UNIVERSITÉ DE NEUCHÂTEL

Le droit à l'intégrité numérique

Réelle innovation ou simple évolution du droit ?

Edité par Florence Guillaume et Pascal Mahon

Helbing Lichtenhahn

LE DROIT A L'INTÉGRITÉ NUMÉRIQUE

Edité par
Florence Guillaume et Pascal Mahon

Faculté de droit de l'Université de Neuchâtel
Helbing Lichtenhahn

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

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

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

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 *lex fori* 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 discorde. 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 auteur[1] 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 auteur[2] 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 moral[4].

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 personne[5].

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 CC[6].

11. L'action en protection de la personnalité[7] 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. 28*a* 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. 28*a* 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. 28*a* 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 531-533*a*, pp. 165-166.

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

6 DESCHENAUX/STEINAUER, N 540-540*a*, 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 570-608*a*, pp. 186-207.

sa personnalité. Enfin, une action en remise du gain réalisé par l'auteur de l'atteinte (art. 28*a* al. 3 CC et art. 423 CO) permet d'éviter que celui-ci ne s'enrichisse au détriment de la victime[8].

12. La portée des droits de la personnalité sera interprétée par le juge civil d'une manière conforme aux garanties constitutionnelles des droits fondamentaux[9]. 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 particuliers[10]. 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 personnalité[11].

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 personnelles[12]. 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 internationale[13]. 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 illicites[16].

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 dommage[17].

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 habituelle[18] 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 part[19]. Ces fors sont ouverts pour toute action fondée sur une atteinte à la personnalité, et notamment une atteinte à l'intégrité physique ou psychique[20]. Ils sont également pertinents pour la protection de l'intégrité numérique[21].

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 protégé[22]. 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 pays[25]. 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 résultat[26].

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 lésé[27].

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 internationale[28]. Les prétentions fondées sur une atteinte à la personnalité entrent clairement dans le champ d'application matériel de la Convention de Lugano[29]. 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 Lugano[30].

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-intérêts[31], 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 Suisse[33].

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 accrue[34].

31. Le deuxième et le troisième fors figurent à l'art. 5 ch. 3 CL. Cette disposition offre la possibilité d'attraire 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 cadre[35].

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 contractant[36].

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 Lugano[37]. 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 for[41]. 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 immédiate[43]. 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 initial[44].

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 Internet[46].

---

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 statutaire[49]. 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 victime[51].

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 attrait »[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 prépondérante[53].

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 saisie[54]. 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 disposition[55].

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 juridictions[56].

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 remplie[57].

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 élection 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 réseau[61]. 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 technologie[63].

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 doctrine[65] 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 répandue[66]. 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 Etat[67]. 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 suisse[69]. 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 suisse[70]. 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 étrangère[71].

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 civil 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 constitutionnelle[72].

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 international[73]. 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 2019[74].

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 complexes[76]. 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 saisi[77].

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'Internet[78]. 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 juridiction[79]. 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 universelle[80].

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'Internet[81]. 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 transfrontière[82] 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 domaine[83].

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 Résolution[84]. 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 résidence[85] 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 prétentions[89]. 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'harceler 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 entier[90]. 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 droit[92].

80. Le rattachement à la *lex fori* présente également l'avantage de faciliter la qualification de l'atteinte. Pour tenir compte des différences – essentiellement terminologiques[93] – 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 vu[94], 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'Internet[95]. 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 internationale[96], 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 cyberespace régissant cet environnement qui serait issue d'un processus d'autorégulation d'Internet[97].

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 cyberespace. L'enjeu consiste en effet à déterminer si une atteinte à l'intégrité numérique peut être localisée dans l'environnement numérique (le cyberespace), 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 calomniée[98].

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'Internet[99]. 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 consacrera 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 boycott[101] 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 conception[102] à laquelle nous nous rallions. Comme nous le verrons si-dessous[103], 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.

numérique[104]. 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 physique[105]. Mais comme nous l'avons vu, cette démarche n'est pas satisfaisante[106].

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 électronique[107]. 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 numérique[108]. 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 sociaux[109]. 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 hypermnésiques[110] 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 aux 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 physiquement[111]. 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 numérique[112]. 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 droits[113], 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 liée[114], partiellement liée[115], voire même pas du tout liée[116] 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 ressenties[117]. 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 débattue[118]. Au niveau suisse et européen, la tendance actuelle est de ne pas reconnaître l'intelligence artificielle comme un sujet de droit[119].

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 personnalité[120]. 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 particulier[121]. 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 réglée 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/SIRBIKYTÉ, 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. Quoi qu'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 DAOs[122].

136. Lorsqu'une DAO subit une atteinte à sa personnalité, par exemple si la plateforme GitHub[123] 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 envisageable[124] 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'autre[125].

141. Même si certaines législations en vigueur réglementent spécifiquement l'utilisation d'Internet[126], 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 numérique[127].

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 règlementaire 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 internationale[128], 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 GAFAM[129] dans une société démocratique[130]. 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 2016[131]. 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 abusifs[132].

145. C'est dans un contexte très tendu que le Congrès américain a convoqué à nouveau ces trois sociétés en 2020[133]. 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 Twitter[134] et que tous les contenus liés au groupe conspirationniste QAnon, fervent supporter du président, avaient été supprimés des réseaux sociaux[135]. 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-Etats[136].

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 extraterritoriale[137], 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 numérique[138]. 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 numérique[139]. 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, 5e éd., Bâle 2009 (cité : Personnes physiques)

ČERKA PAULIUS/GRIGIENÉ JURGITA/SIRBIKYTÉ GINTARÉ, 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 2019, FF 2020 545 (cité : Message Convention 108+)

DESCHENAUX HENRI/STEINAUER PAUL-HENRI, Personnes physiques et tutelle, 4e 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, 5e 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 : Bénédict 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, 4e 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-iil.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, 2e 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, 3e 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

TREPPOZ 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)