

Le droit à l'intégrité numérique

Réelle innovation ou simple évolution du droit ?

Edité par Florence Guillaume et Pascal Mahon

LE DROIT A L'INTÉGRITÉ NUMÉRIQUE

Edité par
Florence Guillaume et Pascal Mahon

Faculté de droit de l'Université de Neuchâtel
Helbing Lichtenhahn



FACULTÉ DE DROIT

Information bibliographique de la Deutsche Nationalbibliothek

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

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

ISBN 978-3-7190-4456-5

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

www.helbing.ch

www.unine.ch/droit

Préface

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

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

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

Préface

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

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

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

Préface

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

Florence Guillaume et Pascal Mahon
Neuchâtel, novembre 2020

Sommaire

ALEXIS ROUSSEL Cofondateur de Bity, Neuchâtel Le droit à l'intégrité numérique de la personne	1
JOHAN ROCHEL Chercheur à l'Université de Zurich L'intégrité numérique dans la Constitution : Entre liberté et technologies numériques	13
PASCAL MAHON Professeur à l'Université de Neuchâtel Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? Le point de vue du droit constitutionnel	43
MARIE-LAURE PAPAUX VAN DELDEN Professeure à l'Université de Genève Le « droit à l'intégrité numérique » du point de vue de la protection de droit civil de la personnalité	65
ANDRÉ KUHN Professeur à l'Université de Neuchâtel Le droit à l'intégrité numérique est-il une innovation ou une extension de l'intégrité physique ?	87

Sommaire

JEAN-PHILIPPE WALTER Commissaire à la protection des données du Conseil de l'Europe L'intégrité numérique : une nécessité du point de vue du droit à la protection des données ?	95
BERTIL COTTIER Professeur associé à la Faculté de droit de l'Université de Lausanne Professeur invité à l'Académie de journalisme de l'Université de Neuchâtel Membre de la Commission fédérale des médias L'intégrité numérique : un obstacle au journalisme d'investigation ?	103
FLORENCE GUILLAUME et SVEN RIVA Professeure à l'Université de Neuchâtel Assistant-doctorant à l'Université de Neuchâtel L'atteinte à l'intégrité numérique appréhendée par le droit international privé.....	117

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

par

Pascal Mahon

Professeur à l'Université de Neuchâtel

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

I. Introduction

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

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

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

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

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

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

Réelle innovation ou simple évolution du droit ? Le point de vue constitutionnel

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

II. Les protections existantes et leur application au numérique

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Cette obligation « constitutionnelle » pour l'Etat de protéger la sphère et la vie privées des individus a du reste entraîné une grande activité régulatrice ou « législative », mais aussi jurisprudentielle, en la matière, et ce au plan international comme au plan national. Pour ce qui est de l'action régulatrice ou du moins promotrice, on peut mentionner, pour ne citer que quelques exemples – et sans prétention aucune à l'exhaustivité – divers règlements et directives de l'Union européenne, dont le fameux « RGPD », soit le *Règlement (UE) 2016/679 du Parlement européen et du Conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, du 27 avril 2016 (RGPD)²⁰, entré en vigueur en mai 2018, sur lequel on reviendra. On peut citer aussi diverses conventions et recommandations, notamment du Conseil de l'Europe, dont la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, du 28 janvier 1981²¹, qui ne fait, elle non plus, pas

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

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

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

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

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

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

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

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

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

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

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

²⁵ CJUE, arrêt (grande chambre) C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés [CNIL]*, du 24 septembre 2019, dispositif : « L'article 12, sous b), et l'article 14, premier alinéa, sous a), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ainsi que l'article 17, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46 (règlement général sur la protection des données), doivent être interprétés en ce sens que, lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application de ces dispositions, il est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur,

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

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

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

²⁷ *Ibidem*, par. 122 et 124.

²⁸ *Ibidem*, par. 123.

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

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

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

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

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

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

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

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

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

A. L'« intégrité numérique » et ses caractéristiques

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

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

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

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

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

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

³⁶ *Ibidem*, N 20.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⁴⁷ PERNOT-LEPLAY, ch. 1.2.

⁴⁸ PERNOT-LEPLAY, ch. 1.2.

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

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

IV. Conclusion

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

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

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

Réelle innovation ou simple évolution du droit ? Le point de vue constitutionnel

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

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

Pascal Mahon

Bibliographie

- AUBERT JEAN-FRANÇOIS, La liberté d'opinion, RDS 1973 I, pp. 429-450
- AUBERT JEAN-FRANÇOIS/MAHON PASCAL, Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999, Zurich/Bâle/Genève, 2003
- BARBEY GRÉGOIRE, Les données personnelles ne sont la propriété de personne, En réponse à la chronique de Philippe Nantermod dans Le Temps intitulée « Données, c'est données, reprendre c'est voler », L'Affranchi, 9 avril 2019 (www.affranchi.ch)
- CHARLET FRANÇOIS, Le Data Protection Officer dans le secteur privé suisse, Jusletter 18 juin 2018
- EPSTEIN LEE/WALKER THOMAS G., Constitutional Law for a Changing America, Rights, Liberties, and Justice, 10^e éd., Washington D.C., 2019
- FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, PJA 2013/6, pp. 837-864
- KAUFMANN CHRISTINE/GHIELMINI SABRINA/MEDICI GABRIELA/PULVER FANNY, Das Recht auf Privatsphäre im digitalen Zeitalter, Staatliche Schutzpflichten bei Aktivitäten von Unternehmen, Studie SKMR, 22 septembre 2016, https://www.skmr.ch/cms/upload/pdf/160922_SKMR-Studie_Privatsphaere.pdf (cité : KAUFMANN et al., *Studie*)
- KAUFMANN CHRISTINE/GHIELMINI SABRINA/MEDICI GABRIELA/PULVER FANNY, Das Recht auf Privatsphäre im digitalen Zeitalter – Staatliche Schutzpflichten bei Aktivitäten von Unternehmen, Update zur SKMR-Studie vom 22. September 2016, 12 février 2020, https://www.skmr.ch/cms/upload/pdf/2020/200107_Privatsphaere_Formatiert_DEF.pdf (cité : KAUFMANN et al., *Update*)
- MÉTILLE SYLVAIN, Le droit au respect de la vie privée : les défis digitaux, Une perspective de droit comparé, Suisse, Etude, Service de recherche du Parlement européen, Bruxelles, Union européenne, octobre 2018, https://serval.unil.ch/resource/serval:BIB_25D40801BCE2.P001/REF
- PERNOT-LEPLAY EMMANUEL, Le droit à la portabilité des données dans le RGPD, Etude en ligne, 25 mai 2018, <https://pernot-leplay.com/fr/droit-portabilite-des-donnees-rgpd/#more-258>

Réelle innovation ou simple évolution du droit ? Le point de vue constitutionnel

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