

9. Pour ce qui est de la jurisprudence, on peut là aussi mentionner – toujours sans prétendre à l'exhaustivité – plusieurs arrêts tant de la Cour de justice de l'Union européenne (CJUE) que de la Cour européenne des droits de l'homme. Ainsi, par exemple, la première de ces cours²³ a reconnu en 2014 déjà une forme de « droit à l'oubli », via un droit à obtenir l'effacement des données personnelles des résultats d'un moteur de recherche²⁴. Plus récemment, en 2019, elle a même admis un droit au « déréférencement » plus étendu, même si, dans le même arrêt, elle a restreint le champ d'application extra-territorial du RGPD²⁵.

²² Voir par exemple le *Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique* (A/HRC/27/37), du 30 juin 2014 ; pour ce rapport, et les autres activités des Nations Unies, notamment du Conseil des droits de l'homme, à propos de cette thématique du « droit à la vie privée à l'ère du numérique », cf. la page dédiée sur le site de l'organisation, <https://www.ohchr.org/FR/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>.

Pour un examen détaillé et complet de toutes ces activités au plan international (ONU, Conseil de l'Europe, OCDE, OSCE et Union européenne), cf. KAUFMANN et al., *Studie*, pp. 7-62, ainsi que Kaufmann et al., *Update*, pp. 5-7.

²³ Pour les deux arrêts mentionnés ci-après dans le texte, et d'autres, notamment l'arrêt de la CJUE C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, du 3 octobre 2019, cf. KAUFMANN et al., *Update*, pp. 4-5.

²⁴ CJUE, arrêt (grande chambre) C-131/12, *Google Spain SL, Google Inc. contre Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, du 13 mai 2014, notamment par. 88 (<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62012CJ0131&from=FR>).

²⁵ CJUE, arrêt (grande chambre) C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés [CNIL]*, du 24 septembre 2019, dispositif : « L'article 12, sous b), et l'article 14, premier alinéa, sous a), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ainsi que l'article 17, paragraphe 1, du 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 (règlement général sur la protection des données), doivent être interprétés en ce sens que, lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application de ces dispositions, il est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur,

10. Quant à la Cour européenne des droits de l'homme, elle admet elle aussi, on l'a vu, que « [l]a protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article »²⁶. Elle souligne cependant qu'un « juste équilibre » doit être « ménagé entre », d'une part, le droit à la protection de la vie privée (et la protection des données), qui découle de l'article 8 CEDH, et, d'autre part, la liberté d'expression et la liberté de la presse, qui résultent, elles, de l'article 10 de la Convention et qui constituent des « fondements essentiels d'une société démocratique »²⁷. La Cour considère en effet que les droits que la Convention « consacre respectivement en ses articles 10 et 8 méritent un égal respect » et que, dès lors, « il y a lieu de ménager un équilibre qui préserve l'essence de l'un et l'autre de ces droits »²⁸.
11. Comme déjà indiqué (N 7 *in fine*), la protection qui résulte de ces dispositions « constitutionnelles », telles que mises en œuvre et concrétisées par les législateurs et les juges, tant « européens » que nationaux, vaut en principe aussi bien pour le numérique que pour l'analogique, elle ne fait *a priori* pas de différence. A vrai dire cependant, du moins selon certains auteurs, un changement de paradigme a eu lieu et peut être constaté avec l'avènement d'Internet

mais sur les versions de celui-ci correspondant à l'ensemble des Etats membres, et ce, si nécessaire, en combinaison avec des mesures qui, tout en satisfaisant aux exigences légales, permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des Etats membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens qui font l'objet de cette demande » ([http://curia.europa.eu/juris/document /document.jsf; jsessionid=7C31B91BD03E8046230053F87E4278E7?text=&docid=218105&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=11517714](http://curia.europa.eu/juris/document/document.jsf?jsessionid=7C31B91BD03E8046230053F87E4278E7?text=&docid=218105&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=11517714)).

²⁶ Arrêt déjà cité (note 13), en la cause *Affaire Satakunnan Markkainpörssi Oy et Satamedia Oy c. Finlande*, par. 137, avec, auparavant, un résumé de la jurisprudence de la Cour en la matière.

²⁷ *Ibidem*, par. 122 et 124.

²⁸ *Ibidem*, par. 123.

et du numérique, en ce sens que « [l]es tribunaux – emmenés par la Cour européenne des droits de l’homme – sont en train de rompre le délicat équilibre entre protection de la vie privée et de l’honneur d’une part, liberté de l’information d’autre part »²⁹, et ce au détriment de la liberté d’expression et d’information, ou de la liberté de la presse, et ce alors même que celles-ci, en tant que fondements de tout Etat démocratique, méritent ou méritaient dans la conception classique une place à part, privilégiée, dans le catalogue des droits fondamentaux³⁰.

12. Quoi qu’il en soit, il existe, on le voit, tant au plan international qu’en droit domestique, tout un arsenal de dispositions, constitutionnelles et légales, qui ont pour but et objet de garantir et de concrétiser le droit à la protection de la vie privée et son corollaire, le droit à la protection des données, ainsi que de protéger la personnalité, y compris et même dans le monde du numérique. Dans ce sens, il est permis de se demander si l’intégrité *numérique* n’est pas une simple extension, « spatiale », en quelque sorte, de l’intégrité physique et, surtout, de l’intégrité psychique. Si l’on s’en tient à sa définition classique, à savoir « ... la faculté humaine d’apprécier une situation et de se déterminer d’après cette appréciation », comme l’a rappelé Johan Rochel dans cet ouvrage³¹, la garantie de l’intégrité psychique protège tout individu à l’encontre de toute mesure étatique qui affecte sa capacité sensitive et cognitive (faculté de percevoir et de comprendre) et sa capacité volitive (capacité de décider ou de juger)³². On pourrait donc être tenté de concevoir l’intégrité numérique comme le prolongement de l’intégrité psychique en lien toutefois avec les technologies

²⁹ Voir, dans cet ouvrage, la contribution de BERTIL COTTIER, *infra*, pp. 103 et ss, N 15.

³⁰ Voir, dans cet ouvrage, la contribution de BERTIL COTTIER, *infra*, pp. 103 et ss, N 14. Sur la notion de liberté méritant « un traitement privilégié de la part des autorités », en raison du rôle qu’elle joue dans la démocratie, comme l’a dit le Tribunal fédéral dans l’arrêt *Aleinick*, en 1970 déjà (ATF 96 I 586), ou de liberté ayant une « position préférée », cf. notamment AUBERT, *Liberté d’opinion*, p. 441 ; sur la doctrine des « preferred freedoms », issue de la jurisprudence de la Cour suprême des Etats-Unis d’Amérique, cf., parmi beaucoup d’autres, EPSTEIN/WALKER, pp. 183 et ss, spécialement pp. 193-195.

³¹ Voir la contribution de JOHAN ROCHEL, *supra*, pp. 13 et ss, N 15.

³² *Ibidem*, N 15, avec des références à la jurisprudence du Tribunal fédéral.

numériques³³, et en conclure que le « droit à l'intégrité numérique » ne recouvre rien de nouveau, ou rien d'autre que ce qui existe déjà, sous l'angle de la liberté personnelle et du droit à la protection de la vie privée et de la protection des données. Du reste, c'est semble-t-il ainsi que le conçoit le Conseil fédéral, qui considère que le droit suisse en vigueur ne présente aucune lacune réglementaire majeure en matière de réseaux sociaux et de médias sociaux et qu'il n'y a dès lors pas de nécessité d'agir³⁴.

13. Dans le même sens, on pourrait sans doute aussi défendre le point de vue que l'inscription d'un nouveau « droit à l'intégrité numérique » n'est pas nécessaire, et n'apporterait pas de changement de fond, l'appareil juridique existant étant certainement susceptible d'offrir la protection souhaitée des droits fondamentaux de la personne confrontée au monde numérique, soit comme utilisatrice, soit comme objet des technologies numériques. En réalité, la réponse à la question posée dépend cependant de la signification et, surtout, du contenu que l'on veut donner à un tel « droit à l'intégrité numérique ».

III. La signification et le contenu d'un éventuel « droit à l'intégrité numérique »

A. L'« intégrité numérique » et ses caractéristiques

14. La relation entre « intégrité numérique », d'un côté, et intégrité(s) physique et psychique, de l'autre, mérite d'être soigneusement appréhendée d'un point de vue conceptuel. L'idée qu'une personne ait une « intégrité » – ou une vie – numérique à côté ou en dehors de son intégrité physique et de son intégrité psychique, et indépendamment de celles-ci, et au même niveau qu'elles, ne fait pas de sens. Comme le montre très bien Johan Rochel, « les expériences négatives que nous faisons par le biais d'activités

³³ Voir toutefois ROCHEL, cité note précédente, qui réfute de manière convaincante cette idée d'une « extension spatiale » de l'intégrité physique ou psychique (N 7 à 11), pour lui préférer celle d'une « extension fonctionnelle » (N 12 à 20).

³⁴ Voir à ce propos MÉTILLE, p. 38, qui se réfère à deux rapports du Conseil fédéral sur le sujet, de 2013 et 2017.

numériques n'impactent pas un moi numérique, elles impactent un esprit et un corps, ceux-là mêmes qui sont protégés par l'intégrité physique et psychique »³⁵. Dans ce sens, l'inscription d'un « droit à l'intégrité numérique » ne saurait être conçue comme la manifestation d'un nouveau droit matériel, mais bien plus comme un « outil » ou – pour reprendre son autre terme – un « vecteur pour signifier la spécificité des dangers liés aux technologies numériques, dangers qui pèsent sur l'intégrité physique et psychique des personnes »³⁶. Elle a donc pour fonction de « mettre en lumière de nouveaux dangers pour la personne humaine dans un contexte marqué par l'omniprésence de technologies numériques »³⁷.

15. Le monde du numérique présente en effet certaines caractéristiques particulières, ou des spécificités, qui distinguent les dangers qu'il recèle pour la protection de la personnalité des atteintes traditionnelles à l'intégrité physique ou psychique. Tout d'abord, alors que celles-ci ont le plus souvent un lien assez étroit avec la personne physique, ce qui les rend plus ou moins directement et immédiatement perceptibles par la personne en question³⁸, il en va différemment avec les technologies numériques. Les activités numériques, au moins celles dont un individu est l'objet, et leurs effets se développent dans un univers spatialement distinct et même très éloigné de cet individu, dans un « espace » où il n'est pas. En d'autres termes, il est généralement difficile, voire impossible, pour une personne, de savoir que des données la concernant sont traitées, de savoir de quelles données il s'agit, de connaître les auteurs ainsi que les buts et les modalités de ces traitements. Les atteintes

³⁵ Pour cette démonstration, voir la contribution de JOHAN ROCHEL, dans cet ouvrage, *supra*, pp. 13 ss, N 12 à 20, spécialement 17 (pour la citation).

³⁶ *Ibidem*, N 20.

³⁷ *Ibidem*, N 20 ; l'auteur, qui illustre en détail ces dangers nouveaux (N 21 à 28), reconnaît du reste lui-même que cette fonction pourrait « être remplie grâce à l'introduction d'un nouveau droit fondamental », mais qu' « elle pourrait également l'être sur la base de droits existants » (N 31).

³⁸ Tel est le cas, notamment, pour toutes les atteintes portées au corps (vaccinations, prélèvements divers, etc.) et, même, à l'intégrité psychique (sérums de vérité, détecteurs de mensonge, etc.) ; peut-être faut-il réserver les mesures de surveillance, encore que certaines – comme la surveillance par des personnes (détectives par exemple) – supposent elles aussi un lien spatial relativement étroit. Voir aussi, à ce propos, FLÜCKIGER, pp. 839-843, qui parle d' « abatement progressif des protections de fait » (p. 841).

potentielles à l'intégrité physique et psychique ainsi qu'à la personnalité sont donc très difficilement perceptibles ou reconnaissables, pour ne pas dire qu'elles ne le sont souvent pas du tout.

16. A cela s'ajoute que les potentialités du numérique sont marquées par une évolution technologique très rapide et une asymétrie de pouvoir et d'information très importante entre celles et ceux qui utilisent les services de la société numérique et celles et ceux qui les offrent et détiennent les données relatives à l'utilisation de ces services. Il en résulte qu'il est difficile de définir concrètement la sphère de protection (les biens protégés) et le contenu du droit à garantir, d'une part, mais qu'il est difficile également, d'autre part, d'assurer son application ou son respect, à l'égard de l'Etat, du secteur public, déjà, mais aussi et surtout à l'égard du secteur privé, des entreprises – généralement multinationales et souvent en situation de monopole – qui détiennent ces masses de données et les clés de leur croisement et de leur analyse. On retombe, là, sur la question de l'effet horizontal des droits fondamentaux, et même si l'on admet un effet horizontal indirect, c'est-à-dire une obligation, pour l'Etat, de protéger la personnalité et la sphère privées des individus (N 7 *supra*), force est de reconnaître que les Etats (nationaux) peinent à imposer ou obtenir le respect des règles qu'ils peuvent mettre en place.
17. Quoi qu'il en soit de ces difficultés liées à l'appréhension de la sphère protégée du droit et à l'effectivité de sa mise en œuvre, la question de savoir si l'introduction d'un éventuel « droit à l'intégrité numérique » représenterait une réelle innovation, de fond, dépend essentiellement du contenu que l'on veut donner ou que l'on accorderait à un tel « droit ».

***B. Le contenu (encore) incertain d'un éventuel
« droit à l'intégrité numérique »***

18. Or, à ce sujet, il faut bien dire que les indications données par celles et ceux qui prônent l'introduction d'un « droit à l'intégrité

numérique » sont souvent assez maigres ou floues³⁹, de sorte qu'il n'est pas aisé de déterminer quels seraient ou pourraient être le contenu et la portée matérielle – au moins souhaités – d'un tel droit. Pourtant, les questions de fond à résoudre – qui sont aujourd'hui en suspens, discutées ou controversées – sont nombreuses et importantes.

19. Un premier point, à mettre en évidence, est celui du lien entre un nouveau « droit à l'intégrité numérique » et celui, déjà reconnu par la jurisprudence, sous l'appellation « droit à l'autodétermination informationnelle ». Comme on l'a vu, les tribunaux ont en effet reconnu, dans le cadre du droit à la protection de la sphère privée, un « droit à l'autodétermination informationnelle », en le définissant comme un droit qui confère à toute personne une forme de maîtrise sur ses propres données personnelles ou un droit qui permet à toute personne de pouvoir déterminer elle-même, à l'égard de tout traitement de données qui la concerne, que ce soit par des entités publiques ou privées, et indépendamment du caractère sensible ou non des données en question, si et dans quels buts de telles données sont traitées (voir N 6 *supra*, avec des références). Or, même s'il semble ainsi défini de manière assez large et ambitieuse – ou généreuse, pour l'individu objet du traitement –, comme un droit de « maîtrise » de « tout ce que d'autres détiennent sur moi », ce droit n'a en réalité pas un contenu très clairement défini et sa portée prête à confusion ou à discussion. Et les tribunaux qui l'ont reconnu semblent plutôt procéder à tâtons, en reconnaissant de manière ponctuelle, certains aspects partiels d'un tel droit, sans jamais véritablement se prononcer de manière systématique sur l'essence même de ce droit⁴⁰.
20. Néanmoins, la question qui se pose – et qui devrait se poser – est celle de savoir si ce « droit à l'autodétermination informationnelle » implique un droit, pour la personne concernée, d'être informée que

³⁹ Ainsi, par exemple, le rapport, précité (note 1), de la Commission 2 *Droits fondamentaux et sociaux, société civile*, de l'Assemblée constituante valaisanne ne donne guère d'explications sur le contenu et les effets qu'aurait concrètement ce droit (p. 5).

⁴⁰ Peut-être parce qu'ils évitent – ou craignent – de (se) poser frontalement la question essentielle, ou peut-être simplement parce que leur fonction se limite à répondre aux (seules) questions concrètes dont ils sont saisis.

des données personnelles sont enregistrées, stockées et éventuellement utilisées, voire commercialisées, autrement dit un droit de savoir qui détient quoi sur elle, et dans quel but, de savoir quelles données et pour quelles utilisations, effectives ou potentielles, un droit allant jusqu'à, et surtout, un droit de consentir, ou non, au traitement et à l'utilisation de ces données. Plus concrètement, diverses questions se posent. Doit-on ou veut-on reconnaître un simple droit de faire rectifier les données erronées, et uniquement celles-là, ou s'agit-il plus largement d'un droit portant sur (toutes) les données personnelles en général ? un droit d'en limiter dans le temps le stockage et l'utilisation ? d'en obtenir l'effacement ou la suppression ? un droit à l'anonymat et à empêcher la ré-identification ? un droit de s'opposer à – ou d'interdire – la récolte, l'enregistrement, le stockage, le traitement et/ou l'utilisation ? ou encore un droit de déterminer ou d'autoriser si et dans quel but des données qui me concernent peuvent être conservées et traitées par des tiers, publics ou privés ?, etc.⁴¹.

21. La question est au fond celle de savoir si le « droit à l'autodétermination informationnelle » est simplement (et seulement) un droit à être protégé, comme le dit l'article 13 de la Constitution fédérale, « contre l'emploi *abusif* des données qui [me] concernent », ou s'il confère beaucoup plus largement, à toute personne, un droit de maîtrise, un droit de propriété en quelque sorte, sur toutes ses données personnelles. Autrement dit, faut-il, comme l'admettent certains, considérer que l'article 13 évoqué est mal rédigé, et qu'il conviendrait d'en supprimer le terme « abusif »⁴², ou, au contraire, comme le précisent d'autres, que ce terme est essentiel et doit subsister, sous peine de sacrifier la liberté

⁴¹ Voir, sur les divers droits spécifiques concrets que comprend le « droit à l'autodétermination informationnelle », FLÜCKIGER, pp. 852-853.

⁴² En ce sens, SCHWAAB, *Projet socialiste*, p. 31 : « L'art. 13 Cst. est mal rédigé, car, même si le droit à l'autodétermination a été consacré par la jurisprudence, une interprétation littérale ne protège que l'utilisation abusive et pas l'utilisation ordinaire des données personnelles. Le droit à la sphère privée doit donc être un vrai droit à l'autodétermination informationnelle (ou intégrité numérique), c'est-à-dire le droit de chacun d'autoriser si et dans quel but ses données peuvent être traitées ». Sur ce débat, avec d'autres références, cf. FLÜCKIGER, pp. 847-848.

d'expression et la liberté des médias sur l'autel de la protection des données⁴³.

22. Avec la reconnaissance, depuis une vingtaine d'années, d'un droit à l'autodétermination informationnelle qui couvre différents aspects, la jurisprudence, notamment du Tribunal fédéral, semble aller progressivement dans le sens d'une conception plus large que la seule protection contre l'emploi *abusif*, quoi qu'encre de manière hésitante et, comme indiqué, faite de touches ponctuelles. Le nouveau RGPD a lui aussi fait un (grand) pas en ce sens avec la reconnaissance d'un « droit à la portabilité des données », qui est une de ses nouveautés. Garanti par l'article 20 du Règlement, le droit à la portabilité des données doit permettre, pour l'utilisatrice ou l'utilisateur d'un service, « une possession effective de ses données »⁴⁴. Concrètement, la disposition⁴⁵ autorise un particulier à récupérer ses données personnelles auprès d'un opérateur ou fournisseur de services, dans un format lisible par machine, afin par exemple de les transmettre à un concurrent ou de les faire analyser⁴⁶.

⁴³ Dans ce sens, la contribution de COTTIER, dans cet ouvrage, *infra*, pp. 103 et ss, N 14 et ss. Dans sa contribution orale, lors du colloque, le professeur Cottier s'était explicitement opposé à l'idée de supprimer le terme « abusif » de l'art. 13 de la Constitution.

⁴⁴ Sur ce droit, et pour d'autres références, voir PERNOT-LEPLAY, ch. 1.1, qui précise que l'utilisateur « n'est plus « prisonnier » d'un service qu'il ne pourrait quitter sans abandonner son historique, ses préférences et autres jeux d'information battis (sic) au fil du temps ».

⁴⁵ L'art. 20 ch. 1 RGPD a la teneur suivante : « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle lorsque a) le traitement est fondé sur le consentement en application de l'art. 6, par. 1, point a), ou de l'art. 9, par. 2, point a), ou sur un contrat en application de l'art. 6, par. 1, point b) ; et b) le traitement est effectué à l'aide de procédés automatisés ». Le chiffre 2 ajoute que la personne concernée a aussi « le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible ».

⁴⁶ PERNOT-LEPLAY, Introduction et ch. 1.1, qui précise : « En pratique, on pourra passer de Spotify à Deezer, ou de Gmail à Protonmail, d'une application de santé ou de sport à une autre, sans y perdre ses données. Ce droit existe déjà pour les

On admet donc que ce droit porte concrètement sur trois aspects, ou « trois droits en un » : le « droit pour un individu de recevoir les données qu'il a partagées avec un responsable du traitement », le « droit de transmettre les données d'un responsable du traitement à un autre » et le « droit d'avoir les données personnelles transmises directement d'un responsable du traitement à un autre »⁴⁷. En d'autres termes, ce nouveau droit à la portabilité des données « renforce la propriété d'un individu sur ses données, à la croisée des chemins entre la protection des données personnelles et le droit de la concurrence ou de la propriété intellectuelle »⁴⁸. Il a de fait aussi pour objectif, ou pour effet, de stimuler une certaine forme de concurrence entre les responsables des traitements et d'instaurer ou de rétablir par voie de conséquence une certaine forme d'équilibre – ou de rééquilibrage – entre personnes concernées (« propriétaires » des données) et (entreprises) responsables du traitement.

23. Indépendamment de l'évolution qui se dessinera encore dans ce domaine – notamment en droit suisse – la question qui se pose, dans notre contexte, est celle de savoir si la reconnaissance d'un « droit à l'intégrité numérique » a ou aurait pour ambition, contenu et/ou effet, d'accentuer encore ce passage d'un droit, « défensif » en quelque sorte, de protection contre l'emploi *abusif* des données personnelles, à un droit beaucoup plus large, de maîtrise, ou de propriété, sur les données personnelles⁴⁹.
24. Dans un contexte différent, une autre question liée à la reconnaissance d'un éventuel « droit à l'intégrité numérique » est celle de conférer aussi à ce droit, en plus de son aspect de droit de protection de la personnalité ou de droit d'auto-détermination en matière de données personnelles, un contenu positif, le rapprochant des droits sociaux ou des « droits-créances ». Une telle composante

numéros de téléphones : la portabilité de votre numéro (une donnée personnelle) entre différents opérateurs est effective depuis plusieurs années ».

⁴⁷ PERNOT-LEPLAY, ch. 1.2.

⁴⁸ PERNOT-LEPLAY, ch. 1.2.

⁴⁹ Pour la reconnaissance plus large du « droit à l'autodétermination informationnelle », comme « droit de propriété *sui generis* », cf. FLÜCKIGER, pp. 853-864, spécialement pp. 858 et ss.

pourrait comprendre différents volets, qu'il appartiendrait à l'Etat de garantir, comme un droit d'accès à l'espace numérique (par la mise à disposition et l'entretien de l'infrastructure technique nécessaire, dans des conditions d'égal accès pour toutes et tous), un droit à la sécurité dans cet espace (notamment un droit d'être protégé contre le cyber-harcèlement), ou encore un droit à la formation ou à l'éducation numérique, de manière notamment à éviter la « fracture digitale »⁵⁰, voire un droit à ne pas devoir participer au monde numérique (droit à une vie « hors ligne » ou droit à un « monde analogique »)⁵¹.

IV. Conclusion

25. On le voit au travers des quelques éléments de réflexion qui précèdent, les potentialités de la reconnaissance d'un éventuel nouveau « droit à l'intégrité numérique », sous forme de droit fondamental, c'est-à-dire de droit inscrit dans le catalogue des droits fondamentaux, sont nombreuses et diverses. Savoir si un tel droit constituerait une « réelle innovation ou une simple évolution du droit » ne peut être déterminé *a priori*, dans l'abstrait. Cela dépend(ra) de la question de savoir ce que l'on veut protéger, c'est-à-dire du contenu concret et de la portée que l'on entend donner à ce nouveau droit, d'une part. Or, l'impression est que ce contenu et cette portée ne sont, à ce stade, pas (encore) entièrement clairs. Et, de ce point de vue, on aurait tendance à dire, en conclusion, que savoir si l'introduction d'un tel droit constituerait une « réelle innovation ou une simple évolution du droit » n'est finalement pas très important. Le contenu nous paraît plus important que la forme : autrement dit, savoir ce que l'on veut protéger, et comment ou jusqu'où, semble plus important que savoir si on le fait à travers – et en développant – les instruments (et droits) existants ou par l'introduction d'un nouveau droit fondamental. Cela même si – et sans oublier que – l'introduction d'un nouveau droit fondamental a

⁵⁰ Sur ces différents aspects, cf. SCHWAAB, *Projet socialiste*, pp. 23 et 29-30, 31 et 35-37 ; de même, la contribution de ROCHEL, *supra*, dans cet ouvrage, pp. 13 et ss, N 43 et 44.

⁵¹ SCHWAAB, *Projet socialiste*, pp. 23 et 29.

ou aurait aussi une signification ou une valeur symbolique, potentiellement dynamisante.

26. La réponse à la question posée dépend(ra) aussi, d'autre part, de ce que l'on peut effectivement protéger, notamment en termes de possibilités et de limites de l'action et de la portée du droit national des droits fondamentaux, qu'ils soient cantonaux et/ou fédéraux, notamment à l'égard de l'activité, multinationale et globale, d'entreprises privées, principales détentrices des données concernées. A cet égard, l'idée même de vouloir introduire un nouveau droit fondamental, un « droit à l'intégrité numérique », n'est pas sans raviver le souvenir de ce que disait le regretté Andreas Auer, à propos du paradoxe entourant souvent la reconnaissance des droits fondamentaux en général, à savoir que les droits fondamentaux sont garantis au moment où on commence à – et pour permettre de mieux – les restreindre.

Bibliographie

AUBERT JEAN-FRANÇOIS, La liberté d'opinion, RDS 1973 I, pp. 429-450

AUBERT JEAN-FRANÇOIS/MAHON PASCAL, Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999, Zurich/Bâle/Genève, 2003

BARBEY GRÉGOIRE, Les données personnelles ne sont la propriété de personne, En réponse à la chronique de Philippe Nantermod dans Le Temps intitulée « Données, c'est données, reprendre c'est voler », L'Affranchi, 9 avril 2019 (www.affranchi.ch)

CHARLET FRANÇOIS, Le Data Protection Officer dans le secteur privé suisse, Jusletter 18 juin 2018

EPSTEIN LEE/WALKER THOMAS G., Constitutional Law for a Changing America, Rights, Liberties, and Justice, 10^e éd., Washington D.C., 2019

FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, PJA 2013/6, pp. 837-864

KAUFMANN CHRISTINE/GHIELMINI SABRINA/MEDICI GABRIELA/PULVER FANNY, Das Recht auf Privatsphäre im digitalen Zeitalter, Staatliche Schutzpflichten bei Aktivitäten von Unternehmen, Studie SKMR, 22 septembre 2016, https://www.skmr.ch/cms/upload/pdf/160922_SKMR-Studie_Privatsphaere.pdf (cité : KAUFMANN et al., *Studie*)

KAUFMANN CHRISTINE/GHIELMINI SABRINA/MEDICI GABRIELA/PULVER FANNY, Das Recht auf Privatsphereim digitalen Zeitalter – Staatliche Schutzpflichten bei Aktivitäten von Unternehmen, Update zur SKMR-Studie vom 22. September 2016, 12 février 2020, https://www.skmr.ch/cms/upload/pdf/2020/200107_Privatsphaere_Formatiert_DEF.pdf (cité : KAUFMANN et al., *Update*)

MÉTILLE SYLVAIN, Le droit au respect de la vie privée : les défis digitaux, Une perspective de droit comparé, Suisse, Etude, Service de recherche du Parlement européen, Bruxelles, Union européenne, octobre 2018, https://serval.unil.ch/resource/serval:BIB_25D40801BCE2.P001/REF

PERNOT-LEPLAY EMMANUEL, Le droit à la portabilité des données dans le RGPD, Etude en ligne, 25 mai 2018, <https://pernot-leplay.com/fr/droit-portabilite-des-donnees-rgpd/#more-258>

SCHWAAB JEAN-CHRISTOPHE, Un projet socialiste pour faire face à la révolution numérique, août 2018, document pdf abrité sur le site de l'auteur, avec un résumé, du 5 mars 2019, <https://www.schwaab.ch/archives/2019/03/05/quelques-propositions-socialistes-pour-faire-face-a-la-revolution-numerique/#content>

Le « droit à l'intégrité numérique » du point de vue de la protection de droit civil de la personnalité

par

Marie-Laure Papaux van Delden*

Professeure à l'Université de Genève

I. Introduction.....	66
II. Brève historique et mise en perspective.....	66
A. Codification de la protection de la personnalité.....	67
B. Caractéristiques des droits de la personnalité	69
C. Mise en œuvre des droits fondamentaux.....	70
III. Question centrale et définition	72
IV. Des « biens » aux « droits » de la personnalité.....	73
V. Protection interne de la personnalité.....	77
VI. Protection externe de la personnalité	78
A. Actions défensives	79
B. Actions réparatrices.....	81
VII. Conclusion	82
Bibliographie	84

* Avec les remerciements à Guillaume Brulhart, étudiant-stagiaire, pour son aide à la rédaction de l'article.

I. Introduction

1. « Le droit à l'intégrité numérique est-il une innovation ou une extension de la personnalité civile ? » Telle est la question qui nous a été posée sous l'angle du droit civil relatif à la protection de la personnalité lors de la Journée organisée par la Faculté de droit de l'Université de Neuchâtel le 21 février 2020. Le droit à l'intégrité numérique n'est qu'aux prémices de son histoire et cette Journée de réflexion peut être saluée pour son caractère innovateur. Le fondement de notre réflexion, nouvelle à défaut de pouvoir reposer à ce jour sur nombre d'auteurs ou d'idées publiées, se basera sur le Code civil, plus particulièrement les art. 27 ss CC.
2. En droit civil, lorsque l'intégrité numérique est traitée, ou à tout le moins l'un de ses aspects, l'approche privilégiée est essentiellement celle de la protection des données, sujet couvert par une autre intervention et que nous n'aborderons que marginalement.
3. L'absence de source est un écueil mais, sans aucun doute, un atout également. Il faut oser une approche innovatrice ou à tout le moins offrir un regard différent sur un sujet nouveau et complexe.
4. Après quelques regards sur le passé et une mise en perspective de la thématique (II), nous aborderons la question centrale des outils du droit civil pour protéger la personne contre des atteintes à sa personnalité, ce qui impliquera d'en saisir la définition (III) ; nous poursuivrons l'analyse sur l'évolution des « biens » aux « droits » de la personnalité (IV), suivie des atouts tirés de la protection de la personnalité, fondée sur la dimension interne (V) puis externe (VI) de celle-ci, telles que consacrées au sein des normes du Code civil, avant de proposer une conclusion tendant à répondre à la question posée (VII).

II. Brève historique et mise en perspective

5. Il faut revenir aux sources pour comprendre les fondements du droit civil protégeant la personnalité, soit la vision initiale du législateur, qui permet de dessiner l'avenir. En ce sens, le passé nous guide vers l'avenir.

A. Codification de la protection de la personnalité

6. La codification de la protection de la personnalité en droit suisse, pierre angulaire du droit helvétique, commence dès le début du XX^e siècle. L'introduction dans le Code civil de 1907 des art. 27 et 28 CC fut particulièrement remarquée¹. Les droits de la personnalité sont, de par leur essence, liés aux développements économiques, techniques et sociaux. L'évolution dans ces domaines étant constante, les droits de la personnalité n'ont cessé de croître et de se réinventer avec le temps. Le législateur a laissé à dessein une place importante au juge et la protection de la personnalité est souvent la résultante d'une pesée des intérêts effectuée par l'autorité judiciaire, dont le pouvoir est considérable, même si le résultat n'est jamais certain. Telle a été la volonté du législateur, déjà en 1907, lequel tenait à ce que le droit de la personnalité soit suffisamment malléable pour pouvoir s'adapter aux évolutions sociétales.
7. La modification de l'art. 28 CC, entrée en vigueur le 1^{er} juillet 1985, n'a pas remis en cause les fondements de cette disposition². En effet, la nouvelle précisait et développait de manière substantielle les moyens de droit à disposition du lésé, tout en conservant à l'art. 28 CC son caractère de norme générale et abstraite, terreau fertile de développement.
8. Il n'en demeure pas moins que le conflit des intérêts en présence peut être tel qu'il nécessite une intervention législative. En effet, la grande flexibilité de l'art. 28 CC pose parfois des problèmes en pratique, étant donné que l'attente d'arrêts jurisprudentiels sur un point par hypothèse disputé, ainsi que leur aspect nécessairement ponctuel, ne suffisent pas à répondre correctement aux enjeux posés. Le domaine de la protection des données est emblématique à cet égard, la nécessité d'une réglementation plus précise ayant

¹ BUCHER, N 389. Voir également : GUILLOD, 2007.

² RO 1984 778 ; FF 1982 II 661. CR CC I-JEANDIN, art. 28 N 3 ; MEIER/DE LUZE, N 729 ; MEIER, N 45.

poussé le législateur à adopter la LPD, qui est par ailleurs déjà dépassée et en révision totale³.

9. La protection de l'intégrité physique et psychique a également amené de nombreux développements législatifs, en particulier l'entrée en vigueur au 1^{er} juillet 2007 de l'art. 28*b* CC ; cette disposition, que le Parlement a renforcée en date du 14 décembre 2018⁴, concrétise les moyens généraux de protection de l'art. 28*a* CC en matière de violence, menaces et harcèlement. Afin de protéger l'intégrité corporelle de certaines atteintes, liées notamment au risque d'exploitation et d'abus découlant de l'utilisation de technologies biomédicales, de nombreuses lois spéciales permettent aujourd'hui de concrétiser et compléter la protection générale de la personnalité, à l'instar de la Loi fédérale relative à la recherche sur l'être humain du 30 septembre 2011⁵, et de celle sur l'analyse génétique humaine du 8 octobre 2004, qui est l'objet d'une révision totale votée le 15 juin 2018⁶. Une tendance du législateur à la « décodification » peut être constatée depuis deux décennies en faveur de lois spéciales⁷.
10. La force des art. 28 ss CC est de conserver une dimension spécifique, le droit de la protection des données l'illustrant. En effet, la LPD, à son art. 2 al. 2, exclut exhaustivement de son champ d'application plusieurs traitements, dont les données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers (let. a), alors que

³ Loi fédérale sur la protection des données du 19 juin 1992, entrée en vigueur le 1^{er} juillet 1993 (LPD ; RS 235.1). Sur la révision totale de la LPD : FF 2017 6565 ss, Message du 15 septembre 2017, et FF 2017 6803 ss, 6815 ss, Projet de loi.

⁴ RO 2007 137 ; FF 2005 6437 6461. Sur la révision de l'art. 28*b* CC : FF 2017 6913 ss, Message du 11 octobre 2017, et FF 2018 7875 ss, Texte de loi voté.

⁵ Loi fédérale entrée en vigueur le 1^{er} janvier 2014 (LRH ; RS 810.30).

⁶ Loi fédérale entrée en vigueur le 1^{er} avril 2007 (LAGH ; RS 810.12) ; sur sa révision totale : FF 2018 3627 ss, Texte de loi voté, et FF 2017 5253, Message du 5 juillet 2017. Pour d'autres exemples : Loi fédérale sur la transplantation d'organes, de tissus et de cellules du 8 octobre 2004, entrée en vigueur le 1^{er} juillet 2007 (Loi sur la transplantation ; RS 810.21) ; Loi fédérale sur les conditions et la procédure régissant la stérilisation de personnes du 17 décembre 2004, entrée en vigueur le 1^{er} juillet 2005 (Loi sur la stérilisation ; RS 211.111.1).

⁷ GUILLOD, 2007, p. 146 ss ; MEIER/DE LUZE, N 564.

les art. 28 ss CC demeurent applicables comblant ce mitage de la protection. Ainsi, les atteintes à la personnalité nées d'un traitement de données qui n'est pas régi par la LPD, comme un agenda ou une lettre égarée dont un tiers prend connaissance, peuvent être saisies par les moyens du droit général de la personnalité⁸. De même, l'anonymisation des données empêche l'application de la LPD, étant donné que celle-ci se rapporte aux données d'une personne identifiée ou identifiable selon l'art. 3 let. a LPD ; les données pseudonymisées échappent ainsi à la LPD lorsque la ré-identification par un tiers ne paraît objectivement possible que moyennant des efforts qui paraissent disproportionnés⁹, alors que les art. 28 ss CC demeurent applicables. La reconnaissance de l'intégrité numérique ne saurait ainsi être traitée exclusivement sous l'angle de la protection des données.

11. C'est dans ce contexte que s'insère la discussion portant sur le droit à l'intégrité numérique en tant qu'éventuel droit relevant de la protection générale de la personnalité à défaut, à tout le moins à ce jour, de lois spéciales.

B. Caractéristiques des droits de la personnalité

12. Dès l'origine, les droits de la personnalité sont caractérisés par leur double aspect. Le premier, qualifié de défensif, correspond au pouvoir discrétionnaire de la personne dans ses rapports avec les tiers. Toute personne a une obligation d'abstention de porter atteinte aux droits de la personnalité d'autrui, qui ont un caractère absolu, opposable à chacun. Cette protection contre les atteintes des tiers est concrétisée aux art. 28 ss CC.
13. Le deuxième aspect concerne la maîtrise de la personne sur elle-même, soit le droit à l'autodétermination. Les droits de maîtrise permettent à leur titulaire de jouir d'un bien à l'exclusion de toute autre personne, sans signifier pour autant que les droits de la personnalité soient illimités. Le droit à l'autodétermination permet à la personne capable de discernement, même privée de l'exercice des droits civils, les droits de la personnalité étant des droits

⁸ AEBI-MÜLLER, 2005, N 555 ; BUCHER, N 466 ; MEIER, N 385.

⁹ ATF 138 II 346, c. 6.1 et 6.5/JdT 2013 I 71. MEIER, N 447.

strictement personnels (cf. art. 19c CC), de prendre des décisions contraires à ses intérêts, que doivent respecter les tiers. Il existe néanmoins des limites aux restrictions excessives qu'accepterait la personne, en particulier l'art. 27 al. 2 CC (cf. *infra* n. 37).

14. Le droit à l'autodétermination en matière de données personnelles a fait couler beaucoup d'encre. En doctrine, il est critiqué jusqu'à remettre en cause sa pertinence même à l'ère numérique, en raison de la perte par l'individu de la maîtrise des données le concernant¹⁰. Le droit à l'autodétermination informationnelle est pourtant un droit fondamental déduit de l'art. 13 al. 2 Cst.¹¹ ; il est également développé par la Cour européenne des droits de l'homme sur la base de l'art. 8 CEDH, le pouvoir innovateur de la jurisprudence strasbourgeoise pouvant être particulièrement relevé en la présente matière (cf. *infra* n. 20)¹².
15. Reconnaître à l'intégrité numérique la qualité de droit de la personnalité lui permettrait de jouir des caractéristiques essentielles de ces droits, à savoir être un droit strictement personnel, absolu, inaliénable et extra patrimonial¹³.

C. Mise en œuvre des droits fondamentaux

16. La protection de la personnalité tend à assurer l'épanouissement de l'individu et la protection des biens essentiels de la personne (cf. *infra* n. 22) ; elle est également assurée par les droits fondamentaux, lesquels s'appliquent aux relations entre particuliers à travers les règles du Code civil. La protection de la personnalité est le corollaire nécessaire de la liberté de la personne d'organiser sa vie privée et sociale ; il appartient au droit d'en fixer les limites tout

¹⁰ FLÜCKIGER, p. 853 ss pour une analyse des critiques doctrinales et plaidant pour la reconnaissance d'un droit constitutionnel de propriété *sui generis* sur ses données personnelles. Sur des adaptations et mesures pour pallier les défauts du droit à l'autodétermination : AEBI-MÜLLER, 2005, p. 286 ; BRUNNER, N 36, 51 et ch. VI.

¹¹ ATF 138 II 346, c. 8.2.

¹² ACEDH GC *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, du 27 juin 2017, n° 931/13, Affaire phare 2017, § 137.

¹³ Sur ces caractéristiques des droits de la personnalité : BUCHER, N 480 ss ; GUILLIOD, 2018, N 137 ss ; MEIER/DE LUZE, N 568 ss.

en sauvegardant la liberté de la personne à l'encontre des interventions d'elle-même ou de tiers¹⁴.

17. La personnalité est protégée par le droit fondamental à la liberté personnelle, consacré à l'art. 10 al. 2 Cst., qui est étroitement lié au droit à la vie (cf. art. 10 al. 1 Cst.). La liberté personnelle comprend notamment l'intégrité physique et psychique. Si le droit civil sur la protection de la personnalité constitue une mise en œuvre importante du droit constitutionnel à la liberté personnelle dans les relations entre particuliers¹⁵, inversement les règles de droit privé peuvent inspirer la détermination du contenu et de l'étendue de la liberté personnelle¹⁶ ; une influence réciproque s'exerce entre les principes résultant des art. 28 ss CC et ceux issus de la liberté personnelle¹⁷. Il est ainsi concevable que le juge civil, saisi par un demandeur faisant valoir une atteinte à son droit à l'intégrité numérique, reconnaisse ce bien de la personnalité (cf. *infra* n. 29), ce qui influencerait partant les contours des droits fondamentaux. Il pourrait lui revenir de précéder le législateur constitutionnel.
18. A cet effet, des initiatives tendent à la reconnaissance d'un droit fondamental à l'intégrité numérique. Les travaux de la Constituante valaisanne présentés lors de la Journée neuchâteloise ouvrent cette voie, reconnaissant « Tout être humain a droit à son intégrité numérique », après la consécration incontestée du droit à l'intégrité physique et psychique ; des initiatives politiques récentes vont dans une direction similaire¹⁸.
19. L'intégration du droit à l'intégrité numérique au niveau constitutionnel est un symbole fort et offre une base solide à l'œuvre jurisprudentielle et législative, en mettant en évidence les défis et dangers qui pèsent sur les libertés individuelles et nécessitent un

¹⁴ BUCHER, N 391.

¹⁵ ATF 113 Ia 262 ; ATF 107 Ia 277, 280.

¹⁶ ATF 106 Ia 28, 32 ; ATF 102 Ia 516, 521. BUCHER, N 386.

¹⁷ BUCHER, N 386.

¹⁸ Le Temps, 26 juin 2020, p. 6 : Le PLR genevois veut protéger l'intégrité numérique en lançant une initiative constitutionnelle cantonale pour un droit à la sauvegarde de l'intégrité numérique en demandant l'ajout, dans la Constitution genevoise, d'un alinéa à l'article sur la protection de la sphère privée. Voir en 2015 déjà la prise de position du PS suisse sur Internet, cf. https://www.sp-ps.ch/sites/default/files/documents/internet_verabschiedet_d_0.pdf.

cadre juridique clair. La reconnaissance d'un droit fondamental permet d'exiger une protection, notamment contre la récupération et l'utilisation des données, y compris le nom, contre le piratage en promouvant la sécurité numérique, contre la traçabilité et les garde-fous qu'il convient de respecter, comme le débat sur l'application de traçage de contact SwissCovid a mis en évidence. Reconnaître le droit à l'intégrité numérique permet par ailleurs également de protéger la liberté négative, à savoir celle de ne pas être connecté, de fuir le développement de ce qui est aussi dénoncé comme un esclavagisme numérique.

20. Les droits de la personnalité consacrés par le droit civil étant une mise en œuvre, une concrétisation, des droits fondamentaux entre personnes privées, cela signifie également que s'il est déduit de l'art. 8 CEDH un droit à l'intégrité numérique, celui-ci pourra emporter l'obligation positive pour les Etats de protéger, notamment par le biais de leur législation, cette intégrité des atteintes perpétuées entre personnes privées. Les particuliers peuvent en outre être fondés à invoquer l'art. 8 CEDH lorsque les tribunaux n'ont pas suffisamment protégé leur droit de la personnalité¹⁹. C'est également une manière forte de faire valoir un nouveau droit à l'intégrité numérique.

III. Question centrale et définition

21. La question centrale en droit civil est de déterminer comment le droit protège une personne contre des atteintes aux biens, qui lui sont propres en tant que sujet de droit.
22. La réponse amène à définir ces biens et partant à expliciter la notion de la personnalité, dont les textes légaux ne donnent pas de définition. Il est admis que la personnalité, au sens de l'art. 28 CC, est l'ensemble des biens ou valeurs qui appartiennent à une personne du seul fait de son existence²⁰. Elle englobe ainsi les attributs ou biens essentiels de la personne.

¹⁹ MEIER/DE LUZE, N 567 *in fine*.

²⁰ BSK ZGB-MEILI, art. 28 N 5 ; CR CC I-JEANDIN, art. 28 N 14 ; BUCHER, N 384 ; GUILLOD, N 134 ; STEINAUER/FOUNTOLAKIS, N 486.

23. En d'autres termes, les « droits de la personnalité » peuvent être définis comme des droits destinés à protéger tout ce qui sert à individualiser une personne et qui est digne de protection au regard des besoins de relations entre les individus (cf. *infra* n. 26)²¹.
24. Etant donné l'importance, toujours croissante, de la technologie au sein de notre société, son impact sur la vie de chaque personne, y compris sur la vie intime, il nous paraît fondé de reconnaître que l'intégrité numérique a acquis le statut d'attribut essentiel de l'être humain qui exige une protection privilégiée contre toute atteinte.
25. Des témoignages de personnes sans domicile fixe (SDF) ont démontré que leur plus grand manque était celui d'être connectées et l'inquiétude sur la fracture numérique qui menace les personnes en situation d'exclusion a mené à des études portant sur l'inclusion numérique des sans-abri²². Il a pu être constaté que 91% des personnes SDF sont équipées d'un téléphone mobile et 71% d'un smartphone, outil devenu indispensable dans leur quotidien. L'accès au numérique tend à être considéré comme un besoin primaire, apte à bouleverser la pyramide de Maslow, représentation de la hiérarchie des besoins.

IV. Des « biens » aux « droits » de la personnalité

26. Pour chaque bien de la personnalité correspond un droit de la personnalité, qui concrétise la protection accordée par le Code civil à la personnalité²³. A l'intégrité corporelle correspond ainsi le droit à l'intégrité corporelle, comme à l'honneur, le droit à l'honneur par exemple. Partant, admettre que l'intégrité numérique est un bien de la personnalité, un attribut essentiel de la personne, implique qu'un droit à l'intégrité numérique est protégé par les art. 28 ss CC.
27. Comme tout bien de la personnalité, l'intégrité numérique doit être circonscrite par l'œuvre jurisprudentielle et, le cas échéant, par le

²¹ ATF 70 II 127/JdT 1945 I 24. GUILLOD, 2018, N 142 ; STEINAUER/FOUNTOLAKIS, N 513.

²² Cf. <http://www.solinum.org/precarite-connectee-6-recommandations-pour-linclusion-numerique-des-sans-abri/> avec des liens qui mènent à l'Etude sur la Précarité connectée et à un livret sur Comment les personnes sans-abri utilisent-elles le numérique ?

²³ CR CC I-JEANDIN, art. 28 N 15 ; BUCHER, N 431 ; MEIER/DE LUZE, N 565.

législateur par le biais de lois spéciales. Ses contours peuvent d'ailleurs varier d'une personne à l'autre, à l'instar du contenu de la vie privée qui n'est pas le même par exemple pour une personnalité publique. De manière similaire, dans la mesure où différents aspects de la liberté personnelle entrent en conflit, il appartient au droit ordinaire de les concrétiser par une pesée et une coordination appropriée, la question ne pouvant être résolue par la simple définition du champ d'application de la liberté fondamentale²⁴.

28. Si l'appartenance de la vie et de l'intégrité physique aux biens de la personnalité est un acquis, il n'en demeure pas moins que la définition du début de la vie, comme celle de sa fin, est des plus complexe et que la consécration de l'intégrité physique ne résout par exemple pas la problématique du don d'organes, laquelle doit néanmoins être interprétée à la lumière de l'appartenance de l'intégrité physique au bien de la personnalité ; la complexité de cette question a d'ailleurs poussé le législateur à légiférer (cf. la Loi fédérale sur la transplantation *supra* note 6).
29. Il convient de souligner qu'il n'existe pas en droit suisse de *numerus clausus* des droits de la personnalité²⁵. Le législateur, dès 1907, a renoncé à introduire dans la loi une énumération, même non exhaustive, des droits protégés. Selon l'élégante formule de Grossen : « cette réglementation n'est exhaustive que par sa généralité »²⁶. La formulation de l'art. 28 CC se veut partant très ouverte ; norme générale et abstraite, elle permet la naissance de nouveaux droits, tels que le droit à la connaissance de ses origines²⁷ et le droit à l'image, dont l'importance lui a permis de devenir autonome²⁸, alors qu'il était initialement protégé indirectement sous l'angle de la sphère privée. L'art. 28 CC est ouvert à une interprétation suffisamment souple pouvant s'adapter aux évolutions de la société ainsi qu'aux nouveaux enjeux et défis en

²⁴ ATF 133 I 110, c. 5.2.3.

²⁵ ATF 95 II 481, c. 6/JdT 1971 I 226. CR CC I-JEANDIN, art. 28 N 23 ; BUCHER, N 435.

²⁶ GROSSEN, p. 18a, formule citée dans l'ATF 95 II 481, c. 6.

²⁷ ATF 134 III 241/JdT 2009 I 411 ; ATF 128 I 63.

²⁸ ATF 138 II 346, c. 8.2 ; ATF 127 III 481, c. 3a/SJ 2001 I 554.

découlant²⁹. Ainsi, le droit de la personnalité est façonné, en grande partie, par l'œuvre jurisprudentielle qui a, dans ce domaine tout particulièrement, une force éminemment créatrice, le juge civil pouvant ouvrir la voie à la reconnaissance d'un droit à l'intégrité numérique (cf. *supra* n. 17).

30. Poursuivant un but didactique, la doctrine tente de classer les biens de la personnalité en différentes catégories, classifications dont la valeur reste relative, tant elles sont en partie insatisfaisantes, voire arbitraires³⁰. Les distinctions portent sur les biens de la personnalité physique, tels que la vie, l'intégrité corporelle, physique ou psychique, les biens de la personnalité affective, soit les relations avec les personnes proches, dont le sentiment de pitié envers le proche décédé, les biens de la personnalité sociale, comprenant notamment le respect de la vie privée, particulièrement bousculée à l'ère numérique, l'image, la voix, les données personnelles³¹.
31. Se pose la question conceptuelle du rattachement de l'intégrité numérique à l'une de ces catégories. Or, cet aspect de l'intégrité peut être incorporé tant à la personnalité sociale, le respect de la vie privée et des données personnelles y étant inclus, qu'à la personnalité affective et physique.
32. Force est de constater que la protection la plus forte est accordée aux biens de la personnalité physique, en particulier à la vie, composante la plus précieuse et fondamentale³² ; de la vie découle la jouissance de l'entier des droits de la personnalité. C'est d'ailleurs en priorité dans le domaine médical que la jurisprudence a développé le principe de la qualité requise du consentement, soit libre et éclairé, pour permettre de justifier une atteinte à l'intégrité physique, exigence reprise par le législateur³³. La qualité du

²⁹ ATF 95 II 481, c. 6/JdT 1971 I 226. GUILLOD, 2018, N 142 ; MEIER/DE LUZE, N 563 ; WERRO, p. 15 ss.

³⁰ ATF 134 III 241/JdT 2009 I 411. AEBI-MÜLLER, 2002, p. 99 ss ; BUCHER, N 439 ; STEINAUER/FOUNTOULAKIS, N 515.

³¹ Sur ces catégories : BSK ZGB-MEILI, art. 28 N 17 ; CR CC I-JEANDIN, art. 28 N 24 ss ; MEIER/DE LUZE, N 586 ss ; STEINAUER/FOUNTOULAKIS, N 513 ss.

³² MEIER/DE LUZE, N 589 ; STEINAUER/FOUNTOULAKIS, N 517.

³³ ATF 133 III 121 ; ATF 119 II 456 ; ATF 117 Ib 197/JdT 1992 I 214 ; ATF 105 II 284. Voir par ex. : art. 16 LRH (cf. *supra* note 5) ; art. 46 al. 1 Loi genevoise sur

consentement est d'ailleurs une source de préoccupation s'agissant de la collecte des données personnelles³⁴.

33. Il y a en conséquence un intérêt particulier à rattacher l'intégrité numérique aux biens de la personnalité physique. Cette approche est corroborée par l'enquête réalisée auprès des personnes vivant en marge de la société et par les craintes d'une fracture numérique (cf. *supra* n. 25). Le cyber harcèlement des jeunes, qui ne fait par ailleurs pas l'objet d'une norme pénale spécifique en droit suisse, permet également d'illustrer le rapport étroit entre l'intégrité numérique et l'intégrité en particulier psychique, le harcèlement en ligne ne permettant plus à la victime de se sentir en sécurité où que ce soit et de reprendre ses forces³⁵. Ces exemples mettent corrélativement en exergue l'urgence du besoin de protection.
34. Accréditant notre point de vue, la Constitution de l'Organisation mondiale de la santé spécifie que la santé est un état de complet bien-être physique, mental et social³⁶. Il faut reconnaître que la caractéristique de l'être humain contemporain est de naître et mourir dans le numérique, au point que la question des données des personnes décédées est amenée à être traitée dans la loi³⁷. Un compte sur un réseau social représente une partie de l'individu, un blog également permettant de parler de meurtre numérique si par hypothèse le réseau social en coupe les accès. L'être humain de nos

la santé du 7 avril 2006, entrée en vigueur le 1^{er} septembre 2006, LS-RS.GE K 1 03. CR CC I-JEANDIN, art. 28 N 62 ss ; BUCHER, N 498 ss ; MEIER/DE LUZE, N 673 ss.

³⁴ Sur la qualité du consentement en matière de protection des données, cf. art. 4 al. 5 LPD : ATF 140 I 2, c. 10.2.2/JdT 2014 I 167. MEIER, N 847 ss sur ces notions importées du droit médical.

³⁵ Voir le Rapport 2012 consacré aux droits de l'enfant, « Enfants et écrans : grandir dans le monde numérique », Paris 2012, qui fait un point exhaustif sur l'apport des nouvelles techniques de communication, mais aussi sur leurs limites et leurs dangers, cf. https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/ddd_ra_e_2012.pdf.

³⁶ Cf. https://www.who.int/governance/eb/who_constitution_fr.pdf. Que les êtres humains ont aujourd'hui une existence numérique au même titre qu'une existence physique et psychique est défendue par l'Association pour la reconnaissance et la protection de la vie numérique (ARPVN ; <http://vienumerique.ch/>).

³⁷ Section 3, art. 16 du projet de la LPD, cf. <https://www.admin.ch/opc/fr/federal-gazette/2017/6803.pdf>.

jours existe, non pas seulement à travers les réseaux sociaux, mais il se construit également à travers eux. La question philosophique d'une vie éternelle dans le numérique est posée, laquelle commence avant même que l'enfant ne soit né, car il n'est pas rare que les écographies soient partagées en ligne. S'il peut être discuté de savoir s'il est acceptable que par exemple une enfant décédée soit « réanimée » pour entretenir une relation avec ses parents, grâce à une interaction virtuelle fondée sur l'exploitation de la masse de données laissée par la personne décédée, mieux vaut encadrer le débat par la reconnaissance d'un droit fondamental à l'intégrité numérique, que le Code civil s'emploiera également à protéger.

V. Protection interne de la personnalité

35. L'art. 27 CC protège la personne contre les engagements excessifs et, à ce titre, les biens protégés sont la capacité civile, ainsi que la liberté de décision.
36. La capacité civile est inaliénable selon l'art. 27 al. 1 CC et les art. 11 à 19 CC sont rendus par ce biais impératifs³⁸. Sous l'angle d'un droit à l'intégrité numérique, la capacité civile, impactée par les technologies, revêt trois composantes distinctes. La première consiste en la capacité à agir comme une personne dans le monde numérique. Elle inclut la garantie et le respect de l'identité, ainsi que la garantie d'un accès à l'espace numérique. La deuxième composante vise la capacité à agir en sécurité, soit à être protégé dans cet espace virtuel. Enfin, la capacité civile inclut la capacité d'agir en liberté, dans le respect de sa vie privée ainsi que de la protection de ses données personnelles. Cette approche est large et ne se limite pas à la notion d'« intégrité informationnelle », préférée par certains auteurs afin de circonscrire les limites du droit à l'autodétermination informationnelle (cf. *supra* n. 14)³⁹.
37. La protection de la liberté de décision par l'art. 27 al. 2 CC signifie que la personne ne peut pas se soumettre entièrement à la volonté

³⁸ CR CC I-MARCHAND, art. 27 N 2 et 17 ; GUILLOD, 2018, N 158 ; MEIER/DE LUZE, N 704.

³⁹ AEBI-MÜLLER, 2005, p. 287 s. ; FLÜCKIGER, p. 855 ; MEIER, N 22.

d'autrui⁴⁰. Ainsi, le débat philosophique quant à la servitude volontaire est tranché en droit suisse : il est contraire aux bonnes mœurs qu'une personne prenne un engagement excessif⁴¹. La perte de contrôle d'un individu dans le monde numérique pourrait être analysée sous l'angle d'une atteinte à la liberté de décision dans la mesure où lesdites données peuvent être utilisées afin d'instrumentaliser les citoyens, notamment lors d'élections⁴².

38. La reconnaissance d'un droit à l'intégrité numérique est essentielle afin d'asseoir les fondements d'une protection qui est due et implique notamment la mise en place de contrôle autre que le contrôle individuel qui n'est plus réaliste ou à tout le moins insuffisant⁴³. Il convient à cet effet de renforcer les droits des autorités de protection. Il en va du respect de la dignité humaine, droit fondamental protégé par l'art. 7 Cst., mis en œuvre en partie par l'art. 27 al. 2 CC, qui ne permet pas que la personne devienne l'objet de la technologie.

VI. Protection externe de la personnalité

39. Les art. 28 ss CC protègent de manière générale la personnalité à l'encontre des atteintes de tiers, notion à comprendre objectivement et non selon le ressenti subjectif de la personne concernée⁴⁴. L'atteinte consiste en un trouble d'une certaine intensité que subit une personne dans sa personnalité du fait du comportement d'un tiers⁴⁵. Elle se comprend dans un sens large, en particulier sous l'angle temporel, dans la mesure où elle vise non seulement celui qui est effectivement atteint, mais aussi celui qui est menacé d'une

⁴⁰ CR CC I-MARCHAND, art. 27 N 40.

⁴¹ Sur les critères du caractère excessif d'une atteinte : CR CC I-MARCHAND, art. 27 N 14 ss ; BUCHER, N 402 ss ; MEIER/DE LUZE, N 709 ss.

⁴² Le Temps, 20 et 27 mars 2018, p. 9 sur le scandale visant l'entreprise britannique Cambridge Analytica accusée d'avoir utilisé les données de millions d'individus pour manipuler les élections américaines en influençant les intentions de vote.

⁴³ BRUNNER, N 50 et ch. VI.

⁴⁴ BSK ZGB-MEILI, art. 28 N 42 ; CR CC I-JEANDIN, art. 28 N 69 ; MEIER/DE LUZE, N 657.

⁴⁵ ATF 120 II 369, c. 2. CR CC I-JEANDIN, art. 28 N 68 ; BUCHER, N 492 ; GUILLOD, 2018, N 165 ; MEIER/DE LUZE, N 655 s. ; STEINAUER/FOUNTOULAKIS, N 553.

atteinte ou encore celui qui subit un trouble consécutif à une atteinte ayant pris fin⁴⁶.

40. La loi s'appuie sur une présomption d'illicéité dès lors que l'atteinte est établie. Le demandeur lésé supporte le fardeau de la preuve de l'atteinte à sa personnalité au sens de l'art. 28 al. 1 CC pour que naisse la présomption d'illicéité ; il n'a pas à prouver une faute de l'auteur, laquelle n'est pas une condition des actions défensives⁴⁷.
41. Selon l'art. 28 al. 2 CC, la présomption d'illicéité peut être renversée en apportant la preuve d'un motif justificatif, à savoir le consentement de la victime, un intérêt prépondérant privé ou public ou la loi ; le fardeau de la preuve incombe au défendeur, auteur de l'atteinte⁴⁸. Calqué sur la systématique légale, l'examen d'une violation des droits de la personnalité se fait en deux étapes, premièrement, l'existence d'une violation d'un droit de la personnalité, ce qui implique la reconnaissance de l'intégrité numérique comme un bien de la personnalité (cf. *supra* n. 26), et deuxièmement, l'analyse d'un éventuel motif justificatif⁴⁹. Si la présomption d'illicéité n'est pas renversée, le Code civil octroie au lésé dans son intégrité numérique deux catégories d'actions de nature différentes, celles qui lui permettent de se défendre et celles d'exiger réparation.

A. Actions défensives

42. Dans le cadre d'une action défensive, l'atteinte à la « valeur » qu'est l'intégrité numérique est directement visée. La loi prévoit trois actions défensives, consacrées par l'art. 28a al. 1 CC, qui assurent la protection de la personnalité à des moments différents : avant, pendant et après l'atteinte⁵⁰. Le juge est amené à respecter le

⁴⁶ CF, Message, p. 685.

⁴⁷ ATF 126 III 161, c. 5a/JdT 2000 I 292. CR CC I-JEANDIN, art. 28 N 86 ; MEIER/DE LUZE, N 660 ; STEINAUER/FOUNTOULAKIS, N 581, 590 et 596.

⁴⁸ ATF 136 III 410, c. 2.3. BUCHER, N 496.

⁴⁹ ATF 136 III 410, c. 2.2.1 ; ATF 134 III 193, c. 4.6 ; ATF 126 III 305, c. 4a ; ATF 127 II 481, c. 2c. MEIER/DE LUZE, N 662 sur cette analyse en deux temps, suivie par la pratique judiciaire, et la controverse y relative en doctrine.

⁵⁰ CR CC I-JEANDIN, art. 28a N 1 ; MEIER/DE LUZE, N 734.

principe de la proportionnalité par rapport au but visé lorsqu'il prononce une mesure, en particulier d'interdiction⁵¹. L'art. 15 LPD renvoie par ailleurs largement à l'art. 28a CC, dont les actions s'étendent à la protection des données personnelles.

43. La première est l'action en prévention ou en interdiction d'une atteinte imminente (art. 28a al. 1 ch. 1 CC) ; il s'agit d'une forme d'action condamnatoire qui exige une menace sérieuse et concrète d'atteinte au moment où le juge rend sa décision⁵². La deuxième, l'action en cessation de l'atteinte est ouverte dans la mesure où l'atteinte actuelle dure encore (ch. 2)⁵³. Par son biais, la large disponibilité des documents électroniques permet par exemple de justifier une correction ou une suppression d'un texte archivé. Enfin intervient l'action en constatation du caractère illicite de l'atteinte, lorsque le trouble que celle-ci a créé subsiste (ch. 3). Tel est le cas lorsque persiste une image négative de la victime, l'action ayant une fonction de réhabilitation, ou lorsqu'il y a un doute sur la licéité du comportement de l'auteur de l'atteinte⁵⁴ ; l'action a ici une fonction de sécurisation qui peut être particulièrement intéressante en matière d'intégrité numérique. Cette forme spéciale de l'action générale en constatation de droit est souvent en pratique associée à des prétentions réparatrices ; elle est sous un angle temporel subsidiaire aux deux autres actions défensives. Le choix de l'action dépendra ainsi essentiellement de la chronologie des événements et surtout du moment auquel le demandeur se situe par rapport à l'atteinte à son intégrité numérique.

⁵¹ BUCHER, N 557 ; GUILLOD, N 172 ; MEIER/DE LUZE, N 7.

⁵² ATF 124 III 72, c. 2a, rendu en matière de concurrence déloyale, qui admet que lorsque l'auteur d'une atteinte n'accepte pas d'avoir agi à tort, il est susceptible de commettre une nouvelle atteinte ; ATF 108 II 344, c. 2b ; ATF 97 II 97, c. 5b/JdT 1972 I 242 ; TF 5A_658/2014 du 6 mai 2015, c. 3.3 ; TF 5A_228/2009 du 8 juillet 2009, c. 4.1. CR CC I-JEANDIN, art. 28a N 4 s. ; CF, Message, p. 685 ; MEIER/DE LUZE, N 755 ; STEINAUER/FOUNTOULAKIS, N 579 ss.

⁵³ TF 5A_170/2013 et 5A_174/2013 du 3 octobre 2013. CR CC I-JEANDIN, art. 28a N 7 ; MEIER/DE LUZE, N 760 ; STEINAUER/FOUNTOULAKIS, N 589.

⁵⁴ TF 5A_286/2012 du 29 octobre 2012 pour un exemple de cette fonction de sécurisation, et pour un exemple de la fonction de réhabilitation : TF 5A_376/2013 du 29 octobre 2013, c. 7.2. CR CC I-JEANDIN, art. 28a N 11 s. ; MEIER/DE LUZE, N 769 ; STEINAUER/FOUNTOULAKIS, N 594 s.

B. Actions réparatrices

44. Les droits de la personnalité n'ont en eux-mêmes aucune valeur pécuniaire (cf. *supra* n. 15), mais une atteinte à ces droits peut avoir des répercussions économiques. L'atteinte se distingue ainsi du préjudice qui est la conséquence d'une atteinte à la personnalité sur le patrimoine ou le bien-être du lésé.
45. Les actions réparatrices, qui ont une fonction de rééquilibrage, sont régies par le droit des obligations et non pas par les art. 28 ss CC, le législateur opérant par un renvoi à l'art. 28a al. 3 CC. L'acte illicite qui ouvre la voie à la réparation est l'atteinte illicite à la personnalité au sens de l'art. 28 CC, soit l'atteinte à l'intégrité numérique. Il faut choisir l'action adaptée à la situation concrète selon la nature des conséquences subies par la victime, tort moral ou/et dommages et intérêts et/ou gain indu obtenu par l'auteur de l'atteinte. Ces actions peuvent se cumuler selon les besoins, seules les actions défensives s'excluant entre elles par rapport à une même atteinte (cf. *supra* n. 43 *in fine*). Les conclusions en dommages et intérêts ou en réparation du tort moral découlant d'une atteinte illicite à la personnalité sont par ailleurs indépendantes et n'impliquent pas de prendre des conclusions en interdiction, cessation ou en constatation de l'atteinte⁵⁵.
46. L'art. 28a al. 3 CC renvoie aux art. 41 ss CO pour l'action en dommages-intérêts, aux art. 47 ss CO pour l'action en réparation du tort moral, l'art. 49 CO étant la disposition générale, laquelle vise la compensation par une somme d'argent des souffrances physiques ou morales endurées du fait de l'atteinte à la personnalité. L'atteinte à un bien appartenant à la personnalité physique est un atout pour obtenir réparation d'un dommage moral, qui doit pouvoir être qualifié de grave⁵⁶. La titulaire d'un blog qui verrait son accès supprimé pourrait selon les circonstances faire valoir des prétentions à ce titre.

⁵⁵ TF 5A_562/2018 du 22 juillet 2019, à défaut de conclusion toutefois, l'atteinte à la personnalité ne peut être formellement constatée dans le dispositif de l'arrêt.

⁵⁶ STEINAUER/FOUNTOULAKIS, N 610. Voir également : CR CC I-JEANDIN, art. 28a N 27.

47. La troisième action réparatrice est l'action en remise du gain au sens de l'art. 423 al. 1 CO relatif à la gestion d'affaires imparfaite, étant donné que la gestion n'a pas été entreprise dans l'intérêt du maître, soit de la victime de l'atteinte à la personnalité ; le lésé n'en a pas moins le droit de s'approprier les profits qui en résultent⁵⁷. Cette action est une originalité du droit suisse ; si elle a rarement trouvé application en pratique, il n'en demeure pas moins qu'à notre sens il n'en est pas tiré tout le profit potentiel et qu'il conviendrait de réfléchir à rechercher par ce biais les profits indus tirés par l'auteur d'une atteinte à l'intégrité numérique.

VII. Conclusion

48. Pour répondre à la question « Le droit à l'intégrité numérique est-il une innovation ou une extension de la personnalité civile ? », nous proposons de remplacer « ou » par « et ». En effet, à l'innovation par la création d'un nouveau droit de la personnalité se greffe une extension du droit de la personnalité.
49. Il s'agit d'un phénomène classique, qui n'est pas déroutant dans le domaine des droits de la personnalité. Des précédents en témoignent, comme le droit de connaître ses origines ou le droit à l'image, qui ont également requis des développements jurisprudentiels pour acquérir le rang de droits de la personnalité autonomes et voir leur champ d'application circonscrit.
50. Accorder le statut de bien de la personnalité à l'intégrité numérique, auquel correspond un droit de la personnalité, permet de poser les fondements à un développement ultérieur jurisprudentiel et au besoin législatif, à l'instar de la protection de l'intégrité physique, bien incontesté de la personnalité, qui a appelé avec le temps de nombreuses lois spéciales. L'importance prise par la technologie sur nos vies est telle qu'il convient de se saisir de cette réalité pour, autant que faire se peut, anticiper et encadrer ses effets. Promouvoir la reconnaissance d'un droit à l'intégrité numérique, aux côtés de l'intégrité physique et psychique, consiste à promouvoir une société numérique humaniste dans le respect des libertés individuelles.

⁵⁷ ATF 143 III 297 ; ATF 133 III 153 ; TF 5A_658/2014 du 6 mai 2015.

« Droit à l'intégrité numérique » et protection de droit civil de la personnalité

L'honneur pourrait en revenir au juge civil dans le cadre du développement de l'art. 28 CC.

Bibliographie

AEBI-MÜLLER REGINA, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes : Unter Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Berne 2005 (cité : AEBI-MÜLLER, 2005)

AEBI-MÜLLER REGINA, Die Persönlichkeit im Sinne von Art. 28 ZGB, in : Geiser Thomas et al. (éd.), Festschrift für Heinz Hausheer zum 65. Geburtstag : Privatrecht im Spannungsfeld zwischen gesellschaftlichem Wandel und ethischer Verantwortung, Berne 2002, p. 99 ss (cité : AEBI-MÜLLER, 2002)

BRUNNER STEPHAN C., Mit rostiger Flinte unterwegs in virtuellen Welten ? : Leitgedanken zur künftigen Entwicklung des schweizerischen Datenschutzrechts, in : Jusletter 4 avril 2011

BUCHER ANDREAS, Personnes physiques et protection de la personnalité, 5^e éd., Bâle 2009

CONSEIL FEDERAL, Message concernant la révision du Code civil (Protection de la personnalité : art. 28 CC et 49 CO), du 5 mai 1982, FF 1982 II 661 (cité : CF, Message)

FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, in : PJA 2013, p. 837 ss

GROSSEN JACQUES-MICHEL, La protection de la personnalité en droit privé (Quelques problèmes en droit actuel), in : RDS 1960 II, p. 1a ss

GUILLOD OLIVIER, Droit des personnes, 5^e éd., Bâle/Neuchâtel 2018 (cité : GUILLOD, 2018)

GUILLOD OLIVIER, Cent ans de sollicitude : un Code civil soucieux de la personne humaine, in : RDS 2007 II, p. 51 ss (cité : GUILLOD, 2007)

JEANDIN NICOLAS, Art. 28 et 28a, in : Foëx Bénédicte/Pichonnaz Pascal (éd.), Code Civil I, Commentaire Romand, art. 1-359 CC, Bâle 2010 (cité : CR CC I – JEANDIN)

MARCHAND SYLVAIN, Art. 27, in : Foëx Bénédicte/Pichonnaz Pascal (éd.), Code Civil I, Commentaire Romand, art. 1-359 CC, Bâle 2010 (cité : CR CC I – MARCHAND)

MEIER PHILIPPE, Protection des données : Fondements, principes généraux et droit privé, Berne 2011

MEIER PHILIPPE/DE LUZE ESTELLE, Droit des personnes : Art. 11-89a CC, Genève/Zurich/Bâle 2014

MEILI ANDREAS, Art. 28, in : Honsell Heinrich/Vogt Nedim Peter/Geiser Thomas (éd.), Kommentar zum Schweizerisches Zivilgesetzbuch I, Art. 1-456 ZGB, 6^e éd., Bâle 2018 (cité : BSK ZGB – MEILI)

STEINAUER PAUL-HENRI/FOUNTOULAKIS CHRISTIANA, Droit des personnes physiques et de la protection de l'adulte, Berne 2014

WERRO FRANZ, La définition des biens de la personnalité : une prérogative du juge, in : Gauch Peter/Werro Franz/Zufferey Jean-Baptiste (éd.), La protection de la personnalité : Bilan et perspectives d'un nouveau droit, Contributions en l'honneur de Pierre Tercier pour ses cinquante ans, Fribourg 1993, p. 15 ss

Le droit à l'intégrité numérique est-il une innovation ou une extension de l'intégrité physique ?^{*}

par

André Kuhn

Professeur à l'Université de Neuchâtel

I. Introduction.....	88
II. La protection pénale de l'intégrité numérique	89
III. Conclusion.....	91
Bibliographie	94

* Certaines parties de la conclusion du présent texte – et surtout les idées qui y sont véhiculées – ont déjà été publiées par l'auteur dans des écrits antérieurs. Là où certain-e-s utiliseront peut-être la notion ridicule d'« auto-plagiat », l'auteur considère qu'il s'agit plutôt d'un phénomène positif, puisqu'il est le reflet d'un mode de pensée logique, cohérent et surtout constant.

I. Introduction

1. Avant de tenter de répondre à la question posée par le titre de la présente contribution – et donc de traiter du sujet autour duquel il nous a été demandé de réfléchir – penchons-nous un instant sur le titre lui-même. On y part en effet de la prémisse qu’il existerait une intégrité numérique, génératrice de droits, et qu’il serait dès lors nécessaire de se déterminer sur le fait de savoir si de nouvelles dispositions légales seraient nécessaires pour préserver ces droits ou si les normes d’ores et déjà en vigueur suffissent à les appréhender. Permettez-moi toutefois de mettre en doute la pertinence même de la prémisse et ainsi l’existence de ce que le titre présente comme un acquis. En d’autres termes, avant de traiter du contenu, traitons de l’intégrité numérique en tant que telle, soit du contenant.
2. Si les intégrités physique, psychique et sexuelle font intimement partie intégrante de tous les êtres vivants depuis le début de leur existence, il semble aller de soi qu’il n’en va pas de même de l’intégrité numérique qui, elle, tire son origine de l’avènement du numérique.
3. Certes, les intégrités physique, psychique et sexuelle ne sont pas protégées de la même manière à travers le temps et l’espace, ni pour tous les êtres vivants, mais cela ne remet pas en question leur existence. C’est ainsi que l’intégrité physique – qui était pourtant intrinsèquement la même – n’avait pas la même valeur pour un maître ou une maîtresse que pour leur esclave et n’était donc pas protégée pareillement pour l’un-e et pour l’autre. Il en va d’ailleurs toujours ainsi de l’intégrité physique de la majorité des animaux par rapport à celle de l’animal particulier qu’est l’être humain. De plus, ce qui vient d’être développé au sujet de l’intégrité physique peut l’être aussi pour les intégrités sexuelle et psychique. L’intégrité sexuelle de l’homme et de la femme n’a pas toujours fait l’objet d’un respect similaire et l’intégrité psychique du ver de terre (soit son libre arbitre par exemple d’aller à droite ou à gauche) nous laisse relativement indifférent-e-s par rapport à celle de l’être humain.
4. De surcroît, le concept d’intégrité numérique est fondamentalement anthropocentrique, et n’est donc pas lié à tout être vivant, mais uniquement à l’être vivant humain. Pour s’en convaincre, il suffit de

tenter de déterminer ce que pourrait être l'intégrité numérique de notre ver de terre...

5. Si donc une protection accrue de la sphère numérique de chaque être humain devait éventuellement être envisagée, de grâce, qu'elle ne le soit pas sous le vocable « intégrité » ! Réserveons ce mot pour des choses bien plus fondamentales que la simple protection – certes nécessaire – des données quelque peu particulières que sont nos données numériques.
6. Si nous devons impérativement vouloir créer une nouvelle intégrité, ce n'est à mon sens pas tellement du côté du numérique anthropocentré qu'il faudrait se tourner, mais bien plus vers un concept plus biocentré d'intégrité environnementale, s'éloignant de l'intégrité étroitement liée à un organisme vivant en tant que tel.
7. Ces quelques considérations introductives ne nous empêcheront toutefois pas de faire comme si une intégrité numérique existait et qu'il serait ainsi nécessaire de déterminer le degré de protection que pourrait lui garantir le droit pénal actuellement en vigueur.

II. La protection pénale de l'intégrité numérique

8. Si l'*identité* numérique ou des données personnelles numérisées font l'objet d'une certaine protection par le droit pénal par l'intermédiaire de dispositions telles que les articles 179^{novies} CP¹ sur la soustraction de données personnelles, 143 CP sur la soustraction de données électroniques et 143^{bis} CP sur l'accès indu à un système informatique, il en va très différemment de l'*intégrité* numérique. Certes, il semble bel et bien y avoir un désir de l'autorité législative d'interdire – et donc de se prémunir contre – l'accès indu à un système informatique dans le but d'y soustraire des données personnelles. Les notions de fichiers contenant des données personnelles sensibles et de profils de la personnalité qui ne sont pas librement accessibles (au sens de l'article 179^{novies} CP) sont par ailleurs définies à l'article 3 de la LPD². Par contre, rien ne nous

¹ Code pénal suisse du 21 décembre 1937 (RS 311.0).

² Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1).

permet de penser qu'une *intégrité* numérique ait été envisagée par l'autorité législative.

9. En matière d'intégrités, le Code pénal suisse ne mentionne que l'intégrité corporelle (citée dans 26 dispositions³) ou physique (dans quatre dispositions⁴), une intégrité psychique (que l'on retrouve dans deux articles⁵) ou mentale (dans une disposition⁶), et une intégrité sexuelle (qui couvre 16 dispositions du Code pénal⁷).
10. Il n'existe de ce fait aucune protection explicite d'une quelconque intégrité numérique à ce jour. La question qu'il reste dès lors à résoudre est celle de savoir si une criminalisation de l'atteinte à une éventuelle intégrité numérique pourrait découler d'une extension de la protection de l'intégrité physique. On pourrait en effet penser que cette dernière comprend l'intégrité psychique – puisqu'en s'en prenant à la santé mentale d'une personne, on touche également à sa santé physique au sens large du terme – et, avec un peu d'imagination, on aurait donc pu étendre encore plus largement l'intégrité physique pour qu'elle couvre aussi une éventuelle intégrité numérique.
11. Un tel raisonnement est toutefois impossible, et ce pour deux raisons. La première est que, formellement, la protection pénale de l'intégrité psychique ne découle pas de la protection de l'intégrité physique. La première existe pour elle-même et indépendamment de la seconde. On le voit par exemple aux articles 122 et 123 CP sur les lésions corporelles, où l'atteinte à la santé fait l'objet d'une mention expresse dans la disposition légale.
12. On ne peut donc pas en déduire qu'il suffirait d'étendre encore un peu le concept d'intégrité physique pour y inclure une éventuelle intégrité numérique. Ce d'autant plus d'ailleurs que, si l'on considérait que l'intégrité numérique est incluse dans l'intégrité physique, alors l'article 221 al. 2 CP sur l'incendie intentionnel ne ferait plus vraiment de sens lorsqu'un tel incendie aurait été commis

³ Art. 18, 28a, 101, 122, 123, 125, 140, 156, 221, 222, 223, 224, 225, 227, 228, 229, 230, 230bis, 237, 238, 264a, 264c, 264e, 271, 349a, 349c CP.

⁴ Art. 64, 75, 119, 264 CP.

⁵ Art. 64, 75 CP.

⁶ Art. 264 CP.

⁷ Art. 64, 75, 187-200 CP.

« dans le but de mettre en danger l'intégrité numérique d'une personne ».

13. Par ailleurs, inclure l'intégrité numérique dans l'intégrité physique reviendrait à étendre largement la punissabilité par rapport à ce qui a été envisagé initialement par l'autorité législative. Et cette remarque nous permet justement de passer à la seconde raison – qui est d'ailleurs la raison principale – pour laquelle il serait impossible, en droit pénal, de considérer que l'intégrité numérique n'est qu'une extension ou une déclinaison de l'intégrité physique. Cet obstacle trouve son fondement dans l'article premier du Code pénal, qui nous indique que l'on ne peut sanctionner quelqu'un que pour un acte qui est expressément réprimé par la loi. C'est ce que l'on appelle le *principe de la légalité*, soit un principe fondamental qui n'est rien de moins que la garantie contre une application arbitraire du droit pénal.
14. Un Etat moderne digne de ce nom – dans lequel tout ce qui n'est pas interdit est autorisé et non où tout ce qui n'est pas autorisé est interdit – ne peut en effet pas se permettre de réprimer quelqu'un pour un acte qui ne fait pas expressément partie de la liste des actes punissables.
15. Il est donc EXCLU – au nom du principe de la légalité – de faire un raisonnement ou une interprétation par analogie en matière de droit pénal, dans la mesure où celle-ci attenterait davantage aux droits des citoyens que ce qui est prévu par la loi !
16. La réponse à la question de savoir si, en droit pénal, l'intégrité numérique peut être une simple extension de l'intégrité physique est dès lors très clairement négative !
17. Si donc une intégrité numérique devait réellement exister et que nous considérions qu'il faut absolument tenter de la protéger par l'intermédiaire du droit pénal, alors ce ne pourrait être qu'une innovation qui nécessiterait de nouvelles normes pénales.

III. Conclusion

18. La dernière question qui se pose en la matière est de savoir s'il est véritablement utile de criminaliser des comportements pour tenter de protéger une intégrité. Sachant en effet qu'en matière de

protection du bien juridique suprême de l'être humain qu'est la vie, cela fait des milliers d'années que nous édictons des lois interdisant de tuer autrui, des milliers d'années que l'on sanctionne les meurtriers et les meurtrières, ce sans pour autant parvenir à éviter que certaines personnes en tuent d'autres, la question n'est pas sans pertinence. Le droit pénal et la sanction que l'on inflige en son nom bénéficient-ils dès lors encore d'une légitimité ? La société n'a en effet pas besoin de lois pénales pour savoir qu'un meurtre est inadmissible et catastrophique⁸. N'en va-t-il pas de même pour l'ensemble des biens juridiques que l'on tente de protéger par l'intermédiaire de dispositions pénales ?

19. On me rétorquera probablement que, si nous ne protégeons pas la vie par le droit pénal, le nombre d'homicides serait bien plus élevé. Mais en est-on vraiment certain ? N'oublie-t-on pas un peu rapidement qu'en ville de Drachten, le fait d'avoir supprimé la signalisation routière a eu pour effet de *diminuer* le nombre d'accidents et d'infractions au Code de la route⁹, montrant ainsi que le fait de valoriser le « savoir SE conduire » peut avoir de meilleurs effets que la simple exigence de « savoir conduire » ?
20. En réalité, criminaliser un comportement procure certainement le sentiment de s'attaquer à un problème et donne surtout bonne conscience, alors qu'en réalité toute criminalisation équivaut à un aveu d'échec d'une politique sociale. Ce n'est en effet que parce que d'autres moyens de résoudre un problème social échouent que l'on criminalise. C'est ainsi notamment que la consommation de stupéfiants n'est pas un problème pénal, mais un problème de santé publique géré de façon désastreuse par le politique, que la criminalisation de la migration est un aveu de notre incapacité à gérer un problème migratoire dont la source réside souvent hors de nos frontières, et qu'il ne serait pas nécessaire de criminaliser la

⁸ Pour un approfondissement de ce genre de mode de pensée, voir BAKER, p. 169, ainsi que HULSMAN/BERNAT DE CELIS ; ROBERT ; KUHN (2009) ; COQUET.

⁹ A ce propos, voir par exemple KILLIAS/AEBI/KUHN, n° 484, ainsi que les références qui y sont citées.

circulation routière si des politiques de prévention adéquates étaient enfin mises en œuvre¹⁰.

21. C'est donc du côté de la prévention situationnelle¹¹ qu'il faudrait se tourner pour tenter de préserver une éventuelle nouvelle intégrité ou de nouveaux biens juridiques, plutôt que de compter sur une plus qu'hypothétique prévention par la dissuasion liée au droit pénal.

¹⁰ A ce propos, voir KUHN (2015), où il est indiqué qu'un véhicule muni d'un GPS intelligent – limitant la vitesse à ce qui est autorisé sur le tronçon emprunté – et d'un Système DADSS (*Driver Alcohol Detection System for Safety*) – qui teste le degré d'alcoolémie au volant en analysant en continu le souffle expiré par le conducteur et qui l'oblige à s'arrêter en cas d'ivresse au volant – n'est tout simplement plus en mesure de permettre la commission de certaines infractions représentant quelque 53% des entrées au casier judiciaire de notre pays.

¹¹ A ce propos, voir par exemple KUHN (2020), pp. 37-42.

Bibliographie

BAKER CATHERINE, Pourquoi faudrait-il punir ? – Sur l'abolition du système pénal, Lyon : Tahin Party, 2004

COQUET MARGAUX, De l'abolition du système pénal – Le regard de Louk Hulsman, Meylan : Campus Ouvert, 2016

HULSMAN LOUK/BERNAT DE CELIS JACQUELINE, Peines perdues – Le système pénal en question, Paris : Le Centurion, 1982

KILLIAS MARTIN/AEBI MARCELO F./KUHN ANDRÉ, Précis de criminologie, 4^e édition, Berne : Staempfli, 2019

KUHN ANDRÉ, Peut-on se passer de la peine pénale ? – Un abolitionnisme à la hauteur des défis contemporains, in : Revue de Théologie et de Philosophie 141 (2009), pp. 179-192

KUHN ANDRÉ, Technologies embarquées et prévention du crime : quelques considérations criminologiques, in : Revue Interdisciplinaire de Circulation Routière 2/2015, pp. 46-50

KUHN ANDRÉ, Quel avenir pour la justice pénale ?, 2^e édition, Charmey : L'Hèbe, 2020

ROBERT CHRISTIAN-NILS, L'abolition, in : Collectif « Octobre 2201 », Comment sanctionner le crime ?, Ramonville Saint-Agne : Erès, 2002, pp. 35-50

L'intégrité numérique : une nécessité du point de vue du droit à la protection des données ?

par

Jean-Philippe Walter

Commissaire à la protection des données du Conseil de l'Europe

I. Introduction.....	96
II. Les droits au respect de la vie privée et à la protection des données : sources et contenu	96
III. La Convention (108) sur la protection des personnes à l'égard du traitement automatisé de données à caractère personnel.....	98
IV. Conclusion	101
Bibliographie	101

I. Introduction

1. La question dont nous débattons aujourd'hui est celle de savoir s'il faut inscrire explicitement dans la Constitution fédérale un droit à l'intégrité numérique au même titre que l'intégrité physique ou psychique, afin notamment de mieux nous protéger lors de la collecte et du traitement de données personnelles. Formulé différemment, il s'agit de savoir si les articles 10 et 13 de la Constitution¹ en relation avec l'article 8 de la Convention européenne des droits de l'Homme du 4 novembre 1950² et de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel³ ne contiennent déjà pas tous les éléments de la reconnaissance d'une telle intégrité numérique ou si nous faisons face à un droit nouveau.
2. Tout d'abord, il me semble important de rappeler que l'être humain est un tout. Il n'y a pas lieu de distinguer entre l'être humain « réel » et son prolongement « virtuel » ou « numérique ». Qu'il agisse ou interagisse dans le monde réel ou dans le monde virtuel, la protection de ses droits humains et libertés fondamentales, y compris son droit au respect de sa vie privée couvre et doit couvrir tous les aspects de la personne et de sa personnalité d'autant plus que la distinction entre l'environnement réel et l'environnement numérique est de plus en plus mince, pour ne pas dire quasi inexistante. Ces droits sont inaliénables et imprescriptibles.

II. Les droits au respect de la vie privée et à la protection des données : sources et contenu

3. Le droit au respect de la vie privée et le droit à la protection des données, tout en étant liés, sont des droits distincts. Le droit au respect de la vie privée est apparu pour la première fois comme un des droits fondamentaux protégés au niveau international dans la Déclaration universelle des droits de l'homme de 1948. Il a ensuite été inscrit en 1950 à l'article 8 CEDH lequel dispose que toute

¹ RS 101.

² CEDH, RS 0.101.

³ Convention 108, RS 0.235.1

personne a droit au respect de sa vie privée. On le retrouve également dans le Pacte international du 16 décembre 1966 relatif aux droits civils et politiques⁴. Ces textes sont certes bien antérieurs au développement de l'informatique, de l'Internet, des téléphones intelligents ou de l'intelligence artificielle qui ont contribué au développement de la société de l'information et des communications avec ses avantages et ses inconvénients, en particulier ses risques pour le respect des droits humains et des libertés individuelles.

4. La jurisprudence de la CEDH a très rapidement reconnu que l'article 8 CEDH couvrait les atteintes résultant du traitement des données personnelles et de nombreux arrêts traitent de violation de la vie privée en relation avec des aspects du monde numérique (surveillance des communications, des courriers électroniques, des connexions à Internet)⁵. Elle reconnaît également un droit à l'autodétermination informationnelle rattaché au droit à la protection de la vie privée⁶ et établit ainsi que la protection des données joue un rôle fondamental pour l'exercice de ce droit. Pour reprendre les termes de la Cour, « l'article 8 de la Convention consacre donc le droit à une forme d'auto-détermination informationnelle, qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne les données qui, bien que neutres, sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits au titre de l'article 8 peuvent être mis en jeu »⁷.
5. Le Tribunal fédéral a très tôt reconnu sous l'angle de la liberté personnelle le droit à l'autodétermination informationnelle⁸ et ce

⁴ Art. 17, RS 0.103.2.

⁵ Pour un bref aperçu de la jurisprudence de la CEDH, voir la fiche thématique « protection des données personnelles », https://www.echr.coe.int/Documents/FS_Data_FRA.pdf et Case Law of the European Court of Human Rights concerning the protection of personal data, <https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36>.

⁶ CourEDH (GC), *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, arrêt du 27 juin 2017, requête no 931/13.

⁷ CourEDH (GC), *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, arrêt du 27 juin 2017, requête no 931/13, consid. 137.

⁸ ATF 109 Ia 146 (consid. 3 non publié).

bien avant que le droit à la liberté personnelle et le droit à la protection des données soient inscrits dans la Constitution ou que nous ayons adopté une législation nationale de protection des données. Le Tribunal fédéral a d'ailleurs confirmé ce droit à l'autodétermination informationnelle dans sa jurisprudence relative à l'article 13 de la Constitution⁹. Toutefois, il est vrai qu'une partie de la doctrine¹⁰ défend l'idée que ce droit ne peut pas être déduit de l'article 13, alinéa 2 de la Constitution qui, pris à la lettre, vise à protéger l'individu d'un emploi abusif de ses données. C'est une approche défensive du droit à la protection des données et non une approche proactive et dynamique du droit à la protection des données. Dès lors, une révision de l'article 13 de la Constitution serait certainement souhaitable pour mieux refléter la dimension actuelle du droit à la protection des données, mais aussi pour ancrer ce droit de la personne à la maîtrise sur les données qui la concernent. A mon sens, la reconnaissance du droit à l'autodétermination informationnelle est ainsi fondamentale à l'heure de la numérisation de la société, des mégadonnées, de l'intelligence artificielle et du profilage des personnes humaines. Ce droit renferme non seulement l'ensemble des droits de l'individu lui permettant d'avoir et d'exercer le contrôle sur ses propres données (droit de décider, droit d'accès, droit d'opposition, etc.), mais également l'obligation pour ceux et celles qui traitent des données de mettre en œuvre les mécanismes et les outils permettant l'exercice de ce droit et à l'Etat d'en assurer le respect notamment par le biais des autorités de protection des données.

III. La Convention (108) sur la protection des personnes à l'égard du traitement automatisé de données à caractère personnel

6. Indépendamment de cette souhaitable mise à jour, on ne peut interpréter l'article 13, alinéa 2 de la Constitution de manière isolée et ne pas tenir compte de la dimension internationale du droit à la protection des données. Ainsi, le Conseil de l'Europe s'efforce de

⁹ Voir notamment ATF 138 II 346 (359 s.) consid. 8.2, 128 II 259, 140 I 2.

¹⁰ Voir notamment ALEXANDRE FLÜCKIGER, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digital ou un nouveau droit de propriété ?, PJA 2013, p. 837 ss.

mettre en place les cadres juridiques permettant de garantir l'Etat de droit, les droits humains et la démocratie également dans le monde numérique. Concrétisant l'article 8 de la CEDH qui consacre le droit au respect de la vie privée, le Conseil de l'Europe a adopté la Convention sur la protection des personnes à l'égard du traitement automatisé de données à caractère personnel (Convention 108) ouverte à la signature le 28 janvier 1981. Cette Convention, rappelons-le, est actuellement le seul instrument international juridiquement contraignant. Elle renferme les principes de base de la protection des données qui sont aujourd'hui universellement reconnus. Elle s'applique à tout traitement de données à caractère personnel du secteur public et du secteur privé, y compris les traitements des services de renseignements. Elle a un caractère ouvert. Non seulement les Etats membres du Conseil de l'Europe peuvent la ratifier, mais les Etats non-européens ayant une législation de protection des données conforme aux exigences de la Convention peuvent y adhérer. Aujourd'hui la Convention a été ratifiée par les 47 Etats membres du Conseil de l'Europe et 8 pays provenant d'Afrique et d'Amérique latine y ont adhéré¹¹. C'est donc un total de 55 pays qui se sont engagés à respecter les dispositions de la Convention. Bien qu'elle ne soit pas d'application directe, la Convention 108 influence et continuera d'influencer la jurisprudence de la CEDH et du Tribunal fédéral. Cette Convention vient d'être modernisée et un protocole d'amendement a été ouvert à la signature des Parties le 10 octobre 2018¹². La désormais Convention 108+, a été signée par la Suisse le 21 novembre 2019 ; notre pays devrait pouvoir la ratifier cette année encore. A ce jour, la Bulgarie, la Croatie, la Lituanie et la Serbie l'ont ratifiée.

7. Si l'on considère l'article 1 de la Convention 108+, on voit que le droit fondamental à la protection des données protège toute personne physique, quelle que soit sa nationalité ou sa résidence, à l'égard du traitement de données à caractère personnel, contribuant ainsi au respect de ses droits de l'homme et de ses libertés fondamentales et notamment le droit à la vie privée. Ceci, quelles

¹¹ Argentine, Cap Vert, Maroc, Maurice, Mexique, Sénégal, Tunisie, Uruguay.

¹² <https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726>.

que soient les modalités du traitement, automatisé ou non, que la personne interagisse de manière numérique ou non.

8. Les considérants de la Convention 108+ précisent que la protection des données vise à garantir la dignité humaine, ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne, et, eu égard à la diversification, à l'intensification et à la mondialisation des traitements de données et des flux de données à caractère personnel, l'autonomie personnelle fondée sur le droit de toute personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait. En réaffirmant ce droit à la dignité humaine, la Convention 108+ et son rapport explicatif nous rappellent que tout être humain doit demeurer sujet des données et ne doit pas être réduit à un simple objet, qui peut être contrôlé, manipulé, tracé, profilé à souhait au travers de puissants algorithmes et de technologies invasives et souvent opaques. Il doit pouvoir garder la maîtrise sur sa vie.
9. Ainsi, le droit positif de la protection des données tend à protéger la personne dans son entier, y compris son intégrité numérique dans la mesure où les données personnelles sont des éléments constitutifs de l'être humain. Ce droit à la protection des données, sans être un droit supérieur, tend à permettre l'exercice et la garantie des droits humains et des libertés fondamentales, y compris le droit au respect de la vie privée lors du traitement de données personnelles. A mon sens, tout en partageant l'objectif des défenseurs du droit à l'intégrité numérique, nous n'avons pas affaire à un nouveau droit et son inscription dans la Constitution fédérale ne renforcera pas le droit à la protection des données. Cette proposition n'est pour autant pas inutile, car elle permet d'alimenter et de clarifier le débat qui doit être mené autour de la société numérique que nous souhaitons. En effet si nous ne voulons pas être de simples objets du numérique et des technologies de l'information et des communications, des victimes soumises à ce que certains dénomment le « capitalisme de surveillance »¹³, il est urgent d'agir et de définir les contours de la société que nous voulons pour notre bien afin que la technologie soit véritablement au service de

¹³ SHOSHANA ZUBOFF, *The Age of Surveillance Capitalism, The Fight for a Human Future at the New Frontier of Power*, Londres 2019 ; Technologies numériques : en finir avec le capitalisme de surveillance, dans *LaRevueDurable*, 2019, N 63.

l'humain et de la société. Tout être humain doit être en mesure de déterminer librement ce qu'il souhaite, y compris le droit de ne pas être connecté.

IV. Conclusion

10. En conclusion, s'il s'avérait nécessaire de réviser notre Constitution, il ne faudrait pas se limiter à simplement compléter l'article 10 en y ajoutant l'intégrité numérique. Il faudrait se montrer plus ambitieux et reformuler l'article 13, alinéa 2 pour mieux ancrer le fondement du droit à la protection des données à savoir le droit de la personne de contrôler et maîtriser ses propres données et le traitement qui en est fait.

Bibliographie

FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, PJA 6/2013, pp. 837-864

ZUBOFF SHOSHANA, *The Age of Surveillance Capitalism, The Fight for a Human Future at the New Frontier of Power*, Londres 2019

L'intégrité numérique : un obstacle au journalisme d'investigation ?

par

Bertil Cottier

Professeur associé à la Faculté de droit
de l'Université de Lausanne
Professeur invité à l'Académie de journalisme
de l'Université de Neuchâtel
Membre de la Commission fédérale des médias

I. Introduction.....	104
II. Le journalisme de données : qui, quoi, comment.....	104
III. Une mission et des instruments pour l'accomplir	107
A. La mission de chien de garde sociétal.....	107
B. Des instruments pour accomplir la mission.....	109
IV. Liberté de l'information et vie privée : un subtil équilibre	109
V. La rupture d'équilibre	111
VI. Pour conclure	112
Bibliographie	114

I. Introduction

1. Disons-le d'emblée, l'intégrité numérique est un principe constitutionnel dont l'avènement (s'il a lieu...) n'a, de prime abord, pas de quoi réjouir les mass-médias. Déjà malmenés par la concurrence des réseaux sociaux, par la multiplication des *fake news* et par de dramatiques chutes des revenus publicitaires, ils ont tout lieu de craindre qu'un renforcement du droit de la personnalité ne vienne entraver leurs investigations et, partant, les empêchent d'accomplir leur mission de chien de garde sociétal.
2. Ces craintes sont-elles fondées ? La plasticité du principe de l'intégrité numérique, de même que sa prime jeunesse, interdisent toute réponse claire et définitive à cette question. Dès lors, le lecteur est averti : il ne doit pas trop attendre de la présente contribution. Au lieu de savantes mais vaines conjectures, celle-ci se contentera d'émettre une mise en garde : la consécration (qu'elle soit constitutionnelle, législative ou jurisprudentielle, peu importe) de l'intégrité numérique menace sérieusement de rompre le délicat équilibre entre liberté de la presse d'une part, protection de la vie privée et de la réputation d'autre part. Un équilibre fragile, qui résulte de décennies de subtils calibrages opérés par le législateur et surtout par les tribunaux suisses et européens.
3. Le risque est d'autant plus grand que cette consolidation du droit de la personnalité entend déployer tous ses effets sur le terrain du numérique, un terrain que vient d'investir, avec succès, le journalisme d'investigation. Dans le sillage du *Big Data* et des puissants instruments d'analyse de vastes volumes d'informations qu'il a développés, une nouvelle discipline médiatique est née : le journalisme de données (de l'anglais *data journalism*). Et c'est justement cette prometteuse discipline qui risque de faire les frais du principe de l'intégrité numérique. Mais voyons cela de plus près.

II. Le journalisme de données : qui, quoi, comment

4. Comme pour tout nouveau bien ou service, les définitions du journalisme de données sont légion, variant selon que l'accent est mis sur la massivité des informations traitées, sur la force de calcul des outils statistiques, sur l'originalité des résultats obtenus ou

encore sur leur intelligibilité pour le lecteur. De ce foisonnement d'explications, nous en retiendrons une : « le journalisme de données, c'est l'art de faire parler les chiffres et les statistiques au nom du droit du public à l'information »¹. Non seulement cette élégante formule met en exergue les caractéristiques essentielles du journalisme de données, mais encore le renvoi à l'art rappelle que derrière les données et les algorithmes, ce sont des êtres humains qui sont à la manœuvre : qui orientent les recherches, qui exploitent les données et qui tirent des conclusions ; avec rigueur et discernement, mais aussi avec la touche de subjectivité qui peut faire la différence.

5. On l'aura compris, dans tout journalisme de données qui se respecte, il y a d'abord des données : non pas une poignée d'informations retentissantes, mais des amas géants de données, plus ou moins banales, plus ou moins structurées, mais toujours plus volumineuses, vu qu'elles résultent de la croissance exponentielle de la numérisation des activités humaines. Des données que les journalistes ont collectées eux-mêmes – quelquefois avec l'aide de lecteurs (mot-clé : *crowdsourcing*) –, ou qu'ils se sont procurées auprès de sources publiques (mot clé : *open data*), ou encore qu'ils ont obtenues par l'entremise de lanceurs d'alerte (mot-clé : *whistleblowing*). Il y a ensuite une infrastructure computationnelle toujours plus performante : les catégorisations, confrontations, connotations et corrélations nécessaires (mot-clé : *data mining*) sont le fruit de calculs statistiques complexes, opérés par des logiciels sophistiqués tournant sur des ordinateurs de dernier cri. Il y a enfin une équipe composée de journalistes d'investigation expérimentés et de « chercheurs »² formés aux techniques du *Big Data*. Ensemble, ils sont capables d'extraire de ces gigantesques réservoirs des informations inédites qui révèlent les bons et les mauvais côtés de la société et des individus qui la composent. Mieux dit : le journalisme de données « cherche à rendre visible une réalité

¹ DEGLISE FABIEN, Le journalisme de données, ou l'art de faire parler les chiffres, Le Devoir (Montréal), 10 septembre 2012.

² Les chercheurs sont des professionnels des médias à la croisée entre le journalisme et la documentation. Leur tâche est de repérer, acquérir et indexer des informations utiles pour des investigations journalistiques.

qui est enfouie dans une base de données, et qui resterait cachée sans un travail de décryptage »^{3, 4}.

6. Passés les tâtonnements et les hésitations de l'enfance, le journalisme de données a aujourd'hui trouvé ses marques, s'imposant comme un must des rédactions des grands quotidiens de la planète : désormais chacune d'entre-elles dispose d'une unité de data-journalistes aguerris⁵. Des unités qui coopèrent étroitement à chaque fois qu'il s'agit d'exploiter des bases de données si considérables qu'elles dépassent leurs forces individuelles. Un pool permanent s'est d'ailleurs très vite constitué : le Consortium international des journalistes d'investigation⁶ qui réunit près de 200 journalistes provenant des médias les plus renommés du monde (BBC, The Guardian, Le Monde, Washington Post, Corriere della Sera, die Welt, El Pais notamment). Son plus grand succès à ce jour est incontestablement la gigantesque enquête sur l'évasion fiscale appelée Panama Papers (2016). Bénéficiant des révélations d'un lanceur d'alerte au sein d'un cabinet d'avocats panaméen, cette enquête a porté sur plus de 11,5 millions de documents confidentiels concernant plus de 214'000 sociétés offshore. Répartie entre plusieurs rédactions, l'analyse informatique de ces documents (plus de 2,6 téraoctets de données !) a permis de dévoiler les montages financiers dont profitaient un grand nombre d'hommes politiques, de capitaines de l'industrie, de sportifs de haut niveau et de vedettes du cinéma ou de la chanson.

³ CLARINI JULIE, Le journalisme de données : nouveau journalisme ?, Les idées claires, chronique diffusée sur France Culture, le 10 février 2011.

⁴ Pour plus d'informations sur les potentialités et les méthodes du journalisme des données, voir GRAY JONATHAN/BOUNEGRU LILIANA/CHAMBERS LUCY (éd.), The Data Journalism Handbook, Sebastopol 2012. Un deuxième volume est en préparation ; certaines des contributions qu'il contiendra sont déjà accessibles sur le site www.datajournalism.com.

⁵ Pour une brève mais probante présentation de l'évolution du journalisme des données, voir l'interview de Simon Rogers, un des pères fondateurs de la discipline, par GAMBINI LETIZIA, Une décennie de datajournalisme : qu'est-ce qui a changé ?, European Journalism Observatory, 6 juin 2019.

⁶ De son vrai nom International Consortium of Investigative Journalism (ICIJ). Pour un panorama des enquêtes de ce collectif (notamment les Swiss leaks, les Implant files et les China cables), voir son site www.icij.org.

7. Né au sein de la rédaction du quotidien britannique The Guardian⁷, le journalisme de données est désormais bien implanté en Suisse. D'abord parce que des journalistes d'investigation du *Matin-Dimanche* et de la *SonntagsZeitung* ont participé aux grandes enquêtes de l'ICIJ, mais aussi parce que les principaux médias de notre pays se sont finalement dotés des ressources humaines et infrastructurelles appropriées. La crise du Covid19 leur a d'ailleurs permis de s'illustrer en apportant régulièrement des informations fiables et détaillées sur le développement de la pandémie, en complément (quand ce n'était pas en contraste) des communications officielles des autorités fédérales et cantonales⁸.

III. Une mission et des instruments pour l'accomplir

A. La mission de chien de garde sociétal

8. Nul doute : le journalisme de données s'est très rapidement imposé comme un outil d'investigation prisé. Cela dit, les médias n'ont pas attendu l'avènement de cet instrument efficace pour enquêter sur les agissements douteux, voire répréhensibles des acteurs sociaux. De fait, le journalisme d'enquête (aussi appelé journalisme d'investigation) a acquis ses lettres de noblesse au milieu du siècle dernier déjà, d'abord aux Etats-Unis, puis sur le continent européen⁹. Contribuant à la bonne gouvernance de la société en mettant au jour ses dysfonctionnements et les abus commis par ses dirigeants, le journalisme d'investigation est volontiers considéré comme la quintessence de la profession. Reste que cette activité, pour prestigieuse qu'elle soit, est particulièrement exigeante. L'enquêteur doit non seulement faire preuve de sagacité et

⁷ Qui demeure un modèle du genre, avec son fameux « Datablog » (www.theguardian.com/data).

⁸ LEHMAN LORIC, *Berichterstattung über Corona: Die Sternstunde des Datenjournalismus*, persoenlich.com, 11 juin 2020.

⁹ Pour une brève histoire du journalisme d'investigation en France et aux Etats-Unis (où il est né à la fin du XVIII^e siècle sous la forme du *muckraking* – expression familière que l'on peut traduire par déterrer des scandales – qui dénonçait corruptions et injustices), voir HUNTER MARC, *Le journalisme d'investigation en France et aux Etats-Unis*, Paris 1997.

d'indépendance, mais encore d'abnégation : les recherches sont fastidieuses (quelquefois), longues (souvent), couteuses (toujours). A tel point que face à la crise financière qui les frappe durement, de nombreux médias ont renoncé aux dispendieuses enquêtes¹⁰. L'émergence du journalisme de données, au rapport couts/bénéfices avantageux, est arrivée à point nommé pour relancer et dynamiser une discipline qui battait de l'aile.

9. Et c'est tant mieux, car juridiquement parlant, la presse a acquis une dimension institutionnelle. Les tribunaux – à commencer par la Cour européenne des droits de l'Homme qui a souvent fait œuvre de pionnier en matière de liberté de l'information – voient en elle une source de renseignements fiables (ce qui compte en ces temps où les réseaux sociaux font régner la désinformation), fruits d'un processus de triage, de contextualisation et de validation de l'information dicté par des règles déontologiques éprouvées¹¹. Il y a plus : les juges attribuent à la presse la mission de veiller à la gestion compétente et impartiale des biens publics en mettant au jour ces ratés et dérapages qui vont des abus et des injustices commis par les autorités publiques aux arnaques des entreprises privées en passant par les arrangements, plus ou moins troubles, entre petits copains. En bref : aux yeux des juges de Strasbourg, la presse est le « chien de garde de la société »^{12, 13}.

¹⁰ COMMISSION FÉDÉRALE DES MÉDIAS, Rapport Aide aux médias : Etat des lieux et recommandations, Bienne 2014, p. 21 s. Aux contraintes financières, il faut ajouter les impératifs rédactionnels du moment : « La tendance est aux petites phrases, aux idées simples et tranchées favorisées par des formats courts et la lecture binaire de l'œuvre. Sur tel sujet d'actualité il faut se prononcer pour ou contre et ne pas trop développer. », CURCHOD ALEXANDRE, Liberté d'expression : Guide juridique pratique et perspectives, Lausanne 2019, p. 137.

¹¹ ATF 141 I 211, c. 3.1 ; ATF 137 I 209, c. 4.2.

¹² L'expression a été utilisée pour la première fois dans CourEDH, arrêt *The Observer et Guardian c. Royaume-Uni* du 26.11.1991, 13585/88, § 59. Depuis, elle revient sans cesse dans les arrêts de la CourEDH relatifs à la liberté de l'information.

¹³ Dans cette perspective, la presse est au service du droit, pour le public, de recevoir des informations ; voir CourEDH, arrêt *von Hannover c. Allemagne (n°2)* du 7.2.2012 (GC), 40660/08 et 60641/08, Rec. 2012-I, § 102.

B. Des instruments pour accomplir la mission

10. La Cour européenne des droits de l'Homme ne s'est pas contentée d'énoncer une formule à succès (elle a été reprise par le Tribunal fédéral¹⁴) ; elle a aussi veillé à fournir aux journalistes les outils de recherche leur permettant d'accomplir leur mission. Afin de favoriser les enquêtes, et en particulier la révélation de malversations cachées, elle a consacré en 1996 le secret rédactionnel¹⁵ ; dans le même but, elle a jugé, quelques années plus tard, que les lanceurs d'alerte devaient (à certaines strictes conditions, il est vrai) échapper aux foudres de la justice¹⁶. Récemment, elle a concédé à la presse (et aux organisations à but idéal) un droit d'accès à l'information détenue par les autorités publiques¹⁷. Enfin, elle a autorisé les journalistes d'enquête à recourir à des moyens d'investigation clandestins (caméras cachées, déguisement d'identité notamment) s'il s'agit de dénoncer de graves abus et s'il n'y a pas d'autres moyens d'établir le bien-fondé des accusations portées¹⁸.

IV. Liberté de l'information et vie privée : un subtil équilibre

11. Le même souci de sauvegarder la mission de chien de garde sociétal de la presse a présidé à la recherche d'un équilibre judicieux entre la liberté de la presse et la protection de la vie privée et de l'honneur. Une opération délicate, car il importe de veiller scrupuleusement à ce que la protection de la personnalité, si légitime soit-elle, ne soit pas érigée en paravent aux malversations. En d'autres termes, l'exception de protection de la personnalité ne doit pas être brandie par ceux qui n'ont pas la conscience tranquille pour mettre un terme brutal et définitif à une enquête journalistique. Comme le souligne

¹⁴ ATF 127 IV 166, c. 2g ; TF 2C_664/2010, arrêt du 6.4.2011, c. 2.2.

¹⁵ CourEDH, arrêt *Goodwin c. Royaume Uni* du 27.3.1996 (GC), 17488/90, Rec. 1996-II, § 39. Le TF s'est rallié à ce point de vue dans l'année qui a suivi : ATF 123 IV 236, c. 8a.

¹⁶ CourEDH, arrêt *Heinisch c. Allemagne* du 21.7.2011, 28274/08, Rec. 2011-V, § 65. CourEDH, arrêt *Gujja c. Moldavie* du 21.7.2007 (GC), 14277/04, Rec. 2008-II, § 73.

¹⁷ CourEDH, arrêt *Magyar Helsinki Bizottság c. Hongrie* du 8.11.2016 (GC), 18030/11, § 164.

¹⁸ CourEDH, arrêt *Haldimann et autres c. Suisse* du 24.2.2015, 21830/09, Rec. 2015-I, § 61.

le Conseil de l'Europe dans ses *Lignes directrices sur la protection de la vie privée dans les médias* (un document qui entend concrétiser sur le terrain des enquêtes médiatiques la jurisprudence pertinente de la Cour européenne des droits de l'Homme) : « la liberté d'expression recevrait un coup fatal si des personnalités publiques pouvaient censurer la presse et le débat public au nom des droits de la personnalité »¹⁹.

12. Il n'y a pas lieu de détailler la jurisprudence nuancée de la Cour européenne des droits de l'Homme et du Tribunal fédéral destinée à pondérer au plus juste les intérêts en conflit. Les ouvrages à ce sujet ne manquent pas²⁰. Qui plus est, pareille présentation n'est pas indispensable à la bonne compréhension de notre mise en garde à l'encontre du principe de l'intégrité numérique. Un rappel sommaire suffira : les enquêtes médiatiques devront être tolérées si elles portent sur des personnes notoires et/ou si elles alimentent un débat sociétal²¹.
13. Au demeurant, les avantages concédés à la presse ont une contrepartie : un comportement responsable des journalistes²². Les juges attendent d'eux qu'ils accomplissent leur mission de chien de garde sociétal dans le respect des règles déontologiques (notamment vérification des allégations, diversification des sources

¹⁹ Lignes directrices approuvées conjointement par le Comité Directeur sur les Médias et la Société de l'Information et le Comité de la Convention protection des données du Conseil de l'Europe : CONSEIL DE L'EUROPE, *Lignes directrices sur la protection de la vie privée dans les médias*, Strasbourg 2018, p. 11.

²⁰ On se contentera de renvoyer le lecteur à deux ouvrages récents : AUBERSON GÉRALDINE, *Personnalités publiques et vie privée – Etude de droit privé suisse à la lumière du droit américain*, Thèse Fribourg, Zurich 2013 et BACHER BETTINA, *Medienfreiheit und Persönlichkeitsschutz – Zivilrechtliche Auswirkungen der Lösung eines Grundrechtskonflikts*, Bâle 2015.

²¹ Pour plus de détails sur les critères de tolérance, voir CourEDH, arrêt *von Hannover c. Allemagne* (n°2) du 7.2.2012 (GC), 40660/08 et 60641/08, Rec. 2012-I, § 108 ss.

²² ZELLER FRANZ, *Das Konzept des « verantwortungsvollen Journalismus » rückt ins Zentrum – Entscheidungsübersicht Verfassungsrecht und EMRK 2016*, Medialex 2017, p. 78 ss.

d'information, audition de toutes les parties impliquées)²³. A défaut, point de protection de la liberté de l'information.

V. La rupture d'équilibre

14. A première vue, tant les prérogatives mises à disposition des journalistes pour accomplir leur mission de chien de garde sociétal que l'impact limité de la protection de la personnalité à l'encontre des médias incitent à la rassurance. De solides garde-fous seraient en place ; le principe d'intégrité numérique, sitôt consacré, s'insérerait dès lors dans l'ordre juridique national sans bousculer les garanties fondamentales préexistantes ; à commencer par la liberté d'expression que le Tribunal fédéral considère comme le fondement de tout Etat démocratique, méritant « dès lors une place à part dans le catalogue des droits individuels garantis par la Constitution et un traitement privilégié de la part des autorités »²⁴. Cette vision des choses correspond à une réalité aujourd'hui dépassée.
15. Traitement privilégié ? Si oui, ce n'est plus la liberté d'expression qui en bénéficie, mais plutôt la protection de la personnalité. Depuis l'émergence d'Internet et de la communication numérique tous azimuts qu'il a favorisée, la donne a changé. Les tribunaux – emmenés par la Cour européenne des droits de l'homme – sont en train de rompre le délicat équilibre entre protection de la vie privée et de l'honneur d'une part, liberté de l'information d'autre part. La rupture a été amorcée par un renforcement du droit à l'image : les représentations visuelles sont jugées en soi plus intrusives que l'écrit²⁵. La rupture a ensuite été entérinée par plusieurs décisions contraires aux nouveaux médias (notamment les plateformes numériques) dont les juges redoutent les effets collatéraux dommageables à la personnalité des individus : « Internet est certes un outil d'information et de communication qui se distingue particulièrement de la presse écrite, notamment quant à sa capacité à emmagasiner et diffuser l'information. Ce réseau

²³ Pour la déontologie journalistique suisse, voir CONSEIL SUISSE DE LA PRESSE, Directives relatives à la « Déclaration des droits et des devoirs du/de la journaliste ».

²⁴ ATF 96 I 586, c. 5.

²⁵ CourEDH, arrêt *Eerikäinen et autres c. Finlande* du 10.2.2009, 3514/02, § 70.

électronique, desservant des milliards d'utilisateurs partout dans le monde, n'est pas et ne sera peut-être jamais soumis aux mêmes règles ni au même contrôle. Assurément, les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée »²⁶. C'est dans ce contexte de protection de la personnalité accentuée, pour ne pas dire exacerbée, que le principe de l'intégrité numérique voit le jour.

16. Autant dire que pour le journalisme de recherche il vient à un mauvais moment. Son instrument phare, le journalisme de données sera aussitôt dans le collimateur, car il procède de collectes et d'analyses massives d'informations (dont une grande partie sont de nature personnelle²⁷) ; partant, il est synonyme de surveillance à grande échelle sur les individus (ce que justement le principe de l'intégrité numérique veut prévenir) et court le risque si ce n'est d'être banni, du moins d'être sérieusement entravé.

VI. Pour conclure

17. On ne saurait mettre un point final à ce message d'alerte sans tenter de concilier le principe de l'intégrité numérique avec la mission de chien de garde sociétal de la presse, et avec le journalisme des données plus spécifiquement. Plusieurs pistes sont envisageables.

²⁶ CourEDH, *Comité de rédaction Pravoye Delo et Shtetel c. Ukraine* du 5.5.2011, 33014/05, Rec. 2011-II, § 63. Pour une analyse fouillée de l'évolution récente de la jurisprudence vers plus de protection de la personnalité dans l'univers numérique, voir POLLICINO ORESTO et SOLDATOV OLEG, *Judicial balancing of human rights online*, in : Susi Mart (édit.), *Human Rights, Digital Society and the Law – A Research Companion*, Oxon/New York 2019, p. 132 ss.

²⁷ Encore faut-il savoir que le Big Data se joue de la distinction entre données personnelles et données non personnelles ; en effet, le croisement de grands amas de données impersonnelles permet de réidentifier des personnes. Voir ROCHER LUC, HENDRICKX JULIEN M. et DE MONTJOYE YVES-ALEXANDRE, *Estimating the success of re-identifications in incomplete datasets using generative models*, *Nature Communications*, 2019, 10:3069, p. 3. Les auteurs donnent notamment l'exemple de journalistes qui sont parvenus à extraire des historiques de recherche anonymisés concernant trois millions de personnes, les préférences en matière d'informations médicales de nombreux politiciens allemands.

18. On peut doubler la norme constitutionnelle ou le dispositif législatif qui consacrera l'intégrité numérique d'une réserve expresse en faveur de la liberté de la presse ; à l'exemple de ce qui s'est fait en matière de protection des données²⁸. L'exception serait ainsi clairement formulée et les journalistes, pour autant qu'ils fassent preuve d'un comportement responsable, pourront continuer à conduire leurs investigations numériques sans être inquiétés. On peut aussi intervenir au niveau du rapport explicatif à la proposition d'instituer une protection constitutionnelle (ou législative) de l'intégrité numérique, en insérant un paragraphe soulignant la nécessité de tenir compte des besoins de la presse lors de l'implémentation concrète de ce principe. Le signal est plus faible, mais à tout le moins les juges seront-ils avertis. On peut enfin ne rien entreprendre et simplement faire confiance aux tribunaux pour rétablir l'équilibre, le moment venu ; tous comptes faits, cette dernière solution est la moins bonne, puisque les juges sont déjà enclins à surprotéger les individus face au numérique.
19. On peut..., on peut..., on peut..., mais finalement on peut aussi se demander si la consécration du principe de l'intégrité numérique vaut la peine. Autrement dit, se justifie-t-il, pour quelques minimes gains en matière de protection de la personnalité, de mettre en péril ce pilier de la démocratie qu'est la liberté de l'information ? A mon avis, c'est trop cher payé !

²⁸

Voir notamment les art. 10 et 13, al. 2, litt. d de la Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1), ainsi que l'art. 85 du Règlement (UE) 2016/679 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 ; JOUE L 119/1) qui impose aux Etats membres de prévoir des dérogations en faveur des traitements de données réalisés à des fins journalistiques.

Bibliographie

AUBERSON GERALDINE, Personnalités publiques et vie privée – Etude de droit privé suisse à la lumière du droit américain, Thèse Fribourg, Zurich 2013

BACHER BETTINA, Medienfreiheit und Persönlichkeitsschutz – Zivilrechtliche Auswirkungen der Lösung eines Grundrechtskonflikts, Bâle 2015

CLARINI JULIE, Le journalisme de données : nouveau journalisme ?, Les idées claires, chronique diffusée sur France Culture, 10 février 2011, <https://www.franceculture.fr/emissions/les-idees-claires-de-clementine-autain/le-journalisme-de-donnees-nouveau-journalisme> (consulté le 21 août 2020)

COMMISSION FEDERALE DES MEDIAS, Rapport Aide aux médias : Etat des lieux et recommandations, Bienne, 7 août 2014, <https://www.emek.admin.ch/fr/themes/aide-aux-medias/> (consulté le 21 août 2020)

CONSEIL DE L'EUROPE, Lignes directrices sur la protection de la vie privée dans les médias, Strasbourg 2018, <https://www.coe.int/fr/web/freedom-expression/-/guidelines-on-safeguarding-privacy-in-the-med-1> (consulté le 21 août 2020)

CONSEIL SUISSE DE LA PRESSE, Directives relatives à la « Déclaration des droits et des devoirs du/de la journaliste », <https://presserat.ch/fr/code-de-deontologie-des-journalistes/richtlinien/> (consulté le 21 août 2020)

CURCHOD ALEXANDRE, Liberté d'expression : Guide juridique pratique et perspectives, Lausanne 2019

DEGLISE FABIEN, Le journalisme de données, ou l'art de faire parler les chiffres, Le Devoir (Montréal), 10 septembre 2012

GAMBINI LETIZIA, Une décennie de datajournalisme : qu'est-ce qui a changé ?, European Journalism Observatory, 6 juin 2019, <https://fr.ejo.ch/innovation-et-numerique/decennie-datajournalisme-change-guardian-google-data-donnees> (consulté le 21 août 2020)

GRAY JONATHAN/BOUNEGRU LILIANA/CHAMBERS LUCY (éd.), The Data Journalism Handbook, Sebastopol 2012

HUNTER MARC, *Le journalisme d'investigation en France et aux Etats-Unis*, Paris 1997

LEHMAN LORIC, *Berichterstattung über Corona : Die Sternstunde des Datenjournalismus*, persoenlich.com, 11 juin 2020, <https://www.persoenlich.com/digital/die-sternstunde-des-datenjournalismus> (consulté le 21 août 2020)

POLLICINO ORESTO/SOLDATOV OLEG, *Judicial balancing of human rights online*, in : Susi Mart (éd.), *Human Rights, Digital Society and the Law – A Research Companion*, Oxon/New York 2019, p. 132 ss

ROCHER LUC/HENDRICKX JULIEN M./DE MONTJOYE YVES-ALEXANDRE, *Estimating the success of re-identifications in : incomplete datasets using generative models*, *Nature Communications*, 2019, 10:3069, <https://www.nature.com/articles/s41467-019-10933-3> (consulté le 21 août 2020)

ZELLER FRANZ, *Das Konzept des « verantwortungsvollen Journalismus » rückt ins Zentrum – Entscheidübersicht Verfassungsrecht und EMRK* 2016, *Medialex* 2017

L'atteinte à l'intégrité numérique appréhendée par le droit international privé

La localisation du lieu de l'atteinte à la croisée
du monde physique et de l'espace numérique

par

Florence Guillaume

Professeure à l'Université de Neuchâtel

et

Sven Riva

Assistant-Doctorant à l'Université de Neuchâtel

I. Introduction.....	120
II. Les règles applicables à l'atteinte à l'intégrité numérique.....	122
A. La qualification d'atteinte à la personnalité en droit matériel.....	122
B. La qualification d'acte illicite en droit international privé.....	125
III. La compétence pour les prétentions relatives à une atteinte à l'intégrité numérique.....	127
A. La compétence des tribunaux suisses selon la LDIP	127
B. La compétence des tribunaux suisses selon la Convention de Lugano	129
1. Le principe de l'ubiquité	129
2. Le principe de la mosaïque.....	132
C. La compétence des tribunaux suisses fondée sur une élection de for	135

IV. Le droit applicable aux prétentions relatives à une atteinte à l'intégrité numérique.....	137
A. L'incertitude quant à la loi applicable	137
B. L'intervention de l'ordre public lorsqu'un droit étranger est applicable	140
V. L'insécurité juridique liée au risque de compétence universelle	142
A. Le principe de proximité confronté à l'universalité d'une atteinte à l'intégrité numérique	143
B. Les règles de conflit proposées par l'Institut de droit international.....	145
1. Le principe holistique.....	146
2. La <i>lex fori</i>	149
VI. L'adaptation des règles localisatrices à l'environnement ubiquitaire d'Internet	150
A. Le paradoxe du rattachement de l'atteinte à l'intégrité numérique au territoire d'un Etat	150
1. Une action, un droit ?	151
2. De la proximité à l'ubiquité.....	153
B. La localisation de l'atteinte à l'intégrité numérique dans le monde physique et l'espace numérique	155
1. Internet en tant qu'outil de l'atteinte	156
2. Internet en tant qu'environnement de l'atteinte	157
3. Le dédoublement du lieu de l'atteinte à l'intégrité numérique....	160
C. La localisation de l'atteinte à l'intégrité numérique dans le seul espace numérique.....	163
1. L'avatar comme personne numérique	164
2. L'intelligence artificielle comme personne numérique.....	166
3. La DAO comme personne numérique	167

VII. L'intégrité numérique : un droit fondamental dont l'Etat ne peut être le seul garant	169
A. La relation quasi-étatique entre les plateformes numériques et leurs utilisateurs	169
B. L'obligation des plateformes numériques de protéger les libertés de leurs utilisateurs	171
VIII. Conclusion.....	174
Bibliographie	177

I. Introduction

1. Le colloque organisé à l'Université de Neuchâtel sur la thématique du droit à l'intégrité numérique, au mois de février 2020, a permis de préciser le cadre juridique suisse de la protection de la sphère privée et de la garantie de la liberté personnelle dans le contexte de l'espace numérique. L'analyse faite par des experts des différents domaines du droit a mis en évidence la capacité d'adaptation du droit suisse face aux défis posés par la numérisation de la société.
2. Les changements sociétaux induits par l'évolution technologique ont indéniablement un impact sur l'environnement juridique. Le droit doit pouvoir encadrer les développements technologiques afin d'éviter leur déploiement dans un champ situé hors du cadre légal. L'évolution de la société dans le numérique offre l'opportunité d'adapter la législation fédérale et cantonale en redéfinissant les droits liés à la personne et en conceptualisant de nouveaux droits, tels que le droit à l'intégrité numérique.
3. Le droit doit être conçu de façon à protéger l'être humain et à garantir le respect des droits fondamentaux non seulement dans le monde physique, mais également dans l'espace numérique. Si cette affirmation paraît évidente, elle est également source de discordes. Peut-on réellement parler d'un espace numérique distinct du monde physique ? En soi, l'être humain ne peut pas se téléporter dans le numérique. Une personne naviguant dans cet espace dématérialisé garde tout de même les pieds sur terre. Elle peut tout au plus se créer un ou plusieurs avatars qui la représentent graphiquement dans l'espace numérique.
4. Ce constat amène un auteur¹ à considérer qu'une éventuelle atteinte à la personne d'un individu ou à ses biens serait nécessairement ressentie par l'individu lui-même dans le monde physique, et non pas dans l'espace numérique. Un autre auteur² a la vision d'un espace propre au numérique dans lequel l'individu a une vie

¹ Voir la contribution de JOHAN ROCHEL, *L'intégrité numérique dans la Constitution : Entre liberté et technologies numériques*, pp. 13 ss du présent ouvrage.

² Voir la contribution d'ALEXIS ROUSSEL, *Le droit à l'intégrité numérique de la personne*, pp. 1 ss du présent ouvrage.

numérique méritant d'être protégée par le droit en tant que telle. Tous les auteurs dont les contributions sont réunies dans le présent ouvrage concordent sur la nécessité de mettre l'être humain au centre du débat sur le droit à l'intégrité numérique, lorsqu'il s'agit de façonner des règles de droit protectrices de la sphère privée, l'intégrité physique et psychique et, plus largement, la personnalité des individus. Il ne fait aucun doute que l'être humain est la raison d'être et la finalité du droit.

5. En partant du postulat de l'existence d'un droit à l'intégrité numérique dans le droit suisse, les auteurs de la présente contribution examinent les circonstances dans lesquelles ce droit peut être invoqué devant les tribunaux helvétiques. Cette question n'est pas aussi tautologique qu'elle puisse paraître au premier abord. Les relations juridiques qui se nouent sur Internet se caractérisent par leur potentielle internationalité. Une atteinte à la personnalité sur Internet est fréquemment commise par une personne se trouvant dans un autre pays que celui dans lequel vit la victime. Il est dès lors nécessaire de recourir aux règles de droit international privé pour déterminer à quelles conditions les tribunaux suisses sont compétents pour apporter leur protection à l'intégrité numérique d'une personne, d'une part, et si cette protection peut être accordée à l'aune du droit suisse, d'autre part. L'application du droit suisse dépend donc d'une analyse préalable de droit international privé.
6. Dans cette contribution, nous commencerons par déterminer les circonstances dans lesquelles les règles de droit international privé sont amenées à s'appliquer et, notamment, la qualification d'une atteinte à l'intégrité numérique (II). Les règles sur la protection de la personnalité étant applicables, nous examinerons les cas où les tribunaux civils suisses sont compétents pour juger d'une atteinte à la personnalité ayant une portée internationale (III), ainsi que la manière de déterminer le droit régissant une telle atteinte (IV). Le recours à ces règles pour juger d'une atteinte à l'intégrité numérique fera ressortir une réelle imprévisibilité quant au for et au droit applicable. Cette situation est insatisfaisante dans la mesure où elle est très préjudiciable à la sécurité juridique (V). Cela nous amènera à redéfinir la portée des règles de droit international privé en considérant qu'elles peuvent localiser une atteinte à l'intégrité numérique non seulement dans le monde physique, mais aussi dans

l'espace numérique. Il y a en effet un lieu de l'atteinte sur Internet, car il s'agit d'une sorte de « territoire » et pas seulement d'un « outil » (VI). Ce lieu peut être localisé précisément, notamment lorsque l'atteinte à l'intégrité numérique intervient sur une plateforme. Au vu de la relation quasi-étatique qui s'instaure entre certaines plateformes numériques ayant acquis une position monopolistique et leurs utilisateurs, il apparaît que la plateforme peut devoir assumer le rôle de garant des droits fondamentaux – et notamment du droit à l'intégrité numérique – de ses utilisateurs (VII). Notre analyse de la portée du droit à l'intégrité numérique nous amènera à nous demander, en guise de conclusion, s'il est opportun de soumettre les cas d'atteinte à ce droit à la justice étatique et s'il ne serait pas préférable de créer des modes alternatifs de résolution des conflits en ligne pour ce type de litiges (VIII).

II. Les règles applicables à l'atteinte à l'intégrité numérique

7. Lorsqu'il est porté atteinte à l'intégrité numérique d'une personne, celle-ci peut demander aux tribunaux civils de protéger ses droits en invoquant une atteinte à sa personnalité. Il est en effet permis de considérer que le droit à l'intégrité numérique fait partie du catalogue évolutif des droits de la personnalité existant en droit matériel suisse (A). En droit international privé suisse, les droits de la personnalité sont qualifiés d'actes illicites. Les règles relatives à ce domaine du droit détermineront la compétence des tribunaux suisses pour juger d'une atteinte au droit à l'intégrité numérique. Elles permettront également de savoir si le droit suisse est applicable à la cause (B).

A. La qualification d'atteinte à la personnalité en droit matériel

8. En droit civil suisse, le terme « personnalité » désigne « l'ensemble des biens (ou des valeurs) qui appartiennent à une personne du seul fait de son existence »³. Il s'agit de biens qui n'ont pas de valeur pécuniaire, tels que l'intégrité physique, la vie privée, la réputation

³ DESCHENAUX/STEINAUER, N 515, p. 161.

ou l'honneur. Une atteinte à un bien de la personnalité peut néanmoins entraîner une perte d'ordre pécuniaire ou un tort moral⁴.

9. A chaque bien de la personnalité correspond un droit de la personnalité. Par exemple, la vie privée est protégée par le droit au respect de la vie privée. La protection de la personnalité par le droit civil permet de protéger contre toute atteinte les valeurs ou qualités qui sont étroitement liées à la personne⁵.
10. En l'absence d'un *numerus clausus* des droits de la personnalité, il appartient à la jurisprudence d'interpréter cette notion et de compléter, au fur et à mesure des « modifications de la vie sociale dues au progrès de la science et de la technique », la liste des droits protégés par l'art. 28 CC⁶.
11. L'action en protection de la personnalité⁷ peut aussi bien viser à prévenir une atteinte imminente qu'à faire cesser une atteinte qui dure encore (art. 28 CC). Il est également possible, subsidiairement, d'intenter une action visant à faire constater le caractère illicite d'une atteinte qui a pris fin, mais qui laisse subsister le trouble qu'elle a créé (art. 28a al. 1 ch. 3 CC). L'atteinte à la personnalité doit être illicite (art. 28 al. 1 et al. 2 CC). Ces actions défensives, qui sont propres à la protection contre les atteintes à la personnalité, peuvent être complétées par des actions réparatrices. Une action en dommages-intérêts fondée sur le droit de la responsabilité délictuelle (art. 28a al. 3 CC et art. 41 CO) peut être intentée lorsque l'atteinte à la personnalité a des répercussions sur le patrimoine du lésé et lui cause un dommage économique. En outre, une action en réparation du tort moral (art. 28a al. 3 CC et art. 49 CO) peut également être envisagée lorsque la victime a subi des souffrances physiques, psychiques ou morales graves à la suite d'une atteinte à

⁴ DESCHENAUX/STEINAUER, N 531-533a, pp. 165-166.

⁵ BUCHER, Personnes physiques, N 384, p. 87.

⁶ DESCHENAUX/STEINAUER, N 540-540a, p. 169.

⁷ Pour une description des actions en protection de la personnalité, voir la contribution de MARIE-LAURE PAPAUX VAN DELDEN, Le « droit à l'intégrité numérique » du point de vue de la protection de droit civil de la personnalité, pp. 65 ss du présent ouvrage, spéc. N 39-47, pp. 78-82 ; BUCHER, Personnes physiques, N 554-594, pp. 120-130 ; DESCHENAUX/STEINAUER, N 570-608a, pp. 186-207.

sa personnalité. Enfin, une action en remise du gain réalisé par l'auteur de l'atteinte (art. 28a al. 3 CC et art. 423 CO) permet d'éviter que celui-ci ne s'enrichisse au détriment de la victime⁸.

12. La portée des droits de la personnalité sera interprétée par le juge civil d'une manière conforme aux garanties constitutionnelles des droits fondamentaux⁹. Peuvent être mentionnés à ce titre notamment le droit à la liberté personnelle, et plus particulièrement le respect de l'intégrité physique et psychique (art. 10 al. 2 Cst. féd.), ainsi que la protection de la sphère privée (art. 13 Cst. féd.), laquelle inclut notamment le droit à l'honneur et à la réputation, le droit à l'autodétermination informationnelle, et la protection des données personnelles. Le juge civil assume ainsi un rôle de garant de la protection des droits fondamentaux, aussi bien contre des atteintes survenant dans le monde physique que dans l'environnement d'Internet.
13. Lorsque, par exemple, le juge civil est saisi d'une action visant à protéger le droit à l'honneur et à la réputation d'une personne subissant un lynchage en ligne, la victime invoquera la protection de sa personnalité par l'art. 28 CC. Ce sont en effet les dispositions de droit civil qui imposent aux particuliers des obligations ou des interdictions à l'égard d'autres particuliers¹⁰. Le juge civil appréciera néanmoins l'atteinte à l'honneur et à la réputation à la lumière du droit fondamental consacré à l'art. 13 Cst. féd.

⁸ Les actions mentionnées dans ce paragraphe constituent les principales actions en protection de la personnalité prévues par le droit suisse, mais cette liste n'est pas exhaustive. Les mêmes actions sont en principe également à disposition en cas d'atteinte causée par le traitement illicite de données personnelles (art. 15 al. 1 LPD).

⁹ Voir MAHON, Droit constitutionnel II, N 27, pp. 47-48.

¹⁰ Les droits fondamentaux ne peuvent en principe pas être invoqués directement à l'égard d'un autre particulier. Il faut cependant réserver l'hypothèse où une personne privée a une position à ce point dominante sur le marché pour qu'il soit légitime qu'un particulier puisse exiger d'elle le respect de ses droits fondamentaux. Voir MAHON, Droit constitutionnel II, N 27, pp. 46-47. La question pourrait se poser, par exemple, du droit à l'autodétermination informationnelle à l'égard d'une entreprise qui fait partie des géants du Web (p.ex. Google, Facebook, Apple).

14. Il est dès lors permis de considérer que le juge suisse peut accorder une protection du droit à l'intégrité numérique en appliquant les règles de droit civil sur la protection des droits de la personnalité¹¹.
15. En droit suisse, l'atteinte à la personnalité qui se produit sur Internet englobe les aspects civils de la protection de la personnalité (p.ex. le droit à l'honneur ou à la réputation, le droit à l'intégrité physique ou psychique) ainsi que l'aspect plus particulier de la protection des données personnelles¹². Nous n'examinerons pas dans la présente contribution les questions ayant trait spécifiquement à la protection des données numériques et limiterons donc notre propos à la protection générale de la personnalité par les art. 28 ss CC.

B. La qualification d'acte illicite en droit international privé

16. La double question de la compétence internationale des tribunaux suisses et du droit applicable à la cause ne se pose que si la situation considérée est internationale. Cela implique, par exemple, que l'auteur de l'atteinte à la personnalité et la victime de cette atteinte soient domiciliés dans des Etats différents, ou que l'acte à l'origine de l'atteinte ait été commis dans un autre Etat que celui où vit la victime. S'agissant d'une atteinte à l'intégrité numérique, ou plus généralement d'une atteinte à la personnalité commise sur Internet, on peut admettre qu'il s'agit en principe d'une situation internationale justifiant l'application des règles de droit international privé. Dès lors qu'un contenu mis en ligne est accessible simultanément partout dans le monde, il sera rare en pratique que tous les éléments de rattachement se trouvent dans le même Etat. Ce n'est que dans cette hypothèse exceptionnelle que la situation juridique serait purement interne.
17. La compétence des tribunaux helvétiques est déterminée par les règles de droit international privé suisses lorsqu'une situation

¹¹ Voir PAPAUX VAN DELDEN, N 26-34, pp. 73-77.

¹² La protection des données personnelles est régie par une loi spéciale : la Loi fédérale sur la protection des données du 19 juin 1992 (LPD ; RS 235.1). Voir p.ex. BUCHER, Personnes physiques, N 461-467, pp. 101-102. Cette loi s'applique notamment pour protéger la personnalité des individus dans le numérique.

juridique est internationale¹³. Ces règles, qui figurent essentiellement dans la Loi fédérale sur le droit international privé (LDIP)¹⁴ et la Convention de Lugano (CL)¹⁵, contiennent des critères de rattachement permettant de localiser la situation juridique considérée dans l'Etat avec lequel la cause présente les liens les plus étroits conformément au principe de proximité. Les critères de rattachement sont, par exemple, le domicile du défendeur ou du demandeur, ou le lieu où l'acte à l'origine de l'atteinte a été commis ou celui où le résultat de l'atteinte s'est fait ressentir. Il existe un for en Suisse si (au moins) une règle de conflit de juridictions rattache la cause au territoire suisse.

18. Lorsque les tribunaux helvétiques sont compétents, le droit applicable est déterminé par les règles de conflit de lois se trouvant en principe dans la LDIP. Ces règles sont également des règles localisatrices se référant à des critères de rattachement permettant d'identifier l'Etat avec lequel la cause présente les liens les plus étroits. Ces critères sont semblables à ceux utilisés pour la compétence des tribunaux mais ne sont pas nécessairement identiques. Il en résulte que le juge suisse ne va pas nécessairement résoudre le litige en appliquant le droit matériel suisse.
19. Les prétentions fondées sur une atteinte à la personnalité sont qualifiées, en droit international privé suisse, d'actes illicites. Cette qualification résulte de l'art. 33 al. 2 LDIP dont le texte précise que « les atteintes aux intérêts personnels sont régies par les dispositions de la [LDIP] relatives aux actes illicites ». La protection de la personnalité en droit international privé relève par conséquent du domaine des actes illicites¹⁶.
20. Les règles de droit international privé régissant les actes illicites sont ainsi applicables pour déterminer si les tribunaux suisses sont compétents pour juger d'une action en prévention ou en cessation

¹³ Les dispositions du Code de procédure civile suisse du 19 décembre 2008 (CPC ; RS 272), à savoir les art. 36 à 39 CPC, ne sont dès lors pas applicables.

¹⁴ Loi fédérale sur le droit international privé du 18 décembre 1987 (LDIP ; RS 291).

¹⁵ Convention de Lugano concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale du 30 octobre 2007 (CL ; RS 0.275.12).

¹⁶ Voir p.ex. BUCHER, CR-LDIP/CL, art. 33 LDIP, N 2, p. 376 ; DUTOIT, Actes illicites sur Internet, pp. 143-144 ; KAUFMANN-KOHLER, p. 91.

de l'atteinte à l'intégrité numérique et, le cas échéant, en réparation du dommage. La portée exacte du droit à l'intégrité numérique dépendra de la loi désignée par les règles de droit international privé relatives aux actes illicites. Le droit à l'intégrité numérique du lésé aura par conséquent les contours définis par le droit suisse uniquement si ses droits de la personnalité sont régis par le droit suisse.

III. La compétence pour les prétentions relatives à une atteinte à l'intégrité numérique

21. La compétence internationale des tribunaux suisses, pour une prétention de nature civile fondée sur une atteinte à l'intégrité numérique, est déterminée par la LDIP (A), respectivement la Convention de Lugano (B) lorsque la cause entre dans le champ d'application de cette convention. Les parties peuvent écarter le for désigné par la LDIP ou la Convention de Lugano, au profit du for de leur choix, en procédant à une élection de for (C).
22. En l'absence de règles consacrées à la protection de l'intégrité numérique, les règles de droit international privé régissant la protection de la personnalité sont applicables. Lorsqu'une personne subit une atteinte à ses droits de la personnalité, elle peut saisir le juge civil d'une action en prévention ou en cessation de l'atteinte ainsi que d'une action en réparation du dommage¹⁷.

A. La compétence des tribunaux suisses selon la LDIP

23. Pour les litiges relatifs aux actes illicites, la compétence des tribunaux suisses est donnée par l'art. 129 LDIP qui prévoit un for en Suisse si le défendeur a son domicile ou sa résidence habituelle¹⁸ en Suisse, d'une part, ou lorsque l'acte illicite ou son résultat s'est

¹⁷ Voir *supra* N 11.

¹⁸ Une personne a son domicile en Suisse si elle y réside avec l'intention de s'y établir, respectivement sa résidence habituelle en Suisse si elle y vit pendant une certaine durée (art. 20 al. 1 lit. a et b LDIP). La résidence habituelle n'est en principe prise en considération que lorsque la personne n'a pas de domicile (art. 20 al. 2 LDIP). Toutefois, l'art. 129 LDIP prescrit un for en Suisse lorsque le lésé a son domicile à l'étranger et sa résidence habituelle en Suisse.

produit en Suisse, d'autre part¹⁹. Ces fors sont ouverts pour toute action fondée sur une atteinte à la personnalité, et notamment une atteinte à l'intégrité physique ou psychique²⁰. Ils sont également pertinents pour la protection de l'intégrité numérique²¹.

24. Il ressort de la jurisprudence que le lieu du résultat se trouve à l'endroit où s'est produit le dommage initial, à savoir la lésion directe et immédiate du bien ou de l'intérêt juridique protégé²². En cas d'atteinte à la personnalité, « seule l'atteinte à l'honneur, à la réputation et à la considération du lésé constitue le dommage initial »²³.
25. Lorsque l'atteinte à la personnalité survient sur Internet, le dommage initial se concrétise « en tous les lieux où il est possible d'accéder aux informations illicites, à savoir n'importe où dans le monde en pratique »²⁴. Dans le cadre de l'interprétation du for au lieu du résultat au sens de l'art. 129 LDIP, la jurisprudence considère ainsi que la simple accessibilité à un site Internet en Suisse ouvre un for dans ce pays²⁵. La doctrine préconise néanmoins d'exiger un autre point de rattachement que la simple possibilité d'avoir accès au texte offensant en Suisse pour que la compétence des tribunaux suisses puisse être admise, de manière à rétablir une certaine prévisibilité au niveau du for du lieu du résultat²⁶.
26. Les tribunaux helvétiques sont également compétents lorsque le dommage économique s'est fait ressentir en Suisse. Le for du lieu du résultat correspond, dans ce cas, en principe au for du domicile du lésé, car c'est généralement en ce lieu qu'est ressenti le dommage économique. Toutefois, la jurisprudence admet qu'en présence d'un

¹⁹ L'art. 129 LDIP prévoit, en outre, un for au lieu de l'établissement d'une société pour les actions relatives à l'activité de cet établissement en Suisse.

²⁰ BONOMI, CR-LDIP/CL, art. 129 LDIP, N 3, p. 1096.

²¹ Voir *supra* N 14.

²² ATF 125 III 103, consid. 2b/aa ; TF 4C.98/2003 du 15 juin 2004, consid. 2.2.

²³ Arrêt de la Cour de justice de Genève du 26 août 2016, ACJC/1116/2016, consid. 4.1.3.

²⁴ DUTOIT, Commentaire, art. 129 LDIP, N 15, p. 585. Dans le même sens : KAUFMANN-KOHLER, p. 115.

²⁵ TF 4A_92/2011 du 9 juin 2011, consid. 2 .

²⁶ DUTOIT, Commentaire, art. 129 LDIP, N 15, pp. 585-586.

préjudice purement patrimonial, le lieu du résultat ne correspond pas nécessairement au domicile du lésé²⁷.

B. La compétence des tribunaux suisses selon la Convention de Lugano

27. La compétence des tribunaux suisses ne peut être fondée sur les règles de conflit de juridictions de la LDIP que si la Suisse n'est pas partie à une convention internationale réglant la compétence internationale²⁸. Les prétentions fondées sur une atteinte à la personnalité entrent clairement dans le champ d'application matériel de la Convention de Lugano²⁹. Les règles de for contenues dans cette convention s'appliquent lorsque le défendeur est domicilié dans un Etat contractant (art. 3 par. 1 CL). Il en résulte qu'il n'est pas possible de fonder la compétence des tribunaux suisses sur une disposition de la LDIP lorsque le défendeur est domicilié dans un Etat contractant de la Convention de Lugano. Si le défendeur est domicilié, par exemple, en Suisse, la compétence des tribunaux suisses doit impérativement être fondée sur une règle de conflit de juridictions de la Convention de Lugano³⁰.

1. Le principe de l'ubiquité

28. La Convention de Lugano permet d'introduire une action fondée sur une atteinte à la personnalité, pour prévenir ou faire cesser l'atteinte, complétée le cas échéant d'une action en dommages-intérêts³¹, à trois fors différents.

²⁷ ATF 133 III 323, consid. 2.3 ; ATF 125 III 103, consid. 2b/bb.

²⁸ L'art. 1 al. 2 LDIP réserve la primauté des conventions internationales en ces termes : « Les traités internationaux sont réservés ».

²⁹ La Convention de Lugano s'applique en matière civile et commerciale au sens de l'art. 1 par. 1 et 2 CL.

³⁰ L'existence d'un domicile du défendeur en Suisse au sens de la Convention de Lugano est examinée par le juge saisi en appliquant « sa loi interne » (art. 59 par. 1 CL), à savoir l'art. 20 LDIP. Pour déterminer si le défendeur a son domicile dans un autre Etat contractant de la Convention de Lugano, le juge suisse appliquera la loi de cet Etat (art. 59 par. 2 CL).

³¹ Voir *supra* N 11 pour les actions admissibles en droit suisse.

29. Le premier for se trouve dans l'Etat du domicile du défendeur (art. 2 par. 1 CL)³². Comme la Convention de Lugano a la primauté sur les règles de droit international privé nationales, la compétence internationale des tribunaux suisses ne peut pas être fondée sur l'art. 129 LDIP lorsque le domicile du défendeur se trouve en Suisse. Toutefois, cette disposition est nécessaire pour déterminer la compétence interne, autrement dit pour identifier le canton dans lequel l'action doit être introduite lorsque le défendeur a son domicile en Suisse³³.
30. Lorsqu'il s'agit de statuer sur une atteinte à la personnalité commise par l'intermédiaire d'Internet, le for du domicile du défendeur n'est souvent pas approprié. L'éloignement entre l'auteur de l'atteinte et la victime est un empêchement sérieux à l'introduction d'une action en justice dans l'Etat du domicile du défendeur. Si Internet facilite considérablement les contacts entre des personnes physiquement éloignées, il n'en reste pas moins que les distances terrestres subsistent. En outre, en cas de pluralité d'auteurs, comme cela sera par exemple souvent le cas dans une situation de cyberharcèlement, il y aura une multiplication des rattachements à tous les domiciles des auteurs, si tant est que ceux-ci puissent être identifiés. Cela peut conduire à une infinité de fors. Dans le domaine des atteintes à la personnalité commises sur Internet, les autres fors ont dès lors une importance accrue³⁴.
31. Le deuxième et le troisième fors figurent à l'art. 5 ch. 3 CL. Cette disposition offre la possibilité d'attirer un défendeur domicilié dans un Etat contractant de la Convention de Lugano « en matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire ». Comme il s'agit d'une compétence internationale et interne, la compétence à

³² Le juge suisse applique l'art. 20 LDIP pour déterminer si le défendeur a son domicile en Suisse lorsqu'il fonde sa compétence sur la Convention de Lugano (art. 59 al. 1 LDIP).

³³ Sur la différence entre la compétence internationale (déterminée par l'art. 2 par. 1 CL) et la compétence interne (déterminée par l'art. 129 LDIP), voir GUILLAUME, N 32, pp. 64-66.

³⁴ KAUFMANN-KOHLER, p. 111 ; DUTOIT, Actes illicites sur Internet, p. 160.

raison du lieu est fixée directement par la Convention de Lugano et l'art. 129 LDIP n'est pas applicable dans ce cadre³⁵.

32. Les fors prescrits à l'art. 5 CL sont des fors alternatifs à celui du domicile du défendeur consacré à l'art. 2 par. 1 CL. Il en résulte que le demandeur a le choix entre le for du domicile du défendeur et le ou les fors de l'art. 5 CL lorsque le défendeur est domicilié dans un Etat contractant de la Convention de Lugano et que cette disposition prévoit la compétence des tribunaux d'un autre Etat contractant³⁶.
33. La notion de « matière délictuelle ou quasi délictuelle » au sens de l'art. 5 ch. 3 CL doit être interprétée de façon autonome en se référant « au système et aux objectifs » de la Convention de Lugano³⁷. La jurisprudence de la Cour de justice de l'Union européenne (CJUE) a précisé cette notion en considérant qu'elle englobe « toute demande qui vise à mettre en jeu la responsabilité d'un défendeur, et qui ne se rattache pas à la “matière contractuelle” au sens de l'article 5, paragraphe 1 »³⁸. On peut admettre sans autre que les atteintes à la personnalité, et notamment les atteintes à l'intégrité numérique, sont qualifiées de prétentions délictuelles ou quasi délictuelles au sens de l'art. 5 ch. 3 CL.
34. La compétence spéciale prescrite à l'art. 5 ch. 3 CL « est fondée sur l'existence d'un lien de rattachement particulièrement étroit entre la contestation et les juridictions du lieu où le fait dommageable s'est produit ou risque de se produire, qui justifie une attribution de compétence à ces dernières pour des raisons de bonne administration de la justice et d'organisation utile du procès »³⁹.

³⁵ Sur les notions de compétence internationale et interne, voir GUILLAUME, N 24, pp. 40-42.

³⁶ Sur l'articulation entre le for de l'art. 2 par. 1 CL et ceux de l'art. 5 CL, voir GUILLAUME, N 48, pp. 97-99.

³⁷ Voir p.ex. CJUE, 17.10.2017, *Bolagsupplysningen c. Svensk Handel*, C-194/16, ECLI:EU:C:2017:766, consid. 25. Cet arrêt rappelle que l'interprétation fournie par la Cour de justice pour l'art. 5 ch. 3 du Règlement (CE) n° 44/2001, dont le texte est identique à celui de l'art. 5 ch. 3 CL, vaut également pour l'art. 7 ch. 2 du Règlement (UE) n° 1215/2012 (*ibid.*, consid. 24).

³⁸ CJCE, 27.09.1988, *Athanasios Kalfelis c. Bankhaus Schröder*, C-189/87, Rec. 1988 p. 5565, ECLI:EU:C:1988:459, consid. 17.

³⁹ Voir p.ex. CJUE, *Bolagsupplysningen* (*supra* note 37), consid. 26.

Cette compétence a la particularité de présenter un lien de rattachement étroit avec deux lieux différents : le lieu de l'événement causal, d'une part, et le lieu de la matérialisation du dommage, d'autre part. La Cour de justice de l'Union européenne a jugé depuis longtemps que cette disposition permet d'agir aussi bien au « lieu où a été commis le fait qui a eu le dommage pour conséquence » qu'au « lieu où le dommage est survenu ou s'est manifesté »⁴⁰. En consacrant ainsi la théorie de l'ubiquité dans le domaine délictuel ou quasi délictuel, la jurisprudence européenne offre au demandeur le choix d'agir en justice dans deux autres Etats que celui du domicile du défendeur.

2. Le principe de la mosaïque

35. Lorsque le dommage s'est produit dans plusieurs Etats contractants de la Convention de Lugano, l'art. 5 ch. 3 CL permet au demandeur d'agir en justice dans chacun des Etats où le dommage est survenu ou s'est manifesté. Si le lésé choisit d'agir dans les différents Etats où il a subi une atteinte à sa personnalité, il doit fractionner ses prétentions et ne peut demander réparation du dommage, dans chaque Etat, que pour le dommage subi dans cet Etat. La Cour de justice de l'Union européenne a consacré le « principe de la mosaïque » en jugeant que le tribunal ne peut statuer, dans ce type de situation, que sur le préjudice subi dans l'Etat du for⁴¹. Si le lésé souhaite demander l'intégralité de ses prétentions en réparation du dommage dans le cadre d'une seule procédure, alors que le dommage s'est matérialisé dans plusieurs Etats, il doit agir au for de l'événement causal (art. 5 ch. 3 CL) ou au for du domicile du défendeur (art. 2 par. 1 CL).
36. Par exemple, dans le cas d'une atteinte à la personnalité portée par un article de presse diffusé dans plusieurs Etats contractants de la Convention de Lugano, il a été jugé que « la victime peut intenter

⁴⁰ Voir p.ex. CJCE, 30.11.1976, *Handelskwekerij G.J. Bier c. Mines de potasse d'Alsace*, Aff. 21/76, Rec. 1976 p. 1735, ECLI:EU:C:1976:166 ; CJCE, 19.09.1995, *Antonio Marinari c. Lloyds Bank*, C-364/93, Rec. 1995 I-2719, ECLI:EU:C:1995:289, consid. 12.

⁴¹ CJCE, 07.03.1995, *Fiona Shevill c. Presse Alliance*, C-68/93, Rec. 1995 I-415, ECLI:EU:C:1995:61, consid. 30 ; CJUE, 25.10.2011, *eDate Advertising c. X*, C-509/09, Rec. 2011 I-10269, ECLI:EU:C:2011:685, consid. 51.

contre l'éditeur une action en réparation soit devant les juridictions de l'Etat contractant du lieu d'établissement de l'éditeur de la publication diffamatoire, compétentes pour réparer l'intégralité des dommages résultant de la diffamation, soit devant les juridictions de chaque Etat contractant dans lequel la publication a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation, compétentes pour connaître des seuls dommages causés dans l'Etat de la juridiction saisie »⁴². Dans cette affaire, comme souvent, le for de l'événement causal coïncidait avec le for du domicile du défendeur et n'élargissait donc pas la palette des fors à disposition.

37. La jurisprudence a également précisé que le lieu de la matérialisation du dommage correspond au lieu où l'acte illicite a produit directement ses effets dommageables à l'égard de la personne qui en est la victime immédiate⁴³. Le for se trouve donc au lieu où est survenu le dommage initial, et non pas au lieu où le lésé a subi un préjudice patrimonial consécutif au dommage initial⁴⁴.
38. Dans un arrêt de principe concernant la portée de l'art. 5 ch. 3 CL, la Cour de justice de l'Union européenne a jugé qu'en cas d'atteinte à la personnalité au moyen de contenus mis en ligne sur un site Internet, la personne qui s'estime lésée a la faculté d'agir en responsabilité pour l'intégralité du dommage causé soit devant les juridictions de l'Etat contractant dans lequel se trouve le domicile de l'émetteur du contenu (i.e. au for du lieu de l'événement causal), soit devant les juridictions de l'Etat contractant dans lequel le demandeur a le centre de ses intérêts (i.e. au for du lieu de la matérialisation du dommage)⁴⁵. C'est en effet principalement dans ce dernier Etat que la réputation de la victime est entachée par un contenu mis en ligne sur un site Internet⁴⁶.

⁴² CJCE, *Shevill* (*supra* note 41), consid. 33.

⁴³ CJCE, *Marinari* (*supra* note 40), consid. 14 et 15.

⁴⁴ CJCE, 10.06.2004, *Rudolf Kronhofer c. Marianne Maier*, C-168/02, Rec. 2004 I-6009, ECLI:EU:C:2004:364, consid. 19.

⁴⁵ CJUE, *eDate Advertising* (*supra* note 41), consid. 52 (concernant la portée de l'art. 5 ch. 3 du Règlement (CE) n° 44/2001, dont le texte est identique à celui de l'art. 5 ch. 3 CL).

⁴⁶ L'application du critère du centre des intérêts est préconisée par une partie de la doctrine suisse dans le cadre de l'interprétation de l'art. 129 LDIP. A notre

39. La Cour de justice a précisé au sujet du centre des intérêts de la victime que « [l']endroit où une personne a le centre de ses intérêts correspond en général à sa résidence habituelle. Toutefois, une personne peut avoir le centre de ses intérêts également dans un Etat membre où elle ne réside pas de manière habituelle, dans la mesure où d'autres indices tels que l'exercice d'une activité professionnelle peuvent établir l'existence d'un lien particulièrement étroit avec cet Etat »⁴⁷.
40. Lorsque la victime est une personne morale poursuivant une activité économique, le centre des intérêts correspond au « lieu où sa réputation commerciale est la plus établie et doit, donc, être déterminé en fonction du lieu où elle exerce l'essentiel de son activité économique »⁴⁸. Ce lieu correspond en principe au siège statutaire de la société, sauf lorsque la personne morale exerce la majeure partie de ses activités dans un autre Etat que celui de son siège statutaire⁴⁹. Le for se trouvera donc dans l'Etat où l'atteinte à la réputation est « ressentie le plus fortement »⁵⁰. La nature matérielle ou immatérielle du dommage est sans incidence sur la détermination du centre des intérêts de la victime⁵¹.
41. Le critère du centre des intérêts de la victime répond à l'objectif de prévisibilité des règles de compétence, puisqu'il permet « à la fois au demandeur d'identifier facilement la juridiction qu'il peut saisir et au défendeur de prévoir raisonnablement celle devant laquelle il peut être attiré »⁵². Pour cette raison, le for du centre des intérêts de la victime ne peut pas être invoqué lorsqu'il n'est pas possible d'identifier ce lieu, notamment lorsqu'il n'est pas possible de

connaissance, il n'a été repris à ce jour que par quelques arrêts cantonaux. Voir p.ex. Arrêt de la Cour de justice de Genève du 26 août 2016, ACJC/1116/2016, consid. 4.2.2.

⁴⁷ CJUE, *eDate Advertising* (*supra* note 41), consid. 49.

⁴⁸ CJUE, *Bolagsupplysningen* (*supra* note 37), consid. 41.

⁴⁹ CJUE, *Bolagsupplysningen* (*supra* note 37), consid. 41 et 42.

⁵⁰ CJUE, *Bolagsupplysningen* (*supra* note 37), consid. 42.

⁵¹ CJUE, *Bolagsupplysningen* (*supra* note 37), consid. 37.

⁵² CJUE, *eDate Advertising* (*supra* note 41), consid. 50.

déterminer l'Etat dans lequel une personne morale exerce son activité économique de façon prépondérante⁵³.

42. Conformément à la jurisprudence ayant consacré le principe de la mosaïque, il est également possible d'introduire une action en responsabilité dans chaque Etat « sur le territoire duquel un contenu mis en ligne est accessible ou l'a été », à condition de fractionner les prétentions en dommages-intérêts en limitant chaque action au dommage causé sur le territoire de l'Etat de la juridiction saisie⁵⁴. Par exemple, le simple fait qu'il soit possible d'accéder en Suisse à des propos diffamatoires publiés sur un réseau social (p.ex. Twitter) crée un lien suffisamment étroit avec cet Etat. Mais dans ce cas, d'éventuelles prétentions en dommages-intérêts devraient être limitées au dommage causé sur le territoire suisse conformément au principe de la mosaïque.
43. Les tribunaux suisses, et en particulier le Tribunal fédéral, s'inspirent de la jurisprudence rendue par la Cour de justice de l'Union européenne en lien avec l'interprétation de l'art. 5 ch. 3 CL lorsqu'ils examinent leur compétence au regard de cette disposition⁵⁵.

C. La compétence des tribunaux suisses fondée sur une élection de for

44. Les parties au litige ont la possibilité de convenir du for, avant ou après la naissance du différend, au moyen d'une prorogation de

⁵³ Voir p.ex. CJUE, *Bolagsupplysningen* (*supra* note 37), consid. 43.

⁵⁴ CJUE, *eDate Advertising* (*supra* note 41), consid. 51.

⁵⁵ Lorsqu'il interprète la Convention de Lugano, le juge suisse reprend en principe la jurisprudence de la Cour de justice de l'Union européenne sur l'interprétation de la Convention de Lugano, du Règlement (CE) n° 44/2001 ou du Règlement (UE) n° 1215/2012, conformément à l'art. 1 du Protocole n° 2 de la Convention de Lugano. Les dispositions de ces textes doivent être interprétées de façon semblable lorsqu'elles peuvent être considérées comme équivalentes (CJCE, 16.07.2009, *Zuid-Chemie c. Philippo's Mineralenfabriek*, C-189/08, Rec. 2009 I p. 6917, ECLI:EU:C:2009:475, consid. 18). Voir p.ex. ATF 140 III 320, consid. 6.1 ; ATF 124 III 382, consid. 6c et d. On relèvera que les tribunaux suisses n'ont pas encore adopté le principe de la mosaïque lorsqu'ils fondent leur compétence sur l'art. 129 LDIP. L'application de ce principe, qui a été développé en lien avec l'interprétation de l'art. 5 ch. 3 CL, lorsque la compétence est fondée sur l'art. 129 LDIP est controversée dans la doctrine suisse.

compétence (art. 5 LDIP ; art. 23 CL). Dans un contexte international, la prorogation de compétence présente l'avantage de supprimer l'incertitude quant au juge compétent et le risque de devoir participer à des procédures se déroulant en parallèle dans plusieurs juridictions⁵⁶.

45. Les parties peuvent choisir de soumettre leur litige aux tribunaux suisses quand bien même aucun élément de rattachement objectif localise la cause en Suisse. Il est également possible de simplement désigner les tribunaux d'un canton particulier afin de clarifier la situation dans l'hypothèse où l'art. 129 LDIP ouvrirait des fors dans plusieurs cantons suisses. Le tribunal élu devra en principe accepter sa compétence et statuer au fond, sauf si la cause n'a pas de lien suffisant avec le for choisi par les parties. Il existe un lien suffisant lorsque l'une des parties a son domicile ou sa résidence habituelle dans le canton dont les tribunaux ont été choisis ou lorsque le droit suisse est applicable au litige (art. 5 al. 3 LDIP). Le tribunal élu ne peut pas décliner sa compétence si l'une ou l'autre de ces conditions est remplie⁵⁷.
46. En présence d'une prorogation de compétence, le champ d'application personnel de la Convention de Lugano est étendu à la situation où le demandeur a son domicile dans un Etat contractant. Autrement dit, la compétence du tribunal choisi par les parties doit être examinée au regard des conditions de validité de l'élection de for prescrites à l'art. 23 CL – et non pas celles de l'art. 5 LDIP lorsque les parties ont choisi un tribunal suisse – si le demandeur ou le défendeur est domicilié dans un Etat contractant. Il en résulte que les règles de conflit nationales relatives à l'élection de for (p.ex. l'art. 5 LDIP) ont un champ d'application très restreint.

⁵⁶ Les prorogations de compétence, même exclusives, ne sont cependant pas toujours respectées par les parties. Il n'est, dès lors, pas possible d'exclure totalement le risque de procédures parallèles. Le juge suisse peut suspendre la cause lorsqu'il a été saisi en second lieu aux conditions prescrites à l'art. 9 LDIP.

⁵⁷ GUILLAUME, N 37, pp. 75-77.

IV. Le droit applicable aux prétentions relatives à une atteinte à l'intégrité numérique

47. Lorsque les tribunaux suisses sont compétents pour juger de prétentions fondées sur une atteinte à l'intégrité numérique, le droit applicable doit être déterminé par les règles de conflit de lois figurant dans la LDIP. Si le droit suisse est applicable, le lésé peut demander la protection de son intégrité numérique au moyen d'une action civile en protection de la personnalité (art. 28 CC)⁵⁸. Toutefois, les tribunaux suisses n'appliquent pas nécessairement le droit suisse et peuvent donc être amenés à devoir statuer sur une éventuelle atteinte à l'intégrité numérique au regard d'un droit étranger.
48. Le droit applicable aux atteintes à la personnalité est en principe déterminé au moyen des règles de conflit de lois régissant les actes illicites. Il existe cependant une règle spéciale pour la violation des droits de la personnalité sur Internet qui s'applique également à l'atteinte à l'intégrité numérique (A). Lorsqu'une telle atteinte doit être examinée à l'aune de la protection offerte par un droit étranger, la question se pose de savoir s'il est possible d'appliquer le droit suisse pour offrir une meilleure protection au lésé (B).

A. L'incertitude quant à la loi applicable

49. En matière d'actes illicites – et notamment d'actes illicites commis sur Internet – la loi offre aux parties la possibilité de s'entendre sur l'application du droit suisse en concluant une election de droit après la survenance de l'événement dommageable (art. 132 LDIP)⁵⁹. A défaut d'élection de droit, le droit applicable est déterminé au moyen de critères de rattachement objectifs tels que le lieu de la

⁵⁸ Voir *supra* N 11.

⁵⁹ L'élection de droit et la prorogation de compétence sont indépendantes l'une de l'autre. Les parties ont ainsi la possibilité de s'entendre sur le for sans convenir du droit applicable, et vice versa.

résidence habituelle de l'auteur ou du lésé, le lieu où l'acte illicite a été commis ou le lieu du résultat de l'acte illicite (art. 133 LDIP)⁶⁰.

50. La détermination du lieu de l'acte est délicate s'agissant d'un acte illicite commis sur Internet qui est un environnement par essence transnational. La doctrine admet que ce lieu correspond, par exemple, au lieu où un email diffamatoire est chargé dans un ordinateur accessible au réseau⁶¹. La détermination du lieu de l'acte peut se révéler cependant très problématique, en pratique, pour ce type de délit. Comme le relève un auteur, « [i]l ne fait pas de doute que ce lieu de chargement pourra se révéler difficile à prouver par le lésé, car l'auteur est tenté d'utiliser tous les moyens techniques à sa disposition pour camoufler ce lieu ou le rendre introuvable »⁶². Par ailleurs, le lieu de l'acte de chargement est, la plupart du temps, fortuit. Un email peut être envoyé par ordinateur portable ou smartphone depuis n'importe quel endroit où le réseau Internet est accessible. Faute d'accessibilité immédiate au réseau, l'email sera stocké en attente et envoyé automatiquement dès que la connexion à Internet aura pu être établie. Enfin, le lieu d'envoi d'un email est très facilement manipulable par l'auteur qui peut choisir unilatéralement de situer son acte dans un Etat dont la législation lui est favorable.
51. Quant au lieu du résultat d'un acte illicite commis sur Internet, il est encore plus délicat à déterminer. Un tel acte produit en effet un résultat potentiellement partout dans le monde où il est possible d'accéder à Internet, en raison de l'ubiquité mondiale de cette technologie⁶³.
52. La question de la violation des droits de la personnalité sur Internet fait l'objet d'une disposition spéciale visant les atteintes à la personnalité « par les médias, notamment par la voie de la presse, de la radio, de la télévision ou de tout autre moyen public

⁶⁰ La règle générale de l'art. 133 LDIP cède le pas à la règle spéciale de l'art. 139 LDIP en cas de violation des droits de la personnalité sur Internet. Voir *infra* N 52.

⁶¹ Voir p.ex. DUTOIT, Commentaire, art. 133 LDIP, N 11, p. 598 ; KAUFMANN-KOHLER, pp. 111-112.

⁶² DUTOIT, Actes illicites sur Internet, p. 149.

⁶³ DUTOIT, Commentaire, art. 133 LDIP, N 11, p. 598.

d'information » (art. 139 al. 1 LDIP)⁶⁴. Il faut admettre avec la doctrine⁶⁵ qu'un site Internet constitue un « moyen public d'information » au sens de l'art. 139 LDIP. Cette norme s'applique également en cas d'atteinte à l'intégrité numérique commise sur Internet.

53. L'application de cette disposition spéciale a pour effet que le lésé a le choix d'invoquer l'un des droits suivants : le droit de l'Etat de la résidence habituelle de l'auteur (art. 139 al. 1 lit. b LDIP), le droit de l'Etat de la résidence habituelle du lésé (art. 139 al. 1 lit. a LDIP) ou le droit de l'Etat dans lequel le résultat de l'acte illicite s'est produit (art. 139 al. 1 lit. c LDIP). Le lésé peut choisir librement le droit qu'il entend appliquer à sa prétention, et donc opter pour le droit qui lui est le plus favorable. Les deux derniers droits ne peuvent cependant être choisis par le lésé que si « l'auteur du dommage [devait] s'attendre à ce que le résultat se produise dans cet Etat ».
54. L'appréciation de la condition de la prévisibilité de la survenance du dommage dans un Etat dépend des circonstances. S'agissant d'une atteinte à la personnalité commise sur Internet, l'information peut être accessible dans la presque totalité des Etats. Certains auteurs réservent cependant l'hypothèse où la langue utilisée est peu répandue⁶⁶. Mais cet obstacle perd de son importance au fur et à mesure de la mise à disposition de tout un chacun, sur Internet, d'outils de traduction performants. En outre, lorsqu'une information se propage rapidement dans une certaine langue, il n'est pas rare que celle-ci soit reprise puis traduite par des internautes à travers le monde, contribuant ainsi à la propagation de l'information. Partant, l'auteur peut en principe s'attendre à ce que son acte ait une répercussion internationale, de telle sorte que la

⁶⁴ L'art. 139 al. 1 LDIP s'applique également aux atteintes à la personnalité résultant du traitement de données personnelles ainsi qu'aux entraves au droit d'accès aux données personnelles (art. 139 al. 3 LDIP). En revanche, le droit applicable au droit de réponse à l'encontre des médias à caractère périodique est déterminé par l'art. 139 al. 2 LDIP. A ce sujet, voir DUTOIT, Actes illicites sur Internet, pp. 154-155.

⁶⁵ DUTOIT, Commentaire, art. 139 LDIP, N 9, p. 635 ; BONOMI, CR-LDIP/CL, art. 139 LDIP, N 2, p. 1159, et réf. citées.

⁶⁶ BONOMI, CR-LDIP/CL, art. 139 LDIP, N 7, p. 1160, et réf. citées.

condition de la prévisibilité de la survenance du dommage doit être facilement admise.

55. Compte tenu de la difficulté – voire l'impossibilité – à déterminer le lieu du résultat ou, au moins, un nombre déterminé de lieux du résultat, ce rattachement crée une incertitude considérable quant au droit applicable à une atteinte à la personnalité sur Internet. A priori, le droit de n'importe quel Etat pourrait en effet s'appliquer aux prétentions du lésé. Pour cette raison, la doctrine préconise un rattachement au lieu de la résidence habituelle du lésé. Certains auteurs vont jusqu'à admettre que le lésé a la possibilité de choisir le droit de sa résidence habituelle même s'il n'y a pas eu de dommage matérialisé dans cet Etat⁶⁷. Autrement dit, la condition de la prévisibilité de la survenance du dommage devrait être considérée comme remplie si l'auteur pouvait prévoir, au moment de l'acte, qu'un dommage était susceptible de se produire dans l'Etat de la résidence habituelle du lésé, même si aucun préjudice n'a finalement été subi dans cet Etat. D'autres auteurs sont d'avis qu'en cas d'absence de dommage dans l'Etat de la résidence habituelle du lésé, il serait préférable de se référer au lieu principal du résultat, « c'est-à-dire celui où le lésé, compte tenu de l'ensemble des circonstances, a subi l'atteinte la plus grave ou la plus évidente à sa personnalité »⁶⁸.

B. L'intervention de l'ordre public lorsqu'un droit étranger est applicable

56. Dans l'hypothèse où le droit suisse n'est pas applicable à la protection de l'intégrité numérique du lésé, il sera nécessaire de déterminer si l'intégrité numérique est protégée dans le droit désigné par les règles de conflit de lois. En l'absence d'une norme consacrant expressément ce droit, il faudra rechercher s'il est possible d'admettre néanmoins l'existence d'un droit à l'intégrité numérique, par exemple par le biais d'une interprétation des droits de la personnalité.

⁶⁷ La question est cependant controversée en doctrine. Voir BONOMI, CR-LDIP/CL, art. 139 LDIP, N 5, p. 1160, et réf. citées.

⁶⁸ DUTOIT, Commentaire, art. 139 LDIP, N 9, p. 635.

57. Lorsque le droit à l'intégrité numérique n'est pas protégé dans la loi étrangère applicable, le juge suisse peut recourir à la réserve de l'ordre public si l'application du droit étranger conduit à un résultat incompatible avec l'ordre public suisse (art. 17 et 18 LDIP). L'intervention de ce mécanisme permet d'appliquer le droit suisse quand bien même la règle de droit international privé désigne une loi étrangère. Le droit à l'intégrité numérique serait dès lors protégé avec la portée qui lui serait reconnue en droit suisse.
58. Ce raisonnement suppose cependant que le droit à l'intégrité numérique soit considéré comme l'une des règles fondamentales qui sous-tendent l'organisation sociale suisse⁶⁹. Autrement dit, le droit à l'intégrité numérique devrait être considéré comme un droit fondamental protégeant les droits de la personnalité et faisant partie, à ce titre, du noyau dur de l'ordre juridique suisse pour pouvoir bénéficier de ce traitement particulier.
59. La réserve de l'ordre public peut être invoquée, en tout cas, si le droit désigné n'accorde aucune protection, dans un cas d'espèce, à l'intégrité numérique de la victime. Par exemple, si une personne fait l'objet d'une humiliation publique sur un réseau social accessible depuis la Suisse et que cela entraîne des conséquences préjudiciables sur sa vie privée, telles qu'un isolement social ou la perte d'un emploi, l'application d'un droit étranger ne permettant pas de protéger la victime est susceptible d'entraîner un résultat incompatible avec l'ordre public suisse. La question de l'application de la réserve de l'ordre public doit cependant être examinée au regard des circonstances du cas d'espèce et des liens de la cause avec l'ordre juridique suisse⁷⁰. En soi, le simple fait que la protection accordée par le droit étranger soit différente de celle qui résulterait de l'application du droit suisse n'est pas suffisant pour écarter l'application de la loi étrangère⁷¹.
60. Dans l'hypothèse où le droit à l'intégrité numérique serait consacré dans la Constitution fédérale, cela donnerait bien évidemment une plus grande force à ce droit devant les tribunaux civils suisses. Ceux-

⁶⁹ Voir p.ex. ATF 135 III 614 ; ATF 117 II 494.

⁷⁰ Voir GUILLAUME, N 79, pp. 186-188.

⁷¹ Voir BUCHER, CR-LDIP/CL, art. 17 LDIP, N 10, p. 241.

ci peuvent néanmoins protéger l'intégrité numérique des personnes même sans que ce droit soit consacré expressément dans une norme constitutionnelle⁷².

61. Quoi qu'il en soit, le droit à l'intégrité numérique fait, selon nous, déjà partie de l'ordre public international suisse. Ce droit fondamental peut en effet être rapproché, notamment, du droit au respect de la vie privée, du droit à la protection des données et du droit à l'autodétermination informationnelle qui sont des droits fondamentaux protégés au niveau international⁷³. A ce titre, le droit à l'intégrité numérique doit être protégé par les tribunaux civils suisses, car l'Etat a un intérêt à protéger la personne humaine dans les relations privées internationales, quelle que soit la loi désignée par la règle de droit international privé. Cela correspond à l'engagement de la Suisse qui s'est déclarée prête à garantir un niveau élevé de protection de la sphère privée et des droits fondamentaux dans l'espace numérique au moment de la signature de la Convention 108+ en 2019⁷⁴.

V. L'insécurité juridique liée au risque de compétence universelle

62. L'application des règles de droit international privé est difficile dans le cadre d'une atteinte à la personnalité au moyen d'un contenu mis en ligne. L'objectif poursuivi par ces règles, qui est de localiser la situation juridique dans l'Etat avec lequel elle présente les liens les plus étroits, paraît incompatible avec le caractère ubiquitaire d'Internet. Les atteintes à la personnalité commises en ligne, et notamment les atteintes à l'intégrité numérique, présentent la

⁷² Voir *supra* N 12-14.

⁷³ Voir l'art. 8 CEDH, l'art. 12 DUDH, l'art. 17 du Pacte ONU II, ainsi que la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (RS 0.235.1 ; Convention 108) et son Protocole d'amendement adopté en mai 2018 (Convention 108+). Voir aussi les contributions de JEAN-PHILIPPE WALTER, L'intégrité numérique : une nécessité du point de vue du droit à la protection des données ?, pp. 95 ss du présent ouvrage, et de PASCAL MAHON, Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? Le point de vue du droit constitutionnel, pp. 43 ss du présent ouvrage, spéc. N 4-13, pp. 45-53.

⁷⁴ CONSEIL FÉDÉRAL, Message Convention 108+. Voir aussi WALTER, N 6-9, pp. 98-100.

particularité d'avoir lieu potentiellement partout dans le monde et peuvent dès lors difficilement être ancrées dans un seul Etat.

63. Il en résulte une forte imprévisibilité quant aux tribunaux compétents pour juger d'une atteinte à l'intégrité numérique (A). L'Institut de droit international a tenté de remédier à cette insécurité juridique en adoptant une Résolution proposant des règles de droit international privé permettant de localiser les atteintes à la personnalité au moyen d'un contenu mis en ligne (B).

***A. Le principe de proximité confronté à l'universalité
d'une atteinte à l'intégrité numérique***

64. Nous avons vu que la LDIP et la Convention de Lugano se réfèrent aux critères de rattachement suivants pour déterminer la compétence des tribunaux suisses et le droit applicable à une atteinte à l'intégrité numérique : le domicile ou la résidence habituelle du lésé ou de l'auteur de l'atteinte, le lieu de l'événement causal (ou « lieu de l'acte illicite ») et le lieu de la matérialisation du dommage (ou « lieu du résultat de l'acte illicite »)⁷⁵. Ces deux derniers critères, qui sont spécifiques au domaine des actes illicites, correspondent à une localisation au « lieu de l'atteinte ».
65. La détermination du lieu de l'atteinte à l'intégrité numérique, autrement dit du lieu où l'acte à l'origine de l'atteinte ainsi que du lieu où le résultat de cette atteinte s'est fait ressentir, se heurte au caractère ubiquitaire d'Internet.
66. Comme le montre l'interprétation qui est faite du lieu de l'atteinte par la Cour de justice de l'Union européenne, l'utilisation d'Internet malmène le principe de proximité. Il s'agit d'un principe central du droit international privé dont l'application permet de déterminer le centre de gravité du rapport juridique en cause. La recherche du lieu de l'atteinte à la personnalité sur Internet a amené la jurisprudence européenne à développer des règles de compétence internationale extrêmement complexes⁷⁶. Ces règles sont difficiles à appliquer, notamment lorsqu'il s'agit de déterminer concrètement le lieu d'une

⁷⁵ Voir *supra* III et IV.

⁷⁶ Voir *supra* N 38-42.

atteinte à la personnalité au moyen d'un contenu mis en ligne ou de chiffrer le dommage survenu dans un Etat particulier.

67. Or, la fixation du for est essentielle dans le cadre d'affaires ayant une portée internationale, comme c'est en principe le cas d'une atteinte à la personnalité causée par un contenu mis en ligne. L'existence et la portée de l'atteinte seront en effet estimées au regard de la loi applicable, laquelle est déterminée par les règles de conflit de lois du for. Il en résulte que la loi applicable au litige peut différer en fonction du juge saisi⁷⁷.
68. C'est la raison pour laquelle il existe un risque important de *forum shopping* en matière d'actes illicites commis sur Internet. Compte tenu du caractère ubiquitaire d'Internet, le lésé a en effet inévitablement le choix entre plusieurs fors et peut, de cette manière, choisir l'environnement juridique qui lui est le plus favorable. La situation est encore plus problématique s'agissant d'une atteinte à la personnalité sur Internet. Cette sorte d'atteinte est universelle et peut donc potentiellement être invoquée devant les tribunaux civils de n'importe quel Etat à travers le monde. Il en va de même d'une atteinte à l'intégrité numérique qui est par essence universelle.
69. La compétence universelle, à savoir la possibilité de saisir la justice dans n'importe quel Etat même si la cause ne présente pas de liens particuliers avec cet Etat, est un risque connu dans les affaires liées à l'utilisation d'Internet⁷⁸. Un tribunal peut d'ailleurs très facilement considérer que la simple accessibilité à un contenu mis en ligne dans sa juridiction constitue un lien étroit avec cette juridiction⁷⁹. Mais ce type de raisonnement s'écarte clairement du principe de proximité en laissant au demandeur, dans une large mesure, la possibilité de choisir le for sans tenir compte de l'intensité des liens de la cause avec l'Etat dont il a choisi unilatéralement les tribunaux.
70. La situation juridique est d'autant plus complexe que chaque Etat adopte ses propres règles de droit international privé. Il n'y a dès lors pas nécessairement de coordination entre les Etats dans la détermination de la compétence de leurs tribunaux pour juger d'une

⁷⁷ Voir GUILLAUME, N 31, pp. 62-64.

⁷⁸ Voir p.ex. TREPPOZ, p. 279.

⁷⁹ SMITH, p. 132.

atteinte à l'intégrité numérique. Il en résulte une insécurité juridique qui est particulièrement regrettable en lien avec la protection d'un droit fondamental.

71. Seule l'adoption d'une convention internationale uniformisant les règles de droit international privé des différents Etats contractants serait susceptible de remédier à cette insécurité juridique. Une coordination au niveau de la compétence internationale est atteinte, par exemple, entre les tribunaux suisses et ceux de l'Union européenne dans le champ d'application de la Convention de Lugano. Mais les règles de compétence internationale en matière civile et commerciale n'ont pas encore pu être unifiées dans le cadre d'une convention multilatérale de portée universelle⁸⁰.

B. Les règles de conflit proposées par l'Institut de droit international

72. C'est pour remédier à cette insécurité juridique que l'Institut de droit international a adopté récemment une Résolution sur les atteintes aux droits de la personnalité par l'utilisation d'Internet⁸¹. Cette Résolution propose une loi uniforme de droit international privé contenant des règles de conflit de lois et des règles de conflit de juridictions applicables en cas d'atteinte transfrontière⁸² à la

⁸⁰ Les travaux de la Conférence de La Haye de droit international privé visant à adopter des règles unifiées de compétence internationale, en matière civile et commerciale, au sein d'une convention de droit international privé ont été récemment repris après un premier échec. A ce sujet, voir <https://www.hcch.net/fr/projects/legislative-projects/jurisdiction-project> (site consulté le 30.10.2020).

⁸¹ INSTITUT DE DROIT INTERNATIONAL, Les atteintes aux droits de la personnalité par l'utilisation d'Internet : compétence, droit applicable et reconnaissance des jugements étrangers, Résolution du 31 août 2019, Session de La Haye 2019, disponible sur : <https://www.idi-iil.org/app/uploads/2019/09/8-RES-FR.pdf> (site consulté le 30.10.2020). A noter que cette traduction française ne correspond pas exactement à la version de la Résolution figurant dans le rapport explicatif d'Erik Jayme et Symeon C. Symeonides à laquelle nous faisons référence.

⁸² La Résolution ne s'applique que dans une situation internationale. Lorsque l'événement causal et les principaux effets dommageables se sont produits dans l'Etat dans lequel résident à la fois l'auteur et le lésé, les règles proposées dans la Résolution ne sont pas applicables (voir art. 2 al. 2 lit. c).

personnalité causée par un contenu mis en ligne. L'objectif de cette Résolution est de contribuer à l'émergence d'un consensus international dans ce domaine⁸³.

1. Le principe holistique

73. Deux principaux constats sont à la base des travaux qui ont conduit l'Institut de droit international à adopter cette Résolution⁸⁴. Premièrement, les règles de droit international privé adoptées par les Etats en matière d'atteinte à la vie privée sur Internet sont diamétralement opposées. Certains Etats ont choisi de privilégier la protection de la vie privée et des autres droits de la personnalité, alors que d'autres favorisent la protection de la liberté d'expression. Il est particulièrement difficile de concilier ces deux approches dans le contexte transfrontière d'actes illicites commis sur Internet. Deuxièmement, l'ubiquité de l'environnement d'Internet a pour conséquence de multiplier les fors à travers le monde. La nature ubiquitaire du contenu et des données mis en ligne sur un site Internet rend la portée de leur diffusion universelle, ce qui entraîne une multitude de fors pour les actions visant à protéger les droits de la personnalité. Il en résulte un manque de prévisibilité, avec pour corolaire une importante insécurité juridique.
74. La Résolution de l'Institut de droit international tente de remédier au risque de compétence universelle et, plus généralement, à l'insécurité juridique existant actuellement en cas d'atteinte à la personnalité sur Internet en limitant le nombre de fors. Quatre fors différents sont proposés pour les actions en réparation ou en prévention d'une atteinte à la personnalité causée par un contenu mis en ligne :

⁸³ Pour ce qui est de la question de la reconnaissance et l'exequatur des décisions en la matière, il est fait renvoi à la Convention de La Haye du 2 juillet 2019 sur la reconnaissance et l'exécution des jugements étrangers en matière civile ou commerciale (cf. art. 9).

⁸⁴ JAYME/SYMEONIDES, Rapport explicatif, pp. 251-252.

- Un for dans l'Etat de la résidence⁸⁵ du défendeur (art. 5 al. 1 lit. a). Si l'action est intentée dans cet Etat, le droit du for est applicable (art. 7 ch. 1).
 - Un for dans l'Etat où le « comportement déterminant de la personne dont la responsabilité est invoquée est survenu »⁸⁶ (art. 5 al. 1 lit. b). Si l'action est intentée dans cet Etat, le droit du for est en principe applicable. Toutefois, si le défendeur a sa résidence dans un autre Etat, le droit applicable est celui de l'Etat avec lequel le défendeur entretient les liens les plus étroits (art. 7 ch. 2).
 - Un for dans l'Etat « sur le territoire duquel les effets préjudiciables les plus étendus se sont produits ou risqueraient de se produire »⁸⁷ (art. 5 al. 1 lit. c). Si l'action est intentée dans cet Etat, le droit du for est en principe applicable. Toutefois, le lésé peut demander que le droit de l'Etat où le comportement déterminant de l'auteur de l'atteinte s'est produit soit applicable (art. 7 ch. 3).
 - Un for dans l'Etat de la résidence du demandeur « si le contenu mis en ligne est accessible dans cet Etat ou si la personne a subi un dommage dans cet Etat » (art. 5 al. 1 lit. d). Si l'action est intentée dans cet Etat, le droit du for est en principe applicable. Toutefois, l'auteur peut demander que le droit de l'Etat sur le territoire duquel « les effets préjudiciables les plus étendus se sont produits » soit applicable (art. 7 ch. 4).
75. La Résolution réserve les accords d'élection de for (art. 6) et d'élection de droit (art. 8). A défaut d'élection de droit, le tribunal choisi appliquera le droit de l'Etat avec lequel le litige entretient les liens les plus étroits. Toutefois, si le tribunal choisi est dans l'un des Etats où la Résolution prévoit un for (cf. art. 5 al. 1), le droit

⁸⁵ La Résolution utilise le terme « résidence » (« *home state* ») pour désigner le domicile ou la résidence habituelle d'une personne (art. 1 ch. 11).

⁸⁶ La Résolution définit le terme « comportement déterminant » (« *critical conduct* ») comme étant « le téléchargement, l'hébergement et la diffusion du contenu mis en ligne, ou toute autre action ou omission, quel que soit, parmi ces comportements, celui qui constitue la cause principale du dommage » (art. 1 ch. 8).

⁸⁷ La version anglaise utilise l'expression « *the most extensive injurious effects* ».

applicable est déterminé de la même manière qu'en l'absence d'une élection de for (art. 7 ch. 5).

76. Le risque de procédures se déroulant simultanément dans plusieurs pays est contré par l'adoption du principe holistique (« *one action, one law for all injuries* »)⁸⁸. En vertu du principe holistique, le demandeur ne peut intenter qu'une seule action pour obtenir réparation de l'atteinte à ses droits de la personnalité « du fait d'un contenu mis en ligne ou de toute autre activité menée sur Internet » contre la personne dont la responsabilité est invoquée « en vue d'obtenir réparation pour les dommages survenant ou risquant de survenir dans un quelconque Etat » (art. 3 al. 1). Le demandeur peut choisir parmi un nombre limité de fors, ce qui permet théoriquement de circonscrire les tribunaux potentiellement compétents.
77. L'adoption du principe holistique écarte notamment le principe de la mosaïque, appliqué par la Cour de justice de l'Union européenne, lequel contraint le lésé à agir dans les différents Etats dans lesquels le contenu litigieux mis en ligne est accessible pour y faire valoir, chaque fois, une partie de ses prétentions⁸⁹. Le principe de la mosaïque entraîne un morcellement des prétentions qui est susceptible d'être préjudiciable au lésé dans la mesure où la nécessaire multiplication des actions en justice peut constituer un frein pour faire valoir l'intégralité du dommage devant les tribunaux. D'une manière générale, le principe de la mosaïque entraîne des coûts procéduraux importants qui peuvent soit s'avérer trop lourds à supporter pour la victime, soit lui offrir le moyen d'harcéler procéduralement l'auteur de l'acte. En outre, l'opération consistant à évaluer le dommage survenu dans chaque Etat peut s'avérer périlleuse. Il est, par exemple, extrêmement complexe de mesurer de façon exacte la réputation d'une personne sur le territoire d'un Etat, notamment s'agissant des personnes connues dans le monde entier⁹⁰. Le principe holistique vise à remédier notamment à ces inconvénients liés au principe de la mosaïque.

⁸⁸ Voir JAYME/SYMEONIDES, Rapport explicatif, pp. 263-264.

⁸⁹ Voir *supra* III.B.2.

⁹⁰ Voir KAUFMANN-KOHLER, pp. 113-114 ; DUTOIT, Actes illicites sur Internet, pp. 162-163.

78. Le respect du principe holistique est assuré par le fait que les tribunaux des autres Etats dans lesquels la Résolution prévoit un for (cf. art. 5 al. 1) doivent s'abstenir de statuer sur une action découlant du même comportement entre les mêmes parties (art. 3 al. 2). Par ailleurs, lorsque le demandeur agit à l'un des fors prévus dans la Résolution, le tribunal saisi ne peut pas refuser de statuer en invoquant, notamment, la doctrine du *forum non conveniens* (art. 5 al. 2).

2. La *lex fori*

79. La Résolution prévoit l'application de principe de la loi du for (art. 7)⁹¹. L'objectif principal est d'éviter que le tribunal doive procéder à une analyse de droit international privé pour déterminer le droit applicable. Le rattachement à la *lex fori* s'impose naturellement dans une situation où l'application de règles localisatrices s'avère problématique. Tel est le cas lorsqu'il n'y a pas vraiment d'Etat avec lequel la cause présente un lien étroit et qu'il est dès lors impossible de déterminer concrètement le centre de gravité du rapport juridique en cause. Ce rattachement permet ainsi d'améliorer la prévisibilité de la loi applicable et donc la sécurité du droit⁹².
80. Le rattachement à la *lex fori* présente également l'avantage de faciliter la qualification de l'atteinte. Pour tenir compte des différences – essentiellement terminologiques⁹³ – existant entre les droits nationaux, la Résolution regroupe sous le terme « droits de la personnalité » la réputation, la dignité, l'honneur, le nom, l'image et la vie privée « ainsi que tout autre droit similaire qui, quel que soit son appellation, est protégé par le droit applicable pertinent » (art. 1 ch. 2). Partant, la protection du droit à l'intégrité numérique entre dans le champ d'application de la Résolution.
81. Il reste à examiner si ces règles permettent de remédier efficacement à l'insécurité juridique liée au risque de compétence universelle en cas d'atteinte portée à l'intégrité numérique d'une personne.

⁹¹ Voir *supra* N 74.

⁹² JAYME/SYMEONIDES, Rapport explicatif, p. 255.

⁹³ JAYME/SYMEONIDES, Rapport explicatif, p. 259.

VI. L'adaptation des règles localisatrices à l'environnement ubiquitaire d'Internet

82. Au vu du caractère à la fois transfrontière et dématérialisé d'Internet, l'ancrage d'une atteinte à l'intégrité numérique dans le territoire d'un Etat – pour déterminer le for et le droit applicable – soulève une difficulté qui s'exprime dans deux dimensions. Dans la dimension horizontale, la localisation de l'atteinte à l'intégrité numérique dans l'Etat avec lequel elle présente les liens les plus étroits n'est qu'une construction juridique qui ne peut pas correspondre à la réalité en raison du caractère planétaire d'Internet (A). Dans la dimension verticale, la localisation de l'atteinte à l'intégrité numérique dans un Etat se heurte systématiquement au caractère virtuel d'Internet qui a pour effet que l'atteinte n'a pas lieu uniquement dans le monde physique, mais s'étend également à l'espace numérique (B). Il est même possible d'imaginer des hypothèses où l'atteinte à l'intégrité numérique se diffuse uniquement de façon immatérielle sans qu'il soit possible de la rattacher au monde physique (C).

A. Le paradoxe du rattachement de l'atteinte à l'intégrité numérique au territoire d'un Etat

83. L'application des règles de droit international privé requiert de localiser une atteinte à l'intégrité numérique dans le territoire d'un Etat particulier au moyen de critères de rattachement. L'identification de cet Etat doit permettre d'ancrer la cause dans l'ordre juridique avec lequel elle présente les liens les plus étroits. L'objectif visé est de garantir la prévisibilité, au niveau du for et de la loi applicable, afin d'apporter une certaine sécurité juridique aux relations privées internationales. La définition des critères de rattachement a une importance toute particulière lorsque les parties ne peuvent pas aisément convenir à l'avance du for et du droit applicable. Ces situations se rencontrent notamment en matière d'actes illicites, et plus particulièrement lors d'atteintes aux droits de la personnalité. Lorsque de telles atteintes ont lieu par l'intermédiaire d'Internet, elles ont potentiellement un impact universel. La localisation en un seul lieu semble dès lors antinomique avec la portée de l'atteinte.

1. Une action, un droit ?

84. La complexité à déterminer les tribunaux compétents pour juger d'une atteinte à l'intégrité numérique illustre bien les limites du principe de proximité lorsque l'atteinte à un droit protégé a lieu par l'intermédiaire d'Internet. En outre, à la difficulté de localiser le for s'ajoute le risque que des procédures ayant le même objet se déroulent en parallèle dans plusieurs Etats.
85. Lorsque la compétence des tribunaux suisses est établie dans un cas concret où une personne invoque une atteinte à son intégrité numérique, cela n'empêche pas que les tribunaux d'un autre Etat puissent être également saisis de la même cause. Le lésé peut en effet procéder devant les tribunaux de plusieurs Etats, par exemple pour faire pression sur l'auteur de l'atteinte. De même, l'auteur présumé peut saisir préventivement les tribunaux d'un autre Etat que celui devant lequel la prétendue victime introduira vraisemblablement son action pour faire constater son absence de responsabilité.
86. Il en résulte un risque de décisions contradictoires, lesquelles seraient préjudiciables à la résolution judiciaire du litige. Ce risque existe toujours dans le cadre d'affaires internationales, mais il est d'autant plus important que la portée universelle d'une atteinte à l'intégrité numérique permet théoriquement de saisir les tribunaux de n'importe quel Etat dans le monde. Comme on l'a vu⁹⁴, le caractère ubiquitaire d'Internet crée un risque de compétence universelle qui compromet la sécurité juridique.
87. C'est précisément pour remédier à cette incertitude quant au for et à la loi applicable que l'Institut de droit international a adopté la Résolution sur les atteintes aux droits de la personnalité par l'utilisation d'Internet⁹⁵. Cette Résolution présente l'intérêt d'introduire le principe holistique en vertu duquel une même affaire ne peut être l'objet que d'une seule action en justice. L'objectif visé est d'offrir une construction juridique permettant aux tribunaux d'un seul Etat de juger de l'affaire dans sa globalité. Si les règles

⁹⁴ Voir *supra* V.A.

⁹⁵ Voir *supra* V.B.

proposées peuvent paraître simples au premier abord, leur application concrète n'en demeure pas moins difficile.

88. La coordination entre les procédures se déroulant en parallèle dans plusieurs Etats est assurée par des règles différentes propres au droit de chaque Etat. Certains appliquent le système de la litispendance internationale⁹⁶, laquelle donne la priorité au premier tribunal saisi, alors que d'autres se réfèrent à la doctrine du *forum non conveniens*, en vertu de laquelle un tribunal peut refuser de statuer s'il estime qu'il serait plus approprié de laisser le tribunal d'un autre Etat juger de l'affaire. Le fait que tous les Etats n'appliquent pas le même système pour coordonner les procédures parallèles est une entrave importante à l'application pratique du principe holistique.
89. Le système proposé dans la Résolution de l'Institut de droit international sur les atteintes aux droits de la personnalité par l'utilisation d'Internet ne peut réellement améliorer la prévisibilité quant au for que si tous les Etats l'adoptent. Il faudrait donc que tous les Etats du monde accordent à leurs tribunaux la compétence de juger de l'affaire dans sa globalité, d'une part, et empêchent leurs tribunaux de statuer si le lésé a déjà introduit une action dans un autre Etat dont les tribunaux sont également compétents, d'autre part. Cette vision est certes louable, mais tient de l'utopie.
90. S'agissant de la détermination de la loi applicable aux prétentions du demandeur, la sécurité juridique ne peut être améliorée dans ce domaine qu'en prescrivant l'application de la loi du for. Le droit applicable dépend alors directement du tribunal saisi, ce qui permet de recentrer le raisonnement de droit international privé sur la détermination du for. Cette conclusion s'est finalement imposée aux rédacteurs de la Résolution de l'Institut de droit international qui ont retenu une application de principe de la *lex fori*. Pareille solution est audacieuse, car les Etats n'osent pas la préconiser par crainte de paraître peu respectueux des autres systèmes juridiques.
91. Si le principe holistique pourrait en théorie apporter une solution idéale au dilemme du rattachement des atteintes aux droits de la personnalité par l'utilisation d'Internet, il est illusoire de croire que

⁹⁶ Le système de la litispendance est suivi par les droits de tradition civiliste, comme le droit suisse (art. 9 LDIP ; art. 27 CL), alors que les droits de *common law* appliquent la doctrine du *forum non conveniens*.

tous les Etats du monde vont l'adopter. « Une action, un droit » restera vraisemblablement une formule mythique dans ce domaine.

2. De la proximité à l'ubiquité

92. Dans ces conditions, le principal mérite de la Résolution de l'Institut de droit international est de circonscrire l'espace judiciaire en rattachant une atteinte à la personnalité commise sur Internet à un nombre limité d'Etats. Les rédacteurs de cette Résolution essaient de définir une solution adéquate pour concilier la nature ubiquitaire d'Internet avec le principe de proximité afin d'éviter une prolifération des fors.
93. Les deux fors fondés sur la personne du demandeur et du défendeur ne posent pas de problème particulier à cet égard. En revanche, les deux autres fors fondés sur l'atteinte se heurtent à la transnationalité des comportements sur Internet. Nous concentrerons dès lors notre analyse sur ces rattachements au lieu de l'acte et au lieu du résultat de l'atteinte à la personnalité.
94. Le premier for, qui se trouve dans l'Etat où l'acte à la base de l'atteinte à la personnalité est survenu, pose problème en pratique lorsque le comportement déterminant s'est produit dans plusieurs Etats. Le lieu de l'acte est difficile à déterminer notamment dans le cas où une suite d'événements divers sont à l'origine du comportement délictueux. Par exemple, la diffusion sur Internet d'un photomontage dégradant implique de télécharger la photo de la personne avant de réaliser le montage, et enfin de le publier sur les réseaux sociaux et/ou de l'envoyer à des tiers par sms ou email. Ces différents actes peuvent avoir lieu dans plusieurs pays, rendant illusoire le rattachement de l'acte ayant porté atteinte au droit à l'image de la victime à un seul et même Etat.
95. Il peut également arriver qu'il soit simplement impossible de déterminer l'Etat dans lequel l'acte à la base de l'atteinte à la personnalité est survenu. Par exemple, un tweet diffamatoire peut être posté sur un smartphone depuis n'importe quel endroit où il est possible d'accéder à Internet. Lorsque l'auteur est en déplacement à l'étranger, le lieu où le tweet a été publié (p.ex. au cours d'une escale dans un aéroport) ne permet pas d'ancrer le

comportement dans un Etat de façon satisfaisante. En outre, en cas de cyberharcèlement, ce n'est pas le fait de poster un tweet qui est problématique, mais l'accumulation de centaines voire de milliers de tweets. Ces multiples ramifications entravent l'application des critères de rattachement aux fins de la détermination du for.

96. Ces exemples montrent qu'il n'y a pas nécessairement un seul lieu de l'acte à la base de l'atteinte, d'une part, et que ce ou ces lieux peuvent être le fruit du hasard, d'autre part. Le for dans l'Etat où l'acte à la base de l'atteinte à la personnalité est survenu est par conséquent non seulement potentiellement multiple, mais également fortuit. Il en résulte une totale imprévisibilité quant aux tribunaux compétents.
97. La Résolution tente de circonscrire le deuxième for, situé dans l'Etat où le résultat de l'atteinte à la personnalité s'est fait ressentir, en désignant l'Etat dans lequel « les effets préjudiciables les plus étendus » se sont produits. Cette formulation dissimule une référence évidente à l'Etat avec lequel la cause présente les liens les plus étroits. Mais le principe de proximité s'accommode mal du caractère ubiquitaire d'Internet. Le simple énoncé de ce for en fait ressortir les limites : cet Etat sera-t-il celui où le lésé est le plus connu, celui où il a le plus de *followers*, celui où il y a le plus de personnes connectées à Internet, ou celui où le lésé a ressenti le plus grand dommage économique ? Faut-il mesurer les effets préjudiciables d'une atteinte à l'intégrité numérique par rapport à l'impact ressenti par la victime dans la vie réelle ou sur les réseaux sociaux ? La réponse à ces questions dépendra probablement des circonstances.
98. Il ressort de ce qui précède que le droit international privé se heurtera toujours à la portée ubiquitaire d'Internet. Il y a une antinomie entre le principe fondateur du droit international privé moderne, selon lequel un comportement doit être rattaché à l'Etat dans lequel le rapport juridique a son centre de gravité, et la règle de base d'Internet en vertu de laquelle tout comportement intervenant en ligne se diffuse instantanément de façon universelle. Aucune construction juridique n'est susceptible de résoudre ce paradoxe de façon satisfaisante. L'ancrage d'une atteinte à un droit de la personnalité commise sur Internet dans le territoire d'un seul Etat

est une démarche intellectuelle qui ne peut pas aboutir à une solution appropriée en pratique.

B. La localisation de l'atteinte à l'intégrité numérique dans le monde physique et l'espace numérique

99. Le constat que les règles de droit international privé ne peuvent que rattacher de façon artificielle un comportement sur Internet, et notamment une atteinte à l'intégrité numérique, à un Etat particulier questionne l'essence même des règles de conflit. Bien plus, la question se pose de savoir s'il est réellement possible de localiser un comportement en ligne dans le monde physique.
100. En soi, il ne s'agit pas d'un sujet nouveau. Des voix s'élèvent dans la doctrine depuis plusieurs années pour contester l'application des règles de droit nationales aux relations privées ayant lieu dans l'environnement numérique d'Internet. Celui-ci devrait être considéré comme un territoire, ou plutôt un espace, indépendant des Etats et gouverné par ses propres règles. Il y aurait ainsi une loi du cyberspace régissant cet environnement qui serait issue d'un processus d'autorégulation d'Internet⁹⁷.
101. Le droit à l'intégrité numérique apporte un éclairage nouveau au débat sur l'opportunité de reconnaître l'existence d'un espace numérique d'Internet indépendant des Etats et gouverné par ses propres règles. La question est particulièrement intéressante du point de vue du droit international privé dont les règles requièrent de procéder à un raisonnement permettant de localiser l'atteinte à l'intégrité numérique dans le monde physique. Cette démarche pose des difficultés en particulier lorsqu'il s'agit de rechercher le lieu où l'acte ayant causé l'atteinte à l'intégrité numérique a été commis (i.e. le lieu de l'acte), d'une part, et le lieu où l'atteinte à l'intégrité numérique est survenue ou s'est manifestée (i.e. le lieu du résultat), d'autre part.

⁹⁷ Voir JOHN PERRY BARLOW, A Declaration of the Independence of Cyberspace, Davos 1996, disponible sur <https://www.eff.org/fr/cyberspace-independence> (site consulté le 30.10.2020). Voir aussi p.ex. JOHNSON/POST, spéc. pp. 1378-1387 ; LESSIG, spéc. pp. 1-8, et réf. citées.

102. Pour localiser une atteinte à l'intégrité numérique aux fins de l'application des règles de droit international privé, deux approches conceptuelles différentes peuvent être suivies. Une première conception consiste à considérer Internet comme un simple outil numérique utilisé pour causer une atteinte à l'intégrité numérique. Cette analyse est réfutée dans une deuxième conception reconnaissant l'existence d'un environnement numérique d'Internet dans lequel il est possible de porter atteinte à l'intégrité numérique. Ce débat sur la portée de l'intégrité numérique s'inscrit dans celui, plus large, des partisans et des opposants au cyberspace. L'enjeu consiste en effet à déterminer si une atteinte à l'intégrité numérique peut être localisée dans l'environnement numérique (le cyberspace), par exemple dans un réseau social (p.ex. Twitter), ou si cette sorte d'atteinte ne peut être localisée que dans le monde physique.

1. Internet en tant qu'outil de l'atteinte

103. La première conception consiste à considérer que l'acte dommageable peut être rattaché à une personne ayant agi en un lieu donné, de même que le lésé a subi l'atteinte à son intégrité numérique « dans sa chair » en un lieu donné. L'atteinte à l'intégrité numérique serait ainsi à la fois causée et ressentie dans le monde physique. Internet est considéré comme un simple outil permettant de commettre l'acte illicite.
104. Par exemple, si des photos compromettantes d'une personne sont diffusées sans son accord sur un réseau social (p.ex. Facebook), Internet n'est qu'un outil permettant de diffuser plus facilement et à grande échelle les photos. En soi, l'effet souhaité (p.ex. l'atteinte à la réputation professionnelle) pourrait tout aussi bien être atteint en placardant les photos sur les murs de la rue dans laquelle la victime travaille. Dans cette manière de voir les choses, l'acte a été commis par une personne assise derrière son ordinateur et le résultat s'est produit sur le lésé qui est atteint dans sa réputation dans sa vie de tous les jours (p.ex. dans son environnement professionnel).

L'accent est mis sur les points de contact entre virtualité et réalité : c'est bien une personne vivante qui est diffamée ou calomniée⁹⁸.

105. Au niveau de l'analyse du droit à l'intégrité numérique, cela revient à considérer qu'il ne s'agirait pas d'un droit spécifique avec une portée propre. Le droit à l'intégrité numérique serait uniquement l'expression du fait que le droit à l'intégrité physique ou psychique protège également la personne des atteintes survenant par le biais d'outils numériques tels qu'Internet⁹⁹. Cette première approche se concentre sur les personnes et leurs actes dans le monde physique en mettant en exergue la particularité des outils numériques et l'ampleur des atteintes qu'ils sont susceptibles de causer. Elle nie toute possibilité de créer des droits et obligations dans un quelconque espace numérique. L'intégrité numérique ne devrait pas mener à reconnaître l'existence d'un espace numérique distinct, car ce nouveau concept ne serait qu'une « extension fonctionnelle de l'intégrité physique et psychique qui porte sur la capacité d'une personne d'utiliser des technologies numériques ou sur la capacité à prévenir d'en être l'objet »¹⁰⁰.

2. Internet en tant qu'environnement de l'atteinte

106. La seconde approche conceptuelle consiste à prendre en compte la dimension spatiale de l'environnement numérique et à reconnaître qu'une personne puisse avoir une existence numérique en parallèle à son existence physique. L'existence numérique de la personne est alors protégée par l'intégrité numérique. Cette analyse amène à s'interroger sur la pertinence de la démarche consistant à localiser une atteinte à l'intégrité numérique dans le monde physique. Dans la mesure où l'auteur a agi sur Internet et que le lésé a subi un dommage également sur Internet, ne faut-il pas considérer qu'une localisation dans l'espace numérique serait plus appropriée ?
107. Dans cette conception, le droit à l'intégrité numérique aurait une portée propre visant à protéger la personne contre les atteintes à son existence numérique. Cela implique d'admettre que toute

⁹⁸ DESSEMONTET, p. 49.

⁹⁹ MAHON, Intégrité numérique, N 14-15, pp. 53-55.

¹⁰⁰ ROCHEL, N 29, p. 25.

personne ayant une activité numérique ou des informations à son sujet sur Internet a une existence numérique propre qui doit être protégée. Il y aurait ainsi un « réel » espace numérique, dans lequel il serait possible de créer des droits et obligations, distinct du monde physique. Le lieu de l'atteinte à l'intégrité numérique (dans l'espace numérique) ne correspondrait donc pas au lieu de l'atteinte à l'intégrité psychique ou physique (dans le monde physique).

108. Par exemple, lorsque le compte Facebook d'une influenceuse est fermé par la plateforme, on pourrait considérer qu'elle subit non seulement une atteinte à son intégrité physique ou psychique dans sa chair et son esprit, mais aussi une atteinte à son intégrité numérique qui se manifeste sur son existence numérique. L'atteinte numérique est même plus importante que l'atteinte physique ou psychique lorsque l'influenceuse a le centre de ses intérêts personnels et économiques en ligne. La perte des *followers* entraînée par la fermeture du compte peut en effet engendrer des conséquences sociales et économiques irrémédiables. La disparition de cet environnement socio-économique pourrait même être considérée comme une sorte de mort numérique. Le lieu de la matérialisation du dommage serait donc essentiellement dans l'espace numérique, et non pas dans le monde physique.
109. Quant au lieu de l'événement causal, le lieu dans le monde physique où l'auteur a agi est-il vraiment pertinent en cas d'atteinte à l'intégrité numérique ? Par exemple, en cas de cyberharcèlement sur Twitter, l'agression a lieu essentiellement en ligne. L'auteur, ou plus souvent les auteurs, ont agi sur le réseau social, en y postant des propos diffamatoires, et non pas dans le monde physique. La publication des messages diffamatoires intervient uniquement sur Internet. Le lieu d'où chacun des auteurs a agi n'est pas pertinent. Comme dans l'exemple précédent, où la victime consacrerait toute son énergie pour récupérer son existence sur Facebook, la victime aura à cœur avant tout d'obtenir la suppression du contenu dégradant figurant sur Twitter et de rétablir sa réputation sur le réseau social.
110. Ces deux exemples montrent qu'il est pertinent de prendre en considération le fait que l'atteinte à l'intégrité numérique a lieu dans l'espace numérique et non pas dans le monde physique. Il est en effet possible de porter atteinte à la personne d'un individu ou à ses

biens dans un espace numérique distinct du monde physique. Cela suppose d'admettre une existence numérique distincte pouvant être atteinte indépendamment de la dimension physique et psychique de la personne.

111. Toutefois, les auteurs qui adoptent cette seconde approche consistant à reconnaître un droit à l'intégrité numérique pour protéger les individus contre les atteintes à leurs droits de la personnalité ayant lieu dans l'espace numérique ne vont pas si loin. Ils estiment en effet que même si l'atteinte à l'intégrité numérique se produit dans l'espace numérique, dans la mesure où elle touche à l'existence de la personne sur Internet, le dommage n'est ressenti que physiquement et/ou psychiquement par la personne elle-même. Par exemple, si une personne fait l'objet d'un appel au boycott¹⁰¹ en ligne, même si l'atteinte a lieu sur les réseaux sociaux dont elle se trouvera de fait interdite d'accès, elle en subira les conséquences dans le monde physique où elle perdra son emploi et sa réputation professionnelle.
112. Dans cette approche conceptuelle intermédiaire, le droit à l'intégrité numérique est considéré comme un prolongement du droit à l'intégrité physique ou psychique. Plusieurs auteurs dont les contributions sont réunies dans le présent ouvrage suivent cette conception¹⁰² à laquelle nous nous rallions. Comme nous le verrons si-dessous¹⁰³, nous sommes cependant d'avis que même si l'atteinte a bien lieu dans l'espace numérique, il n'en reste pas moins que la matérialisation du dommage se produit aussi bien dans l'espace numérique (p.ex. l'expulsion des réseaux sociaux) que dans le monde physique (p.ex. la perte de l'emploi).
113. Un auteur franchit un pas supplémentaire en conceptualisant une « vie numérique » digne d'être protégée par le droit à l'intégrité

¹⁰¹ Le terme « appel au boycott » vise ici une humiliation publique organisée à grande échelle sur les réseaux sociaux dont l'objectif est de faire « disparaître » une personne de l'espace numérique et du monde physique en portant atteinte à sa réputation. Cette culture de l'annulation (*cancel culture*) s'est manifestée, par exemple, dans le cadre du mouvement #MeToo.

¹⁰² PAPAUX VAN DELDEN, N 33-34, pp. 76-77 ; WALTER, N 2, p. 96.

¹⁰³ Voir *infra* 3.

numérique¹⁰⁴. Il serait dès lors concevable d'avoir une vie dans le numérique dissociée de la vie dans le monde physique. Le droit à l'intégrité numérique aurait ainsi une portée propre, distincte de celle du droit à l'intégrité physique ou psychique. Une personne pourrait par conséquent être atteinte dans son intégrité numérique sans que son intégrité physique ou psychique soit également touchée avec la même intensité.

3. Le dédoublement du lieu de l'atteinte à l'intégrité numérique

114. Du point de vue du droit international privé, si on suit l'approche consistant à qualifier Internet de simple outil permettant de commettre l'atteinte à l'intégrité numérique, cela revient à appliquer les critères de rattachement tels qu'interprétés par la jurisprudence en cas d'atteinte commise sur Internet pour localiser l'atteinte à l'intégrité numérique dans le monde physique¹⁰⁵. Mais comme nous l'avons vu, cette démarche n'est pas satisfaisante¹⁰⁶.
115. A notre avis, Internet est bien plus qu'un simple moyen de transmettre des informations. Cette technologie a donné lieu à un environnement propre qui est devenu fondamental pour tout individu dans son épanouissement personnel, social et culturel. Il s'agit d'une sorte de territoire numérique séparé du monde physique par une frontière électronique¹⁰⁷. Les individus y ont une présence passive constante de par les données qui s'y trouvent à leur sujet, tout en ayant la possibilité de s'y rendre à tout moment.
116. Le fait de porter atteinte à la personnalité d'un individu par l'intermédiaire d'Internet est un acte qui est placé volontairement dans l'espace numérique. C'est bien l'intégrité numérique de la

¹⁰⁴ ROUSSEL, N 12, p. 6 : « [L]e droit à la vie comprend notre existence numérique. La vie numérique a étendu les contours de notre personnalité juridique. ».

¹⁰⁵ Dans ce sens : DUTOIT, Actes illicites sur Internet, p. 144 : « Internet ne crée nullement un nouvel espace (*cyberspace*), mais constitue plus modestement un moyen de communication utilisant un espace préexistant [...]. Quel que soit le caractère virtuel d'Internet, il arrive forcément un moment où la réalité refait surface. Si les réseaux sont virtuels, les acteurs sont bien réels. ».

¹⁰⁶ Voir *supra* VI.A.

¹⁰⁷ Voir JOHNSON/POST, p. 1379.

victime qui est visée, pas uniquement son intégrité physique et/ou psychique. Ceci n'exclut pas que la personne soit également atteinte psychiquement en son for intérieur et/ou que l'acte entraîne également des répercussions physiques sur la victime.

117. Le parallèle entre l'espace numérique et le monde physique apparaît clairement dans l'exemple d'une interdiction d'utiliser les réseaux sociaux. L'interdiction d'entrer et de se déplacer librement dans l'espace numérique des réseaux sociaux équivaut à une interdiction d'entrée et de mouvement sur le territoire d'un Etat. La sentence correspond, dans les deux situations, à un bannissement.
118. Corrélativement, il nous paraît souhaitable de reconnaître l'existence d'un droit à l'intégrité numérique avec une portée propre pour protéger la personnalité dans l'espace numérique. Ce droit, dont la protection est assurée en matière civile à l'art. 28 CC, permet aux individus de sauvegarder leur existence numérique contre les atteintes sur Internet. Cette protection doit pouvoir être invoquée, en principe, aussi bien par une personne physique qu'une personne morale.
119. Cette approche conceptuelle reconnaissant une existence numérique dissociée de l'existence physique a une influence sur le raisonnement de droit international privé. La localisation de l'atteinte portée à l'existence numérique d'une personne directement dans l'espace numérique paraît en effet plus appropriée qu'un rattachement au monde physique. Cela amène à devoir interpréter les règles de droit international privé en prenant en considération le fait que l'atteinte à l'intégrité numérique ne doit pas nécessairement être ancrée dans le monde physique mais peut être localisée directement dans l'espace numérique¹⁰⁸. Les critères de rattachement classiques doivent ainsi être redéfinis pour tenir compte du fait qu'ils ne sont pas adaptés aux atteintes aux droits de la personnalité causées par l'utilisation d'Internet. Cette démarche

¹⁰⁸ JOHNSON/POST, p. 1370, avaient déjà constaté en 1996 que « *Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and [...] the ability of physical location to give notice of which sets of rules apply* ».

est nécessaire pour prendre en compte le fait qu'il y a un lieu de l'atteinte dans l'espace numérique.

120. L'atteinte peut même être localisée précisément dans l'espace numérique en distinguant différents « lieux » ou « communautés » constituées, notamment, des réseaux sociaux¹⁰⁹. Une atteinte à l'intégrité numérique peut être localisée, par exemple, au sein même du réseau social où la victime subit une campagne de publicité négative (p.ex. Twitter). Une atteinte à l'intégrité numérique peut également être localisée dans un moteur de recherche indexant systématiquement les liens Internet concernant une personne. Google, par exemple, définit en quelque sorte la réputation numérique (*e-reputation*) d'une personne au moyen de ses algorithmes de référencement hypermnésiques¹¹⁰ et peut, à ce titre, causer une atteinte à l'intégrité numérique.
121. A notre avis, cette analyse doit être privilégiée, car elle est la seule à même de concilier le principe de proximité avec la nature ubiquitaire d'Internet. Il s'agit de reconnaître que le centre de gravité d'une atteinte à l'intégrité numérique se trouve dans l'espace numérique et d'en déduire la conséquence logique qu'il existe un lieu de l'atteinte sur Internet. Cette démarche évite de devoir interpréter les critères de rattachement applicables pour désigner les fors fondés sur l'atteinte (i.e. les fors au lieu de l'acte et au lieu du résultat) de manière incompatible avec l'objectif de prévisibilité des règles de conflit. Toute interprétation de ces critères en vue d'une localisation de l'atteinte à l'intégrité numérique uniquement dans le monde physique conduit à une fiction de rattachement de la cause dans l'Etat avec lequel elle présente les liens les plus étroits. Notre approche conceptuelle du droit à l'intégrité numérique en droit international privé révèle ainsi que les présomptions à l'origine des

¹⁰⁹ Dans ce sens : LESSIG, p. 84 : « *Cyberspace is not one place. It is many places. And the character of these many places differ in ways that are fundamental. These differences come in part from differences in the people who populate these places [...].* ».

¹¹⁰ Le droit à l'oubli reste délicat à exercer à l'égard des moteurs de recherche. Sur le droit au déréférencement, voir CJUE, 13.05.2014, *Google Spain c. Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317. Plus récemment (au sujet de la portée géographique du droit au déréférencement) : CJUE, 24.09.2019, *Google c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, ECLI:EU:C:2019:772 ; CJUE, 24.09.2019, *G.C. et al. c. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, ECLI:EU:C:2019:773.

critères de rattachement définis dans les règles de conflit ne sont pas adaptées aux atteintes au droit de la personnalité commises sur Internet. Il est nécessaire de reconsidérer la portée de ces règles en admettant l'éventualité que le lieu de l'atteinte ne se trouve pas nécessairement dans le territoire d'un Etat.

122. La reconnaissance d'un droit à l'intégrité numérique distinct de celui protégeant l'intégrité physique ou psychique des individus ne doit pas occulter le fait qu'un même acte peut avoir lieu et/ou avoir des effets aussi bien dans le monde physique que dans l'espace numérique. Les deux espaces sont en effet interconnectés. L'atteinte à l'intégrité numérique a également des répercussions physiques et psychologiques sur la victime. Il n'y a fondamentalement qu'une seule et même personne touchée à la fois dans son existence numérique et dans son existence physique.
123. Un seul et même acte peut donc être à l'origine d'une atteinte à l'intégrité numérique (dans l'espace numérique) et d'une atteinte à l'intégrité physique et psychique (dans le monde physique) même si la portée de ces deux atteintes n'est pas nécessairement identique. Il faut en conclure qu'il y a une sorte de dédoublement du lieu de l'atteinte qui se matérialise aussi bien dans le monde physique que dans l'espace numérique.

C. La localisation de l'atteinte à l'intégrité numérique dans le seul espace numérique

124. Après avoir admis que le droit à l'intégrité numérique a une portée propre protégeant la personnalité dans l'espace numérique, d'une part, et que le lieu de l'atteinte à ce droit peut être situé aussi bien dans le monde physique que dans l'espace numérique, d'autre part, il convient d'examiner s'il existe des situations où le lieu de l'atteinte peut se trouver uniquement dans l'espace numérique. Autrement dit, est-il possible de concevoir une atteinte à l'intégrité numérique qui ne se matérialise pas dans le monde physique ?
125. Pour qu'une atteinte à la personnalité ne soit pas ressentie dans le monde physique, la personne qui la subit ne doit avoir aucun rattachement avec celui-ci. Or, le droit ne connaît actuellement que deux types de personnes : les personnes physiques et les personnes

morales. Les personnes physiques se trouvent physiquement dans le monde physique et ressentent *de facto* les atteintes à leur personnalité au moins en partie psychiquement et/ou physiquement¹¹¹. Les personnes morales, quant à elles, sont une construction juridique par laquelle on accorde la fiction de la personnalité à un groupe social, lui-même composé de personnes physiques et/ou morales. Pour l'heure, la personnalité morale ne peut être accordée que par la loi d'un Etat, rattachant ainsi inévitablement les personnes morales au monde physique.

126. Pour rencontrer un cas de figure où l'atteinte à l'intégrité numérique se matérialiserait exclusivement dans l'espace numérique, il faudrait qu'une forme de personnalité n'existe que dans le monde numérique sans avoir un quelconque rattachement avec le monde physique. Nous aurions alors affaire à une personnalité numérique qui, *a priori*, devrait résulter d'une fiction juridique au même titre que la personnalité morale. L'évolution rapide de la technologie amène à s'interroger sur l'attribution de la personnalité juridique à des entités existant uniquement dans l'espace numérique¹¹². Si une personne numérique peut être un sujet de droit au même titre que les personnes physiques et morales, ou en tout cas être un titulaire de droits¹¹³, alors il est également possible de protéger son intégrité numérique.

1. L'avatar comme personne numérique

127. Parmi les nombreuses possibilités qu'offre l'espace numérique, la participation aux réseaux sociaux est sans doute l'une des activités à laquelle se livrent le plus les internautes. Lorsqu'une personne se crée un profil dans le but de partager du contenu (écrit, photo ou vidéo), elle se constitue une identité à part entière dans l'environnement numérique. Cette identité, que l'on peut qualifier

¹¹¹ Voir *supra* N 122-123.

¹¹² ALLGROVE, p. 71, relève à ce sujet que : « *the attribution of legal personality to bots is conceptually no different to its attribution to corporations, idols, ships, trade unions or, indeed, humans ; it is simply a decision to identify another nexus of legal rights and obligations upon which legal logic can act.* »

¹¹³ On pourrait envisager d'admettre qu'une personne numérique soit titulaire du droit à l'intégrité numérique sans avoir la personnalité.

d'identité numérique, présente la caractéristique de pouvoir être totalement liée¹¹⁴, partiellement liée¹¹⁵, voire même pas du tout liée¹¹⁶ à la réelle identité de la personne. L'environnement numérique permet ainsi à une personne de se constituer plusieurs identités numériques différentes dans ce spectre. Il est même possible pour un tiers de constituer une identité numérique d'une personne, avec ou sans son consentement.

128. Cette diversité d'identités numériques amène à se demander si une identité numérique pourrait être distincte de la personne physique ou morale qu'elle représente dans l'espace numérique. Si tel était le cas, il serait concevable qu'une identité numérique puisse subir une atteinte qui ne serait pas ressentie, à titre personnel, par la personne titulaire de cette identité. Cela reviendrait à considérer chaque identité numérique comme étant un avatar et à se demander si cet avatar pourrait être touché dans son intégrité numérique.
129. Dans cette hypothèse, lorsqu'un avatar subit une atteinte à son intégrité numérique, il faut rechercher le lieu où l'atteinte se fait ressentir. L'avatar étant une représentation numérique d'une personne ayant la caractéristique d'être indépendante de cette dernière, l'atteinte est uniquement ressentie dans l'espace numérique. C'est l'avatar, et non pas la personne, qui est victime de l'atteinte. Un avatar subit une atteinte à son intégrité numérique, par exemple, lorsqu'un réseau social tel que Facebook ou Twitter ferme le compte d'une personne contre son gré. L'avatar associé au compte subit alors une mort numérique dont les effets se font ressentir uniquement dans l'espace numérique.
130. Toutefois, nous réfutons l'idée qu'une personne puisse se dédoubler lorsqu'elle agit dans l'espace numérique. L'activité de la personne dans l'espace numérique est intrinsèquement liée à son existence dans le monde physique car c'est dans ce dernier lieu que les conséquences de son activité numérique sont ressenties¹¹⁷. A notre

¹¹⁴ Un profil LinkedIn qui retranscrit avec précision le parcours professionnel de la personne.

¹¹⁵ Un profil Instagram où la personne se met en scène.

¹¹⁶ Un site de discussion où les utilisateurs s'identifient par des pseudonymes afin de rester anonymes.

¹¹⁷ Voir *supra* N 122-123.

sens, il ne faut pas considérer que l'activité d'une personne physique ou morale sur Internet génère un doublon numérique que l'on pourrait qualifier d'avatar. Ceci amènerait à reconnaître une dissociation entre les deux « mondes » et signifierait qu'un acte illicite commis sur Internet à l'encontre d'une personne ne la toucherait pas directement, mais aurait uniquement un impact sur son avatar. Or, cette construction ne parvient pas à convaincre et doit être écartée. Les avatars des personnes physiques et morales ne constituent pas la population du numérique.

2. L'intelligence artificielle comme personne numérique

131. Il apparaît assez naturellement que l'intelligence artificielle puisse être qualifiée de personne numérique. Elle serait l'équivalent dans l'espace numérique de la personne physique dans le monde physique. Toutefois, la possibilité de qualifier une intelligence artificielle de personne reste une question philosophique grandement débattue¹¹⁸. Au niveau suisse et européen, la tendance actuelle est de ne pas reconnaître l'intelligence artificielle comme un sujet de droit¹¹⁹.
132. Un point central du débat est de déterminer le stade à partir duquel une intelligence artificielle est suffisamment intelligente, c'est-à-dire notamment capable de prendre des décisions tout en apprenant de

¹¹⁸ Voir p.ex. ALLGROVE, pp. 28-44 ou TURNER, pp. 175-205 pour un recensement de la littérature au sujet du débat sur la question de savoir s'il faut accorder la personnalité juridique à l'intelligence artificielle, et à quelles conditions.

¹¹⁹ Le Parlement européen a récemment adopté une résolution concernant un régime de responsabilité civile pour l'intelligence artificielle (Résolution du 20.10.2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle ; 020/2014(INL)) dans laquelle il exprime clairement que l'intelligence artificielle (IA) n'a « ni la personnalité juridique ni la conscience humaine » (consid. 6 du texte de la Proposition de Règlement). Partant, ce sont les personnes qui « créent, entretiennent ou contrôlent le risque associé au système d'IA » qui doivent être tenues pour responsables et non pas l'intelligence artificielle (N 7 de la Résolution). La Suisse suit la même optique en considérant que « [l]es robots n'ayant pas de personnalité juridique, une personne physique ou morale sera responsable des préjudices causés par l'IA si les conditions de responsabilité sont remplies. » (CONSEIL FÉDÉRAL, « Intelligence artificielle » – Lignes directrices pour la Confédération du 25.11.2020, p. 9).

sa propre expérience, et autonome pour qu'on puisse lui reconnaître des attributs de conscience et donc une personnalité¹²⁰. Selon nous, la question de l'autonomie est essentielle car tant qu'une intelligence artificielle n'est pas autonome, elle doit être rattachée à son créateur (ou son détenteur) et elle ne peut constituer une personne numérique à part entière qui serait titulaire de ses propres droits et obligations et serait ainsi capable de subir des atteintes à sa personnalité. Ce niveau d'intelligence n'a, à notre connaissance, pas encore été atteint. Mais la question n'en reste pas moins pertinente.

133. Si, à l'avenir, une intelligence artificielle ayant atteint un niveau d'intelligence et d'autonomie suffisant pour être titulaire de ses propres droits et obligations subissait une atteinte à sa personnalité, elle pourrait notamment se prévaloir du droit à l'intégrité numérique. L'atteinte commise par le biais d'Internet ne pourrait être localisée que dans l'espace numérique car le lieu de l'atteinte pourrait difficilement être rattaché à un Etat particulier¹²¹. En outre, l'intelligence artificielle ressentirait l'atteinte à sa personnalité dans l'espace numérique car c'est dans ce lieu qu'elle existe.

3. La DAO comme personne numérique

134. Les personnes morales retrouvent également leur équivalent dans l'espace numérique à travers les *Decentralized Autonomous Organizations* (DAOs). Les DAOs sont des véhicules numériques ayant vu le jour grâce à la technologie blockchain et présentant, à certains égards, des ressemblances avec les véhicules juridiques connus en droit suisse. Elles permettent à un groupe de personnes de mettre en commun leurs ressources et de gérer des actifs cryptographiques, par exemple des bitcoins, de manière décentralisée en vue d'atteindre un but commun. L'utilisation des actifs cryptographiques est régie par un modèle de gouvernance prédéfini à l'avance par la communauté dont les règles sont

¹²⁰ Voir notamment le *Test of Capacity for Personhood* établi par HUBBARD, p. 419. Voir aussi BENSOUSSAN/BENSOUSSAN, N 642, p. 146, selon lesquels plus une intelligence artificielle est intelligente et autonome, moins il est justifié de lui appliquer un régime similaire à celui de la chose ; ČERKA/GRIGIENÉ/SIRBIKYTĖ, pp. 11-12.

¹²¹ Voir *supra* N 116.

exécutées automatiquement par le code informatique. Les membres d'une DAO s'organisent donc entièrement dans l'espace numérique.

135. Le droit de certains Etats, dont l'Etat du Vermont aux Etats-Unis et Malte, prévoit la possibilité de constituer des DAOs, ce qui leur permet de s'« ancrer » dans ces juridictions et de bénéficier de la personnalité juridique. Le droit suisse ne règle pas ces nouvelles formes d'organisations sociales et il n'est donc pas possible de constituer une DAO en Suisse. Quoiqu'il en soit, la vaste majorité des DAOs existent simplement sur Internet, hors de tout cadre légal et elles déploient leurs activités principalement – voire exclusivement – dans l'espace numérique. Leurs membres, qui peuvent être répartis à travers le monde, sont généralement anonymes. Ces DAOs n'entretiennent donc aucun lien particulier avec un quelconque ordre juridique. A l'heure actuelle, aucun Etat n'accorde la personnalité juridique à ce type de DAOs¹²².
136. Lorsqu'une DAO subit une atteinte à sa personnalité, par exemple si la plateforme GitHub¹²³ ferme la page dédiée à son développement, c'est l'entité qui est visée, et non pas les membres à titre individuel. Même si elle ne dispose pas de la personnalité juridique, c'est la DAO qui souffre du dommage en tant que personne numérique, à l'instar de toute autre société qui subirait une atteinte similaire. L'atteinte est donc à la fois commise et ressentie dans l'espace numérique. Toutefois, il semble peu probable qu'une DAO puisse faire valoir son droit à l'intégrité numérique devant les tribunaux suisses tant que la personnalité juridique ne lui est pas accordée par le droit suisse. Les DAOs qui ne sont pas constituées selon le droit d'un Etat se retrouvent donc, pour l'heure, impuissantes face aux atteintes à leur personnalité.

¹²² Voir RIVA, pp. 619-638 au sujet de la reconnaissance des DAOs dans l'ordre juridique suisse, dans l'hypothèse où elles sont constituées selon la loi d'un Etat et celle où elles existent simplement sur Internet.

¹²³ GitHub est une plateforme d'hébergement qui permet notamment aux développeurs informatiques de garder la trace de toutes les versions du code de leurs projets.

VII. L'intégrité numérique : un droit fondamental dont l'Etat ne peut être le seul garant

137. Il ressort de l'analyse qui précède qu'il est envisageable¹²⁴ que certaines personnes (les intelligences artificielles et les DAOs) puissent avoir une existence exclusivement numérique digne d'être protégée par l'intégrité numérique. L'atteinte à l'intégrité numérique ne se matérialise donc pas nécessairement dans le monde physique. Partant, le lieu de l'atteinte à l'intégrité numérique peut être situé non seulement dans le monde physique, mais aussi simultanément ou exclusivement dans l'espace numérique. Les règles de droit international privé doivent donc être réinterprétées de manière à permettre une localisation du lieu de l'atteinte directement dans l'espace numérique.
138. Les plateformes offrant à tout un chacun un environnement propice à l'épanouissement personnel, social et culturel (p.ex. Facebook, Twitter) jouent un rôle central dans la définition de cet espace numérique. Une relation quasi-étatique s'est établie entre certaines plateformes qui jouissent d'une position dominante et leurs utilisateurs (A). Les Etats rencontrent de réelles difficultés à obtenir le respect des droits fondamentaux dans l'environnement numérique de ces plateformes. Cette situation nouvelle amène à redéfinir le rôle de l'Etat en tant que garant du respect des droits fondamentaux dans l'espace numérique et à confier ce rôle aux plateformes elles-mêmes (B).

A. La relation quasi-étatique entre les plateformes numériques et leurs utilisateurs

139. Les normes constitutionnelles ont le double rôle de protéger les individus contre des atteintes par l'Etat à leurs libertés et d'obliger l'Etat à garantir les libertés des individus. Il appartient au législateur national d'intégrer les normes protectrices dans son droit matériel afin d'assurer la protection des individus entre eux dans leurs relations horizontales. Par exemple, le droit à la vie inscrit à l'art. 10 Cst. féd. protège notamment contre la peine de mort. Ainsi, l'Etat ne peut pas ôter la vie. Le pendant de cette norme constitutionnelle

¹²⁴ Si ce n'est déjà aujourd'hui, tout au moins dans un proche avenir.

est retranscrit dans le code pénal qui sanctionne les individus ayant commis des infractions à la vie.

140. Cependant, dans le cas du droit à l'intégrité numérique, le besoin d'inscrire cette norme dans la Constitution semble avoir son origine dans l'expansion des plateformes numériques telles que Google, Facebook et Twitter. Les sociétés dirigeant ces plateformes ont acquis une position dominante vis-à-vis de leurs utilisateurs dans le monde entier. Les Etats sont déchirés entre le devoir de garantir un réseau Internet libre et ouvert, d'un côté, et le besoin de légiférer afin de sauvegarder les droits des usagers et les intérêts nationaux, de l'autre¹²⁵.
141. Même si certaines législations en vigueur réglementent spécifiquement l'utilisation d'Internet¹²⁶, les plateformes numériques jouissent d'une grande liberté dans l'application de ces règles et continuent d'imposer leur modèle d'affaires. Ce sont les plateformes qui édictent le cadre juridique applicable aux internautes et ceux-ci n'ont d'autre choix que d'y adhérer ou de s'exiler. Tout utilisateur est ainsi forcé d'accepter les règles d'utilisation des plateformes numériques qui sont devenues indispensables pour accéder à de l'information, et pour certaines personnes, pour générer leurs revenus. Cette situation inédite a pour conséquence que les Etats ne sont plus en mesure de garantir la liberté personnelle de leurs citoyens lorsque ceux-ci sont dans l'espace numérique¹²⁷.
142. C'est alors aux sociétés privées derrière les plateformes numériques que revient le rôle de garant des libertés des individus lorsqu'ils utilisent les plateformes numériques, car c'est contre elles que les libertés sont principalement dirigées dans l'espace numérique, à l'instar des Etats dans le monde physique. La position dominante des plateformes numériques crée une relation verticale entre elles et leurs utilisateurs qui est comparable à la relation existant entre les

¹²⁵ Voir MASSIT-FOLLÉA, pp. 17-45.

¹²⁶ Par exemple, le RGPD (Règlement (UE) n° 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 (règlement général sur la protection des données)) impose aux plateformes un cadre réglementaire pour le traitement des données personnelles.

¹²⁷ Voir MAHON, Intégrité numérique, N 16, pp. 55.

Etats et leurs citoyens. Il en résulte que les plateformes numériques entretiennent une relation quasi-étatique avec leurs utilisateurs.

B. L'obligation des plateformes numériques de protéger les libertés de leurs utilisateurs

143. La particularité du droit à l'intégrité numérique est que ce droit vise avant tout à protéger les libertés des individus lorsqu'ils se trouvent dans un environnement où l'Etat n'est pas en mesure d'assurer la protection des droits fondamentaux. Le but premier du droit à l'intégrité numérique n'est donc pas de protéger le citoyen contre l'Etat, mais l'utilisateur contre la plateforme numérique. La relation quasi-étatique existant entre une plateforme et ses utilisateurs a pour effet que c'est contre la plateforme que le droit à l'intégrité numérique vise à protéger les individus. De même, c'est avant tout à la plateforme que revient le devoir de protéger l'intégrité numérique des individus lorsque ceux-ci se trouvent dans son environnement. Le droit à l'intégrité numérique faisant partie des droits fondamentaux protégés à l'échelle internationale¹²⁸, les plateformes numériques ont le devoir de garantir ce droit de façon universelle, quand bien même le lieu de l'atteinte se trouve dans l'espace numérique.
144. Charger des sociétés privées du rôle de garant des droits fondamentaux peut sembler excessif. Mais ce concept s'inscrit dans un débat philosophique et politique déjà existant sur le rôle des GAFAM¹²⁹ dans une société démocratique¹³⁰. Le Congrès des Etats-Unis a convoqué les représentants de Facebook, Google et Twitter en 2017, après qu'il ait été établi que leurs plateformes avaient été utilisées dans le but d'influencer les élections présidentielles de 2016¹³¹. Ces sociétés ont alors été contraintes à prendre des mesures afin d'empêcher la prolifération de fausses nouvelles (*fake news*), sans quoi le Congrès aurait été dans l'obligation de réglementer les plateformes numériques. Elles se sont ainsi retrouvées, malgré elles, à devoir garantir les libertés des

¹²⁸ Voir *supra* note 73.

¹²⁹ Acronyme des géants du Web : Google, Amazon, Facebook, Apple et Microsoft.

¹³⁰ Voir *supra* note 10

¹³¹ Voir DOUEK.

utilisateurs de leurs plateformes, dont le droit à l'information et le droit à se former une opinion libre et éclairée, en instaurant des mécanismes permettant de vérifier la véracité des informations postées sur leurs plateformes et de filtrer les contenus considérés comme abusifs¹³².

145. C'est dans un contexte très tendu que le Congrès américain a convoqué à nouveau ces trois sociétés en 2020¹³³. Elles se sont retrouvées confrontées à de nouvelles critiques, en particulier venant de la droite républicaine, alors que le président américain Donald Trump s'était fait censurer 65 fois entre mai 2018 et octobre 2020 sur Twitter¹³⁴ et que tous les contenus liés au groupe conspirationniste QAnon, fervent supporter du président, avaient été supprimés des réseaux sociaux¹³⁵. Certains membres du Congrès ont reproché à Facebook, Google et Twitter de prendre parti sur des questions politiques et de censurer les idées de la droite. Selon eux, ces trois sociétés violent les droits des utilisateurs, en particulier leur liberté d'expression et d'opinion. Autrement dit, l'argument invoqué est une atteinte à l'intégrité numérique des personnes qui ont été censurées et/ou bannies des plateformes concernées.
146. Le Congrès américain a donc invoqué les garanties constitutionnelles pour, dans un premier temps, soutenir l'idée que

¹³² Voir l'étude menée par VOSOUGHI/ROY/ARAL en 2018 qui a établi que les algorithmes utilisés par les réseaux sociaux contribuent à la prolifération des fausses informations, ce qui peut avoir des effets préjudiciables sur la société : « *False news can drive the misallocation of resources during terror attacks and natural disasters, the misalignment of business investments, and misinformed elections.* » (p. 5).

¹³³ La Chambre des Représentants américaine avait rendu au préalable un rapport sur la concurrence dans les marchés numériques faisant part des dangers que représentent les géants du Web : « *The effects of this significant and durable market power are costly. The Subcommittee's series of hearings produced significant evidence that these firms wield their dominance in ways that erode entrepreneurship, degrade Americans' privacy online, and undermine the vibrancy of the free and diverse press. The result is less innovation, fewer choices for consumers, and a weakened democracy.* » (p. 7). Voir U.S. HOUSE JUDICIARY COMMITTEE'S SUBCOMMITTEE ON ANTITRUST, COMMERCIAL, AND ADMINISTRATIVE LAW, *Investigation of Competition in Digital Markets*, 2020, disponible sur : https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf (site consulté le 30.10.2020).

¹³⁴ Voir WEAVER/SCHEMMEL.

¹³⁵ Voir ORTUTAY.

les géants du Web ont l'obligation de protéger les droits des internautes qui naviguent sur leurs plateformes en limitant au maximum la prolifération des *fake news* et, dans un deuxième temps, pour empêcher ces mêmes sociétés de violer les droits des internautes en les censurant. Ce faisant, le Congrès américain a reconnu la position monopolistique ainsi que l'immense pouvoir que Facebook, Google et Twitter ont acquis à l'échelle mondiale et a érigé ces plateformes, en quelque sorte, au rang de quasi-Etats¹³⁶.

147. Ensemble, ces trois plateformes forment la base d'un territoire numérique, séparé du monde physique, dont certains Etats semblent prêts à reconnaître l'existence à la périphérie de leur propre territoire. Cette partie de l'espace numérique qui peut être définie précisément, dans la mesure où elle correspond aux plateformes numériques concernées, est un environnement particulier où le respect des droits fondamentaux – et notamment le droit à l'intégrité numérique – peut être revendiqué directement à l'encontre des sociétés privées derrière les plateformes.
148. Lorsque l'atteinte à l'intégrité numérique se produit dans l'espace numérique délimité par Facebook, Google et Twitter (et toute autre plateforme profitant d'une position dominante dans l'économie numérique), il doit être possible d'agir en justice contre ces sociétés pour demander la protection de ce droit. Comme le droit à l'intégrité numérique est un droit fondamental universel à la portée extraterritoriale¹³⁷, les plateformes numériques doivent garantir ce droit de façon universelle. Toutefois, la possibilité d'agir en justice contre lesdites sociétés pour faire valoir une atteinte à l'intégrité numérique ne sera possible que dans les Etats qui suivent une position semblable à celle du Congrès américain en reconnaissant le rôle de quasi-Etats de ces sociétés et/ou leur rôle de garant du droit à l'intégrité numérique.

¹³⁶ Voir WICHOWSKI qui caractérise les géants du Web de « *net-states* », car ils agissent de manière semblable aux gouvernements en bâtissant des empires par le biais d'investissements colossaux dans des projets qui sortent complètement de leurs domaines d'activités. Des infrastructures d'utilité publique telles qu'une monnaie ou la fourniture d'accès à Internet se retrouvent privatisées, rendant ainsi la tâche de plus en plus difficile pour les Etats de réguler les *net-states*.

¹³⁷ Voir *supra* IV.B.

VIII. Conclusion

149. En 2020, il semble de plus en plus irréaliste de vivre entièrement hors ligne sans aucune donnée personnelle ni identité en ligne. Il n'est tout simplement plus possible d'empêcher nos données de migrer dans l'espace numérique¹³⁸. Chacun d'entre nous a une existence numérique, même sans en avoir conscience. Bien plus, il y a une perte de contrôle de nos données personnelles qui sont continuellement prélevées à notre insu. Le risque qu'il soit porté atteinte aux droits de la personnalité s'en trouve accru. Les Etats en sont bien conscients et tentent d'améliorer la protection de la sphère privée et des droits fondamentaux de leurs citoyens dans l'espace numérique¹³⁹. C'est dans ce contexte de besoin élevé de protection de l'existence numérique que la question de la protection de l'intégrité numérique se pose.
150. L'intégrité numérique présente la particularité de protéger les individus contre des atteintes qui ont lieu – par définition – en ligne. L'atteinte à l'intégrité numérique a bel et bien lieu dans l'espace numérique et non pas uniquement dans le monde physique. Mais la frontière entre le monde physique et l'espace numérique est floue, car la vie et l'existence numérique d'une personne se croisent continuellement. On peut ainsi constater un phénomène de dédoublement du lieu de l'atteinte qui peut se matérialiser simultanément dans le monde physique et dans l'espace numérique. Une atteinte aux droits de la personnalité commise au moyen d'Internet n'est en effet pas uniquement virtuelle, mais est aussi subie dans le monde réel dans la mesure où la victime en ressent les effets dans son corps et son esprit. Toutefois, dans certains cas, le lieu de l'atteinte à l'intégrité numérique pourrait se trouver uniquement dans l'espace numérique. Il s'agit de l'hypothèse particulière des personnes numériques (l'intelligence artificielle et les DAOs) qui n'ont pas d'existence dans le monde physique et qui

¹³⁸ Voir KATSH/RABINOVICH-EINY, pp. 11-12 : « *In recent years, living offline entirely without either a data presence or an online identity has become less of a realistic option. The distinction that used to be made between the "virtual world" and the "real world" is losing meaning [...]. One simply cannot prevent data about oneself from migrating into cyberspace.* » (p. 12).

¹³⁹ Voir p.ex. la Convention 108+ (*supra* note 73).

ne peuvent donc ressentir l'atteinte à leur intégrité numérique que dans l'espace numérique.

151. Le constat qu'une atteinte à l'intégrité numérique peut être localisée dans l'espace numérique ébranle les fondations du droit international privé. Le centre de gravité d'une atteinte à l'intégrité numérique peut se trouver à la fois dans le monde physique et dans l'espace numérique, voire exclusivement dans l'espace numérique dans le cas des personnes numériques. Il en résulte une nécessaire redéfinition des règles de conflit dont la fonction première est de localiser la cause dans le territoire d'un Etat. L'existence d'un lieu de l'atteinte à l'intégrité numérique sur Internet doit être prise en compte dans l'application des règles de droit international privé de manière à permettre une possible localisation de la cause dans l'espace numérique. Cette démarche respecte mieux l'objectif de prévisibilité des règles de conflit que les diverses interprétations qui en sont faites visant à localiser à tout prix les atteintes à la personnalité par l'utilisation d'Internet dans le territoire d'un Etat.
152. Ce raisonnement serait abouti s'il était possible d'agir en justice pour demander le respect du droit à l'intégrité numérique auprès d'un organisme se trouvant dans l'espace numérique. A ce jour, il n'existe pas encore d'instance officielle auprès de laquelle il serait possible de demander la protection des droits de la personnalité dans l'espace numérique. Il n'y a pas non plus de tribunal supranational compétent pour ce type d'affaires.
153. Dans ces conditions, la victime d'une atteinte à l'intégrité numérique n'aura pas d'autre choix que de s'en remettre à la justice de l'Etat qui accordera à ses tribunaux la compétence de juger de la cause. Ce for devra être trouvé dans le monde physique au moyen des règles de droit international privé des Etats. Or, il est impossible d'ancrer le centre de gravité d'une atteinte à l'intégrité numérique dans le territoire d'un seul Etat. La victime de l'atteinte se trouvera ainsi dans une situation d'insécurité juridique quant au for, quant au droit applicable et, par voie de conséquence, quant à la portée de ses droits de la personnalité.
154. L'insécurité juridique existant en droit civil fait écho à l'impuissance des Etats à protéger les droits fondamentaux de leurs citoyens dans l'espace numérique. Il en résulte une sorte de glissement du pouvoir

étatique vers les plateformes numériques occupant une position monopolistique. Celles-ci sont amenées à devoir prendre le rôle de l'Etat pour assurer le respect des règles qu'elles ont elles-mêmes édictées en prononçant et en exécutant des décisions, telles que la modération du contenu mis en ligne par la censure ou le bannissement. Le Congrès américain semble déjà avoir reconnu l'existence d'une relation quasi-étatique entre les grandes plateformes qui jouissent d'une position dominante – de type Google, Facebook et Twitter – et leurs utilisateurs en imposant à ces plateformes l'obligation de protéger les droits des internautes qui naviguent dans leur environnement numérique. Facebook a ainsi lancé à la fin de l'année 2020 son Conseil de surveillance (*Oversight Board*) dont l'objectif est de juger de l'application par la plateforme de ses règles de modération des contenus au regard de la protection des droits fondamentaux des utilisateurs.

155. Il est ainsi possible de discerner les premiers signes de l'émergence de juridictions en ligne ayant la compétence de juger des causes dont le centre de gravité se trouve sur Internet. Si ces modes alternatifs de résolution des conflits en ligne devaient se développer, la fonction localisatrice de la règle de droit international privé aurait alors à nouveau tout son sens lorsque le critère de rattachement désigne un lieu de l'atteinte dans le territoire numérique. Ce « territoire » pourrait être défini, par exemple, par l'environnement numérique d'une plateforme.

Bibliographie

ALLGROVE BENJAMIN, Legal Personality for Artificial Intellects : Pragmatic Solution or Science Fiction ?, juin 2004, disponible sur : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=926015 (site consulté le 30.10.2020)

BENSOUSSAN ALAIN/BENSOUSSAN JÉRÉMY, IA, robots et droit, Bruxelles 2019

BONOMI ANDREA, Art. 129 et 139 LDIP, in : Bucher Andreas (édit.), Commentaire romand, Loi fédérale sur le droit international privé – Convention de Lugano, Bâle 2011 (cité : CR-LDIP/CL, BONOMI)

BUCHER ANDREAS, Art. 17 et 33 LDIP, in : Bucher Andreas (édit.), Commentaire romand, Loi fédérale sur le droit international privé – Convention de Lugano, Bâle 2011 (cité : CR-LDIP/CL, BUCHER)

BUCHER ANDREAS, Personnes physiques et protection de la personnalité, 5^e éd., Bâle 2009 (cité : Personnes physiques)

ČERKA PAULIUS/GRIGIENĖ JURGITA/SIRBIKYTĖ GINTARĖ, Is it possible to grant legal personality to artificial intelligence software systems ?, Computer Law & Security Review 2017, pp. 1-15

CONSEIL FÉDÉRAL, Message relatif à l'approbation du protocole du 10 octobre 2018 portant amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 6 décembre 1919, FF 2020 545 (cité : Message Convention 108+)

DESCHENAUX HENRI/STEINAUER PAUL-HENRI, Personnes physiques et tutelle, 4^e éd., Berne 2001

DESSEMONTET FRANÇOIS, Internet, la propriété intellectuelle et le droit international privé, in : Boele-Woelki Katharina/Kessedjian Catherine (édit.), Internet : Which Court Decides ? Which Law Applies ? – Quel tribunal décide ? Quel droit s'applique ?, La Haye/Londres/Boston 1998, pp. 47-64

DOUEK EVELYN, Congress' Grilling of Tech Companies in 2017 Foreshadows the Debates of 2018, Lawfare, 11 Janvier 2017, disponible sur : <https://www.lawfareblog.com/congress-grilling-tech-companies-2017-foreshadows-debates-2018> (site consulté le 30.10.2020)

DUTOIT BERNARD, Droit international privé suisse – Commentaire de la loi fédérale du 18 décembre 1987, 5^e éd., Bâle 2016 (cité : Commentaire)

DUTOIT BERNARD, Compétence législative et compétence judiciaire en cas d'actes illicites commis sur Internet en droit international privé suisse, in : Bénédicte Jérôme et al. (édit.), Responsabilité civile et assurance – Etudes en l'honneur de Baptiste Rusconi, Lausanne 2000, pp. 143-171 (cité : Actes illicites sur Internet)

GUILLAUME FLORENCE, Droit international privé – Partie générale et procédure civile internationale, 4^e éd., Bâle/Neuchâtel 2018

HUBBARD PATRICK, “Do Androids Dream?”: Personhood and Intelligent Artifacts, Temple Law Review, Vol. 83 (2010-2011), pp. 405-474

JAYME ERIK/SYMEONIDES SYMEON C., Internet and the Infringement of Privacy : Issues of Jurisdiction, Applicable Law and Enforcement of Foreign Judgments, disponible sur : <https://www.idi-il.org/app/uploads/2019/06/Commission-8-Internet-and-privacy-infringement-Symeonides-Travaux-La-Haye-2019.pdf> (site consulté le 30.10.2020) (cité : Rapport explicatif)

JOHNSON DAVID R./POST DAVID, Law and Borders – The Rise of Law in Cyberspace, Stanford Law Review 1996, Vol. 48, pp. 1367-1402

KATSH ETHAN/RABINOVICH-EINY ORNA, Digital Justice – Technology and the Internet of Disputes, New York 2017

KAUFMANN-KOHLER GABRIELLE, Internet : mondialisation de la communication – mondialisation de la résolution des litiges ?, in : Boele-Woelki Katharina/Kessedjian Catherine (édit.), Internet : Which Court Decides ? Which Law Applies ? – Quel tribunal décide ? Quel droit s'applique ?, La Haye/Londres/Boston 1998, pp. 89-142

LESSIG LAWRENCE, Code : And Other Laws of Cyberspace, Version 2.0, 2^e éd., New York 2006

MAHON PASCAL, Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? Le point de vue du droit constitutionnel, pp. 43 ss du présent ouvrage (cité : Intégrité numérique)

MAHON PASCAL, Droit constitutionnel – Droits fondamentaux, Vol. II, 3^e éd., Bâle/Neuchâtel 2015 (cité : Droit constitutionnel II)

MASSIT-FOLLÉA FRANÇOISE, La régulation de l'internet : fictions et frictions, in : Carmes Maryse/Noyer Jean-Max (édit.), Les débats du numérique, Paris 2013, pp. 17-45

ORTUTAY BARBARA, YouTube follows Twitter and Facebook with QAnon crackdown, AP News, 15 octobre 2020, disponible sur : <https://apnews.com/article/youtube-qanon-conspiracy-theories-ef03a889e68239de6692ce42666d97d8> (site consulté le 30.10.2020)

PAPAUX VAN DELDEN MARIE-LAURE, Le « droit à l'intégrité numérique » du point de vue de la protection de droit civil de la personnalité, pp. 65 ss du présent ouvrage

RIVA SVEN, Decentralized Autonomous Organizations (DAOs) in the Swiss Legal Order, Yearbook of Private International Law, Vol. 21 (2019/2020), pp. 601-638

ROCHEL JOHAN, L'intégrité numérique dans la Constitution : Entre liberté et technologies numériques, pp. 13 ss du présent ouvrage

ROUSSEL ALEXIS, Le droit à l'intégrité numérique de la personne, pp. 1 ss du présent ouvrage

SMITH GRAHAM, Cyberborders and the Right to Travel in Cyberspace, in : Kohl Uta (édit.), The Net and the Nation State : Multidisciplinary Perspectives on Internet Governance, Cambridge/New York 2017, pp. 125-144

TREPOZ EDOUARD, Jurisdiction in the Cyberspace, Revue suisse de droit international et européen (RSDIE) 2016, pp. 273-287

TURNER JACOB, Robot Rules – Regulating Artificial Intelligence, Cham 2019

VOSOUGHI SOROUSH/ROY DEB/ARAL SINAN, The spread of true and false news online, Science, Vol. 359 (2018), pp. 1146-1151

WALTER JEAN-PHILIPPE, L'intégrité numérique : une nécessité du point de vue du droit à la protection des données ?, pp. 95 ss du présent ouvrage

WEAVER CORINNE/SCHEMMEL ALEC, Twitter, Facebook Censored Trump, Campaign 65 Times, Leave Biden Untouched, mrc News Busters, 19 octobre 2020, disponible sur : <https://newsbusters.org/blogs/techwatch/corinne-weaver/2020/10/19/twitter-facebook-censored-trump-campaign-65-times-leave> (site consulté le 30.10.2020)

WICHOWSKI ALEXIS, 'The U.S. can't regulate Big Tech companies when they act like nations', The Washington Post, 29 octobre 2020, disponible sur : <https://www.washingtonpost.com/outlook/2020/10/29/antitrust-big-tech-net-states/> (site consulté le 30.10.2020)

La question de la protection de l'intégrité numérique se pose dans le contexte du respect des droits de la personnalité dans l'espace numérique. La protection de l'intégrité physique et psychique peut-elle être étendue à l'intégrité numérique ? Est-il nécessaire de créer de nouvelles règles de droit pour protéger l'intégrité numérique ?

Le présent ouvrage offre une analyse transversale du droit à l'intégrité numérique en rassemblant les contributions des intervenantes et intervenants au colloque qui s'est tenu à l'Université de Neuchâtel, en date du 21 février 2020, sur le thème « Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? ». Il s'ouvre sur deux contributions présentant le concept de droit à l'intégrité numérique dont il ressort que ce droit doit être mis en relation avec la reconnaissance d'une vie numérique (*Alexis Roussel*) ; le rôle de ce droit est de cristalliser une conception de la liberté individuelle dans l'environnement numérique (*Johan Rochel*). Les contributions suivantes analysent le droit à l'intégrité numérique du point de vue du droit constitutionnel (*prof. Pascal Mahon*), du droit civil (*prof. Marie-Laure Papaux van Delden*), du droit pénal (*prof. André Kuhn*), du droit à la protection des données (*Jean-Philippe Walter*), de la liberté de la presse (*prof. Bertil Cottier*) et du droit international privé (*prof. Florence Guillaume et Sven Riva*).