Le droit de la vulnérabilité au risque du numérique

Poullet, Yves

Published in:
L'identité en question

Publication date:
2022

Document Version
le PDF de l'éditeur

Sous la direction de
Laura Rizzerio et
Dominique Lambert

L'identité en question

Entre parcours de vulnérabilités et chemins d'autonomie

UNIVERSITÉ DE NAMUR

L'identité en question

Entre parcours de vulnérabilités et chemins d'autonomie

Sous la direction de
Laura Rizzerio
et Dominique Lambert

L'identité en question

Entre parcours de vulnérabilités et chemins d'autonomie

Philosophies
Religions
& Sociétés

PRESSES
UNIVERSITAIRES
de Namur

Collection *Philosophies, Religions & Sociétés*
n° 4

Rue Grandgagnage, 19
5000 Namur (Belgique)
Tél : +32 (0) 81 72 48 84
E-mail : pun@unamur.be
Site web : https://www.pun.be

Dépôt légal : D/2022/1881/10
ISBN – version papier : 978-2-39029-119-0
ISBN – version numérique : 978-2-39029-120-6

Imprimé en Belgique

Le droit de la vulnérabilité au risque du numérique[1]

Yves Poullet

1. Le fil rouge – L'invitation qui m'a été faite à parcourir les relations entre trois concepts : le concept de vulnérabilité, celui de droit et, enfin, celui de numérique m'a séduit. D'emblée, il m'apparaissait que les applications d'un numérique de plus en plus ubiquitaire et « intelligent » non seulement renforçaient les vulnérabilités traditionnelles, mais en introduisaient d'autres plus essentielles qui touchaient à notre fragilité d'êtres humains. Dans le même temps, il était indéniable que le numérique nous permettait de dépasser ces vulnérabilités et d'accroître nos capacités de connaissance, d'action, voire notre identité. Cette ambiguïté ou, plutôt, cette « double face » du numérique ne devait-elle pas être l'objet d'une attention particulière d'un droit au service de la société et, plus précisément, à l'intérieur de celle-ci, au service des « faibles », des personnes handicapées, des « exclus » et des « sans voix » ?

Se dessinait dès lors la logique du propos. Ne fallait-il pas tout d'abord circonscrire ce qu'était la vulnérabilité (I), avant de s'interroger sur les relations que traditionnellement le droit entretenait avec la vulnérabilité et s'interroger sur les tendances nouvelles de cette relation (II) ? Relater ensuite l'ambiguïté de l'impact des applications numériques sur le sort des « vulnérabilités » et, au-delà, de la vulnérabilité humaine (III) devait m'amener, c'était mon espoir, à mieux comprendre la façon dont le droit tente de corriger ces impacts négatifs, tout en soulignant les limites et parfois les dangers de cette intervention (IV), avant de conclure mes réflexions non point définitivement, mais temporairement, dans la mesure où celles-ci s'arrêtent à un stade d'une évolution technologique largement imprévisible.

Sur tous ces points, je serai sommaire, conscient que bien des choses pourraient être ajoutées sur chacun des thèmes évoqués. Mon souci consiste plus à dégager des idées fortes et non à détailler les multiples législations qui seront évoquées. Pour l'analyse en profondeur de certaines dispositions

[1] Le manuscrit a été remis en février 2018. Même s'il a été relu en août 2020, il n'a pu tenir compte de textes ou réflexions plus récents. Le lecteur voudra bien en excuser l'auteur.

légales que j'évoque, je renvoie par ailleurs le lecteur à un ouvrage de ma Faculté de droit de Namur récemment publié[2].

I. La vulnérabilité – Un concept en quête de définition

2. Le concept de vulnérabilité est approché de mille manières par les philosophes – Certains l'approchent de manière négative, soulignant que le concept vise des situations où les personnes concernées se trouvent dans l'incapacité d'exercer pleinement leur potentialité d'êtres humains ; d'autres, à l'inverse, soulignent que ces situations de vulnérabilité constituent une expérience positive. Elles offrent, pour ceux en situation de vulnérabilité, une expérience positive, une opportunité d'agir au-delà d'eux-mêmes et de s'autodéterminer : « Paradoxalement, c'est d'ailleurs dans les situations où la vie s'éprouve particulièrement vulnérable qu'elle est sans doute capable de se posséder elle-même, d'initier en son être des formations nouvelles »[3].

Cette seconde approche, certes anthropologiquement défendable et en tout cas généreuse, ne rejoint pas celle de l'entendement commun ni celle du droit. Parcourant les nombreuses définitions que la littérature offrait, je me suis arrêté à celle proposée par des sociologues belges[4] : « La vulnérabilité se présente comme une expérience influençant négativement la capacité d'agir des individus, leur capacité à créer des situations socialement valorisantes pour s'intégrer pleinement dans la société. » La définition me paraissait intéressante à divers titres. Le premier est qu'elle définissait l'individu non comme une entité abstraite, une entité en soi, un « sujet de droit » autonome, jouissant pleinement de son libre arbitre et pleinement conscient, elle le voyait au contraire comme une capacité limitée d'action sur ce qui l'entoure, capacité que diverses contraintes intrinsèques au sujet ou extrinsèques à lui limitent, voire flétrissent, et ne lui permettent pas de réaliser pleinement ses virtualités[5].

3. Cette première pensée en amenait une autre – Comment ne pas voir dans cette définition une allusion à la théorie des « *capabilities* »,

---

[2] H. Jacquemin et M. Nihoul (dir.), *Vunérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018. *Cf.* également, de manière plus spécifique à propos de la vulnérabilité des personnes âgées, l'ouvrage collectif publié sous la direction de C. Hervé, M. Stanton et M. Deschenes, *Les personnes âgées et le numérique*, Coll. Éthique biomédicale et normes juridiques, Paris, Dalloz, 2019.

[3] D. Doat, « La vulnérabilité : esquisse d'une reconstruction conceptuelle », *Revue de théologie et de philosophie,* n° 48, 2016, p. 751.

[4] P. Brotcorne, L. Damhuis, V. Laurent, G. Valenduc et P. Vendramin, *Diversité et vulnérabilités dans les usages des TIC*, Gent, Academia Press, 2010, p. 63, http://www.belspo.be/belspo/ta/publ/academia-usagesTIC-U1527.pdf.

[5] Sur ce point, lire l'ouvrage de B. Feltz, M. Missal et A. Sims (dir.), *Free Will, Causality, and Neuroscience*, Leiden/Boston, Éd. Brill/Rodoi, 2020.

développée par le prix Nobel d'économie : A. Sen[6] ? Cette théorie généreuse exige de l'État qu'il offre à tous les citoyens les conditions qui effectivement les rendent capables, dans le contexte socio-économique et culturel qui est le leur, de devenir « *fuller social persons, exercising their own volitions and to interact with – and influence – the world in which they live* ». Sen insiste en effet sur le fait que la maîtrise de l'environnement par l'individu n'est pas évidente et ne dépend pas de son seul bon vouloir, mais présuppose en particulier un rôle actif de l'État, qui doit rendre possible cette maîtrise. Par ailleurs, le concept souligne la nécessité de prendre en compte les conditions d'effectivité de libertés posées non comme des « en-soi », mais comme un but à atteindre[7]. Il s'agit, très concrètement, de s'interroger, en particulier pour les personnes vulnérables, sur les moyens qui leur sont offerts pour la réalisation d'elles-mêmes dans un contexte où des choix certes parfois limités, mais pleins de signification, restent possibles. J'aurai l'occasion (*infra*, n° 8) de souligner combien cette démarche rejoint celle du droit à travers sa proclamation des droits de l'homme.

4. De la vulnérabilité et des catégories de personnes vulnérables – Sans doute, faut-il, à la lumière de ce que nous en disent les anthropologues, distinguer diverses vulnérabilités. Il est coutume de les rassembler sous deux catégories. La première regroupe les vulnérabilités intrinsèques liées à la constitution physiologique de certaines personnes : les personnes handicapées mentales ou physiques, les enfants, les personnes

---

[6] A. Sen, « Elements of a theory of human rights », *Philosophy and Public Affairs*, n° 32, 2004, p. 315 et s. ; *Commodities and Capabilities*, Amsterdam/New York, Elsevier Science Pub. Co., 1985 ; « Economics, law and ethics », *in* R. Gotoh et P. Dumouchel (dir.), *Against Injustice, the New Economics of Amartya Sen*, Cambridge, Cambridge University Press, 2009 ; et « Human rights and capabilities », *Journal of Human Development*, 2, 2005, n° 6, p. 155-166. À noter la même référence à la notion de « capacité » défendue par D. Doat (« La vulnérabilité, *cit*. », p. 737) à propos des personnes vulnérables : « En ce sens premier de "capacité", la vulnérabilité ou le fait pour tout être sensible d'être "vulnérable" en raison de son mode d'être, indique un état de possibilité propre à toute vie susceptible de recevoir des modifications en vertu d'une cause externe. »

[7] M. Nussbaum, « Capabilities and human rights », *Fordham Law Review*, n° 2, 1997, p. 273-300 ; L. Costa, *Virtuality and Capabilities in a World of Ambient Intelligence*, Dordrecht, Springer, 2016, p. 75 et s., résume la thèse de Nussbaum qui s'appuie sur une conception « aristotélicienne » de la démocratie : « *Nussbaum makes a noteworthy point concerning the theoretical affiliation of the capability approach. She connects the approach with the political thinking of Aristotle, arguing "that human flourishing has material and institutional necessary conditions that can be described and also realized". "Aristotelian Social Democracy", says Nussbaum, is broad in the sense "it is concerned with the good living not of an elite few, but of each and every member of the polity" and it is deep as "it is concerned not simply with money, land, opportunities, and offices, the traditional political distributables, but with the totality of functionings that constitute the good human life". From this perspective, the task of the political arrangement is to secure the conditions of a full, good life, or human flourishing for people. Therefore, the "broadness" of the capability approach is related to its concerns with equality and its "depth" related to its focus on what people are effectively able to "be" and "do".* »

âgées, autant de sous-catégories classables sous ce vocable. La seconde comprend, sous le vocable de vulnérabilités extrinsèques ou relationnelles, différentes sous-catégories considérées pour des raisons financières (les pauvres) ou de position économique défavorable (les consommateurs), mais également au regard de considérations sociales (les femmes, les étrangers, aujourd'hui, les LGBT…) comme susceptibles d'être défavorisées. Les anthropologues ont l'habitude de distinguer, de ces vulnérabilités, une troisième catégorie, celle ontologique : la vulnérabilité de tout être humain, celle constitutive de notre condition d'être humain, fragile et souffrant. Cette distinction est utile. La protection du droit a suivi cette distinction, élargissant progressivement son domaine, depuis certaines catégories de personnes caractérisées par une vulnérabilité intrinsèque à celles frappées de vulnérabilités extrinsèques et, plus récemment, elle entend couvrir notre vulnérabilité fondamentale. On le verra, le droit du numérique s'intéresse tant à des catégories particulières de vulnérabilité qu'à celle ontologique de l'homme.

II. Le droit et la protection de la vulnérabilité : une question de sens

5. L'essence du droit est en particulier de soutenir le faible contre le fort – L'expression est forte, elle n'est pas sans rappeler celle du R. P. Lacordaire qui déjà, en 1848, proclamait : « Entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime et la loi qui affranchit »[8]. Cette attention particulière du droit vis-à-vis de la vulnérabilité s'explique aisément. Le droit poursuit une œuvre de justice au sens le plus noble du terme. Certes, la justice ne se conçoit pas uniquement comme un impératif de justice « distributive » (*répartir les richesses créées au mieux des intérêts de chacun, sans oublier personne*), par opposition à celle dite commutative (*veiller à la sécurité et à l'égalité dans les échanges*), autre face de la justice humaine, mais, indéniablement, c'est son essence de tenter l'équilibre entre, d'une part, ordre, sécurité et affirmation des droits de chacun (droit à « sa » propriété, droit à la liberté de ses transactions, « droit » à son développement personnel) et, d'autre part, le souci d'autrui, d'un développement de tous, le devoir de solidarité. L'adage « De chacun selon ses moyens, à chacun selon ses besoins » traduit maladroitement cette exigence de solidarité : le droit pour chacun d'avoir une vie digne exige la garantie d'accès à ce qui, dans une société donnée, est jugé nécessaire pour une vie digne. Ce devoir de l'État d'offrir à chacun les moyens d'une vie digne peut justifier

[8] H.-D. Lacordaire, « Du double travail de l'homme », *in Œuvres du R. P. Henri-Dominique Lacordaire de l'ordre des Frères prêcheurs*, vol. IV, Paris, Poussièlgue Frères, 1872, p. 471-495.

des discriminations positives, comme l'affirment Rawls[9] et bien d'autres auteurs.

6. Les droits de l'homme au secours de la vulnérabilité – Parlant de dignité[10], le lecteur se voit renvoyé aux autres droits de l'homme dont l'exercice n'est possible que dans la mesure où, à la proclamation de chacune des libertés, s'attache une obligation dite « positive » de l'État de la rendre effective et de veiller, le cas échéant, à ce que les acteurs privés veillent également à la traduction concrète de cette exigence. Depuis la *Convention européenne des droits de l'homme* en 1950, la Cour européenne de Strasbourg a maintes fois rappelé, en ce sens, le principe d'obligations positives des États et d'effet horizontal de la proclamation de ces libertés[11]. La protection des vulnérables y trouve une seconde justification de l'intervention de l'État.

Ainsi, la liberté d'expression n'exige-t-elle pas que chacun, peu importe son niveau intellectuel ou sa fortune, ait l'accès à l'information détenue par l'État si l'on souhaite qu'il puisse jouer son rôle de citoyen et donc de critique de l'action publique ? Le même souci explique que chacun puisse s'exprimer dans sa langue, bénéficie de traductions, y compris en langage Braille ou langue des signes, etc. ? La liberté d'opinion religieuse exige que l'employeur ne puisse interdire les portes de son entreprise à des personnes issues de minorités religieuses. Les conséquences du droit à la vie privée, en particulier, se sont élargies considérablement à la faveur des

---

[9] J. Rawls, *Théorie de la justice*, Paris, Seuil, 1997 ; R. Boudon, « Justice sociale et intérêt général : à propos de la *Théorie de la justice* de Rawls », *Revue française de science politique*, n° 25/21975, p. 193-221. *Cf.* également R. Dworkin, *Taking Rights Seriously*, Cambridge, Harvard University Press, 1977.

[10] Sur la distinction entre dignité et autonomie, lire A. Rouvroy et Y. Poullet, « The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy », *in Reinventing Data Protection?*, Dordrecht, Springer, 2009, p. 159 et s. « *Dignity should not be reduced to autonomy. It says more. Although originally a virtue of outstanding persons and a virtue of self-control in healthy life – qualities which can be lost, for instance by lack of responsibility or in extreme illness – it has been universalised as a quality of the person as such. It now refers to both the intrinsic value of the individual and the intersubjective value of every human being in its encounter with the other. Thus, it expresses the outstanding position of the human individual in the universe as being capable of both autonomy in rational action and involvement in a good life for and with the others in just institutions. Respect for the dignity of human being is respect for its inviolability in common life. Dignity concerns both oneself and the other: I must behave with dignity, and I must consider the dignity of the other; I must not give up civilised and responsible behaviour, and the other should not be commercialised and enslaved. Human rights are built on this principle of dignity.* »

[11] Sur la signification de ces deux principes et la multiplication de leurs applications en matière de vie privée, lire F. Sudre, « Rapport introductif », *in Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Coll. Droit et Justice, Bruxelles, Bruylant, n° 63, 2005, p. 27 et s.

principes rappelés ci-dessus[12]. N'y voit-on pas la source de l'obligation des administrations de se rendre accessibles aux personnes handicapées, leur devoir de prévenir les candidats à des logements sociaux des risques environnementaux liés à cette localisation ? Les employeurs se voient interdire toute discrimination envers les femmes, les personnes étrangères. La loi est tenue d'établir l'égalité entre enfants naturels et ceux adoptés (arrêt *Marckx*). Progressivement, le concept de vie privée a couvert l'« ensemble des prérogatives qui apparaissent nécessaires pour amener le développement de la personnalité de l'individu dans une société donnée et pour assurer ainsi la vitalité de nos sociétés démocratiques ». Que la prise en considération des atteintes à la vulnérabilité de l'homme induites par les applications de plus en plus ubiquitaires et intrusives de notre société du numérique explique l'obligation positive de nos États de légiférer vis-à-vis de ces nouveaux risques, en particulier, en développant des lois de protection des données imposées tant aux autorités publiques que privées[13]. Je reviendrai sur ce point, mais, auparavant, parlons de la manière dont le droit s'est préoccupé de la vulnérabilité.

7. La protection des personnes vulnérables à l'heure du Code civil et la multiplication de législations spécifiques relatives à des catégories de personnes vulnérables aux XIX^e^ et XX^e^ siècles – Depuis la nuit des temps, et notre Code civil de 1804 en porte la trace, le droit a souhaité protéger les personnes atteintes ou susceptibles d'être atteintes dans leur capacité de développement au vu tantôt de leur jeunesse, tantôt de leur faiblesse de caractère ou handicap mental (les fous, les prodigues, mais également, jusqu'il y a peu, les femmes) en les dotant d'un représentant chargé de protéger leurs intérêts économiques : un tuteur, un administrateur des biens… Plus récemment, et toujours en lien avec cette vulnérabilité

[12] Sur cette extension, Y. Poullet, *La vie privée à l'heure de la société du numérique*, Coll. Cahiers du CRIDS, Bruxelles, Larcier, n° 45, 2019, p. 60 et s., et l'analyse des décisions de la Cour de Strasbourg à propos du concept de vie privée. À propos de la notion de « vie privée », *cf.* aussi l'arrêt *Pretty* de 2002 qui conclut : « Comme la Cour a déjà eu l'occasion de l'observer, la notion de "vie privée" est une notion large, non susceptible d'une définition exhaustive. Elle recouvre l'intégrité physique de la personne [...]. Elle peut parfois englober des aspects de l'identité physique et sociale d'un individu [...]. Des éléments tels, par exemple, [que] l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle relèvent de la sphère personnelle protégée par l'article 8 [...]. Cette disposition protège également le droit au développement personnel et le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur [...]. Bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, la Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8. »

[13] Sur ce point, lire not. l'ouvrage majeur de F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990, et l'article de J. Herveg, « Réflexions autour de la protection des données et des vulnérabilités », *in* H. Jacquemin et M. Nihoul (dir.), *Vunérabilités et droits*, *cit.*, p. 33 et s.

intrinsèque sans doute, dans bien des cas, plus provisoire, la loi a entendu protéger les patients, notamment par des obligations d'information et de plus grande transparence imposée aux praticiens de l'art de guérir. Progressivement, les législations ont élargi le concept de vulnérabilité et, au-delà de la vulnérabilité intrinsèque propre aux premières catégories reconnues par le droit ancien, le droit du XXe siècle a élargi la protection à de nouvelles catégories, cette fois caractérisées par leur vulnérabilité extrinsèque due à leur situation de dépendance économique. Cette extension s'est opérée par la multiplication de nouvelles législations particulières et la création d'institutions nouvelles : les pauvres ont ainsi bénéficié de la protection et d'allocations sociales ; les consommateurs, de lois dites de protection des consommateurs. Le droit du travail a entendu protéger les employés de la puissance patronale. Plus récemment encore, la vulnérabilité due cette fois aux risques de la considération sociale négative attachée à des catégories de population a fait l'objet d'interventions du législateur : ainsi, la prévention du racisme, de l'homophobie, des personnes étrangères est au cœur des législations modernes.

8. De la nécessité récente d'une protection de la vulnérabilité ontologique de la personne humaine – Des concepts nouveaux – Toutes ces interventions législatives se caractérisent par la désignation de catégories particulières de population bien identifiées en leur sein par des caractéristiques communes. Récemment se fait jour la réclamation poussée, y compris par nos juges, d'une législation plus transversale prenant en compte la faiblesse de chacun, sans qu'il faille nécessairement s'en référer à son appartenance à une catégorie déterminée. Deux exemples récents m'en convainquent : la réforme actuelle menée en Belgique en matière de droit des contrats consacre, en son article 5.41 du projet de Code des obligations, la notion d'abus de circonstances qu'elle définit comme suit : « déséquilibre manifeste entre les prestations par suite de l'abus par l'une des parties des circonstances liées à la position de faiblesse de l'autre partie »[14]. De son côté, la loi du 26 novembre 2011 introduit dans notre Code pénal la notion d'abus de la situation de faiblesse d'autrui (loi du 26 novembre 2011) et, au recours adressé par certains contre le caractère flou de cette législation peu respectueuse à leurs yeux du principe de « prévisibilité » de la loi pénale, la Cour constitutionnelle, le 7 novembre 2013, répond en justifiant l'extension de la manière suivante : « dans une société démocratique, la protection des personnes en situation de faiblesse constitue une condition essentielle pour protéger les droits fondamentaux

[14] *Cf.*, sur cette disposition, son origine et ses commentaires, les réflexions de H. Jacquemin, « Protection du consommateur et numérique en droits européen et belge », *in* H. Jacquemin et M. Nihoul, *Vunérabilités et droits*, *cit.*, p. 241 et s. Dans le même ouvrage, lire également F. Georges et J.-B. Hubin, « La protection de la personne en droit des obligations », p. 67 et s.

de chacun »[15]. La nécessité de prise en compte de la vulnérabilité de chacun dans notre société moderne exige cette extension.

9. Des risques liés à notre société du numérique au droit quasi constitutionnel de la protection des données – Le numérique se caractérise, aujourd'hui et chaque jour un peu plus, par diverses caractéristiques : la dimension ubiquitaire de son infrastructure, à l'heure de l'« Internet des objets » ; la capacité quasi illimitée de ses possibilités de transmission, de traitement et de diffusion ; le caractère de plus en plus intrusif de ses applications et, enfin, la puissance de ceux qui, grâce à ces systèmes, détiennent un pouvoir informationnel sans précédent. Ces caractéristiques permettent de comprendre la nécessité d'une protection non plus d'une catégorie, mais de l'ensemble des citoyens. La digitalisation de nos sociétés permet d'influer sur les capacités de développement de chaque citoyen, de mettre en cause notre dignité humaine et nos libertés et, enfin, de prévoir, d'influencer, de manipuler (*nudges*), voire de déterminer nos comportements. C'est à ces risques courus par tout homme, au-delà des seuls internautes, que les législations de protection des données à caractère personnel entendent répondre. Cette réponse s'origine dans l'élargissement du concept de vie privée, consacré en particulier par l'article 8 de la Convention des droits de l'homme du Conseil de l'Europe. Au départ, les rédacteurs de la Convention le conçoivent de manière négative comme la protection d'un espace clos dont nous pourrions écarter autrui afin de pouvoir nous retirer en nous-mêmes. L'espace clos peut s'entendre au sens physique du terme : les quatre murs de la maison ; il peut s'entendre au sens communicationnel : notre correspondance. Aujourd'hui, sans dénier cette conception négative de la notion, mais, au contraire, en la voyant comme son élargissement à une dimension plus positive, la jurisprudence range sous cette notion toutes les garanties exigées afin que nous puissions réaliser notre capacité de développement. Ainsi, dans une société de l'information de plus en plus envahissante, mais dont les infinies ressources peuvent contribuer à notre développement personnel, la notion de vie privée est désormais approchée comme unissant fondamentalement deux droits pareillement nécessaires au développement de notre personnalité, d'une part, celui traditionnel à la « séclusion », au secret[16] et, d'autre part, le droit

[15] *Cf.*, sur la disposition légale et le débat autour de cette disposition, N. Colette-Bazecqz, « La protection pénale des personnes vulnérables dans l'environnement numérique », *in* H. Jacquemin et M. Nihoul, *Vunérabilités et droits*, *cit.*, p. 135 et s.

[16] Sans doute, serait-il important de revitaliser ce droit à la « séclusion » au regard des évolutions de la technologie et de leur ubiquité interdisant dorénavant de pouvoir échapper au regard et à la sollicitation d'autrui. Nous reviendrons à cet égard sur un arrêt important de la Cour fédérale allemande de 2008 qui analyse l'ordinateur personnel (et, au-delà, tout terminal [mon mobile, mon robot…]) comme un « domicile » dont je dois pouvoir exclure autrui qui ne pourra y pénétrer qu'avec mon consentement. Il est par ailleurs intéressant de souligner, en droit du travail, la reconnaissance récente par l'article 16 de la loi du 26 mars 2018 relative à la confiance

à la maîtrise de notre « image informationnelle » ou, selon l'expression souvent retenue, le « droit à l'autodétermination informationnelle », c'est-à-dire à pouvoir contrôler : qui détient des informations à notre propos ? Lesquelles ? Pour quelle(s) utilisation(s) ?

Ainsi, les législations de protection des données se déduisent de notre droit à la vie privée. L'importance de l'enjeu du numérique pour nos développements personnels, nos libertés et notre dignité est devenue telle que les autorités européennes ont consacré celui-ci, à l'article 8 de la Charte européenne des droits de l'homme et à l'article 17 du Traité de Lisbonne, comme un droit quasi constitutionnel qui s'énonce comme suit :

> « 1. Toute personne a droit à la protection des données à caractère personnel la concernant ;
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur [la] base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données la concernant et d'en obtenir la rectification ;
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

10. Les principes essentiels du RGPD[17]. Ou comment lutter contre certains risques de vulnérabilité nés du numérique – Quelques mots sur les principes essentiels développés par le Règlement général de la protection des données[18], pris en application de cette consécration, me permettent d'éclairer le lecteur sur les moyens envisagés de prévenir les risques liés au numérique et d'assurer les conditions de développement de nos personnalités dans une société du numérique. Comme indiqué d'emblée, cette rapide description ne dispense pas d'une analyse plus détaillée des vulnérabilités nouvelles ou accrues dues au numérique, ni surtout d'un

---

dans l'économie et au renforcement de la cohésion sociale (*M.B.*, 30 mars 2018) d'un droit limité à la déconnexion, de manière à éviter le harcèlement au travail en dehors des heures de bureau (pour le regret des limites mises à la loi en ce qui concerne ce droit à la déconnexion, lire K. Reyniers, « Een recht op deconnectie, of hoe omgaan met techno-stress? », *Tijdschrift voor Sociaal Recht*, n° 1, 2019, p. 87-109).

[17] *Règlement général de protection des données* (en abrégé, « RGPD »), adopté le 27 avril 2016 et mis en vigueur le 25 mai 2018, *J.O.*, L 119 du 4 mai 2016, p. 1-88, disponible sur http://data.europa.eu/eli/reg/2016/679/oj. *Cf.* également la modification de la Convention n° 108 du Conseil de l'Europe « pour la protection des personnes à l'égard du traitement des données à caractère personnel », adoptée à la 128e session du Comité des ministres, le 18 mai 2018. Le texte et le long rapport explicatif sont accessibles sur le site du Conseil de l'Europe : www.coe.int/dataprotection.

[18] Pour plus de détails sur les différentes dispositions dudit RGPD, *cf.* C. de Terwagne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR)*, Coll. Cahiers du CRIDS, Bruxelles, Larcier, n° 44, 2018. *Cf.* également le bon résumé proposé par J. Herveg, « Réflexions autour de la protection des données, *cit*. », p. 333 et s.

retour plus critique, ces risques ayant été identifiés, sur l'adéquation des dispositions du RGPD pour limiter, voire annihiler, ces risques[19].

La protection s'entend des risques créés par les traitements de données à caractère personnel. Qu'entend-on par données à caractère personnel ? Celles qui permettent directement ou indirectement de nous identifier. Cette extension à toutes les données, y compris triviales (ma présence à tel endroit, mon parcours, ma tension à tel moment), se justifie. Sans doute, ces données, prises individuellement, sont sans grande valeur sémantique (au contraire de mon revenu ou de ma profession)[20], mais leur accumulation liée à l'intelligence artificielle de nos ordinateurs qui peuvent entrecroiser toutes ces données triviales confère ou permet d'attribuer aux résultats ainsi obtenus une valeur statistique prédictive (M. X. est, à 95 % de chances, un grand voyageur, fortuné et aimant l'art contemporain…). Il est à noter que des principes plus sévères entourent le traitement de données dites sensibles soit à la base, soit comme résultat du traitement – comme dans l'affaire *Cambridge Analytica* : les données relatives aux opinions politiques, syndicales, philosophiques ou religieuses, les données de santé, celles génétiques et biométriques. Il est clair qu'outre leur portée sémantique, ce sont les risques de discrimination liés à leurs traitements qui justifient une réglementation plus sévère.

11. Les limites au traitement – L'article 5 du RGPD énonce les principes de base applicables à tout traitement considérés *a priori* comme des balises nécessaires à la protection de nos libertés, de notre dignité et à la prévention de risques de discrimination. Le traitement doit poursuivre une finalité légitime, dans le cadre d'hypothèses, considérées comme conditions nécessaires, mais non suffisantes : le consentement, l'exécution d'un contrat existant ou à venir, les missions légales d'intérêt général et un intérêt légitime poursuivi par le responsable du traitement supérieur à ceux de la personne concernée. À ce premier principe s'ajoute celui de proportionnalité : ne traiter que les seules données nécessaires à la poursuite du but légitime et celui de sécurité. S'y ajoute un dernier principe, celui de non-suffisance, particulièrement bienvenu à l'heure des systèmes experts et d'intelligence artificielle. Il s'entend de l'interdiction de fonder une décision vis-à-vis d'un individu sur la seule base d'un traitement informatique.

12. Les droits subjectifs attribués à la personne concernée – La transparence est le premier de ces droits subjectifs, permettre à la personne concernée d'être informée des données traitées par autrui, le cas échéant,

[19] Nous renvoyons le lecteur aux nombreux ouvrages critiques relatifs au RGPD et not. à notre ouvrage, *La vie privée à l'heure de la société du numérique*, *cit.*

[20] Il y a trente ans, le coût du stockage était tel que les ordinateurs ne traitaient que des données à forte valeur sémantique. À l'heure où les capacités et le coût de nos ordinateurs permettent de traiter un nombre illimité de données, c'est le traitement des données qui leur donne sens.

des sources de telles données, des buts poursuivis par le traitement et des communications opérées ; autoriser la personne concernée, si elle le souhaite, de pouvoir accéder à de telles informations contribue à combattre l'opacité du fonctionnement des systèmes d'information qui nous entourent et à réagir. Sur ce dernier point, les législations de protection des données et le RGPD en particulier accordent à la personne concernée le droit de corriger les données, de s'opposer à la poursuite d'un traitement, voire de retirer son consentement ou de réclamer un « droit à l'oubli ». Ce dernier droit doit lui permettre, par exemple, d'exiger que des données publiées sur le Web soient « déréférencées », voire – et c'est le sens de la récente loi Peeters – que des données sur le cancer vécu par un patient ne puissent plus être traitées par des assureurs-vie, au-delà d'une période de rémission. On ajoute – et c'est une nouveauté bienvenue du RGPD – que l'action menée contre le responsable de traitement, qui n'aurait pas respecté les principes ou les droits de la personne concernée, peut être collective grâce à la reconnaissance d'une sorte de *Class Action*. L'Autorité de protection des données peut également jouer un rôle dans la défense des personnes concernées ; elle dispose de prérogatives importantes, jusqu'à la sanction administrative sévère, pour faire respecter les dispositions du RGPD ou des lois nationales qui les complètent.

13. La responsabilisation des organismes qui traitent les données – Afin d'assurer l'effectivité des principes, le RGPD enjoint au responsable du traitement de prendre ses responsabilités afin que soit assuré le respect des principes et des droits subjectifs accordés à la personne concernée. Il lui est demandé, seul ou collectivement par des codes de conduite, labels ou certifications, de garantir ce respect : c'est le principe dit d'*accountability*. Dans le cas où le traitement crée des risques plus élevés d'atteinte à la protection des données, le RGPD réclamera même de ce responsable qu'il nomme un délégué à la protection des données ou, avant de démarrer un traitement, qu'il évalue au terme d'un *Privacy Impact Assessment* les risques des traitements qu'il envisage.

Ce principe va même plus loin. Le RGPD part du principe que, si la technologie est le risque, elle peut en même temps être la solution. C'est le sens donné aux principes de *Privacy by design* ou *Privacy by default* qui exigent que, dès la conception d'un traitement, les responsables veillent à concevoir un système qui intègre dans son fonctionnement les principes de la protection des données. Ainsi, le premier principe exige, tantôt, que le responsable limite technologiquement l'accès de chacun au sein d'une entreprise aux seules données pertinentes par rapport aux fonctions et missions de la personne qui souhaite l'accès (grâce à des systèmes d'*Identity Management*) ; tantôt, qu'il « pseudonymise » automatiquement des données médicales ; tantôt, en cas de vidéosurveillance, qu'il floute les

visages ne permettant la reconnaissance des individus qu'aux seules autorités compétentes et en cas d'infractions. Le second principe veille à ce que les systèmes utilisés par les personnes concernées soient paramétrés de manière telle que ces derniers offrent la solution la plus protectrice à leurs usagers. Ainsi, le terminal sera programmé de manière à ce qu'il n'accepte pas les cookies, que le GPS efface automatiquement les trajets suivis après une certaine durée, etc. Enfin, toujours sur le plan des exigences techniques, le RGPD exige des responsables de traitement la portabilité des données collectées auprès de la personne concernée. Il s'agit de rendre la personne concernée effectivement libre de choisir son prestataire et, par exemple, de réclamer à la plate-forme de réseau social les données communiquées pour pouvoir migrer vers un autre réseau social.

III. La vulnérabilité aux risques du numérique

14. L'ambivalence fondamentale de la technologie et du numérique, en particulier – Le numérique, comme langue d'Ésope, constitue tout à la fois une chance pour notre développement personnel quand, dans le même temps, il met à mal nos vulnérabilités. Sans doute, est-ce à nos sociétés et sans doute d'abord à nous-mêmes d'utiliser de manière positive ces outils, selon le principe éthique « *Do good and do not harm* »[21]. L'objet technologique, qu'il soit mis à la disposition de l'intervention sur le vivant dans le cadre de la biologie expérimentale ou de la médecine ou, dans le cas qui nous occupe, utilisant le traitement de l'information ou sa communication, doit, dans son développement, être guidé par deux principes : celui de la « *beneficence* », c'est-à-dire l'apport bénéfique et, à l'inverse, celui de la « *non-maleficence* », c'est-à-dire le rejet d'une technologie dont la structure, le *design* porterait en lui-même des risques négatifs pour l'individu et/ou pour la société dans son ensemble[22]. Ainsi, le premier principe

[21] *Cf.*, à ce propos, mais en matière de biotechnologies et biomédecine, les travaux de T.L. Beauchamps et J.F. Childress, *Principles of Biomedical Ethics*, New York, Oxford University Press, 2001. « *The principle of "*Non-Maleficence*" requires an intention to avoid needless harm or injury that can arise through acts of commission or omission. In common language, it can be considered "negligence" if you impose a careless or unreasonable risk of harm upon another. The "*Beneficence*" principle refers to actions that promote the well-being of others.* » Sur l'application de ce principe dans le cadre de notre société numérique, lire notre ouvrage, *Éthique et droits de l'homme dans notre société du numérique*, Coll. Mémoires, Académie royale de Belgique, 2020.

[22] Quatre points nous paraissent à relever. Le premier est le rejet de toute technologie qui porte des risques d'impacts négatifs. C'est la condamnation des technologies dites « malfaisantes ». Le deuxième point est relayé par des textes juridiques et de nombreux documents récents : il réclame que les infrastructures, produits et services du numérique soient élaborés selon le principe de l'*Ethical value by design*. Le troisième point forme le contrepoint du premier. L'éthique et le droit se doivent de supporter l'innovation technologique, dans la mesure où celle-ci apporte un bien pour l'humain. Cette vue *a priori* positive de l'innovation réclame certes pour déterminer le bénéfice apporté à l'humanité la prise en compte de la multiplicité des intérêts entre prestataires,

conduit à des choix technologiques qui chercheront à maximiser l'apport bénéfique de ces technologies sur la population. À l'inverse, le second principe appelle au rejet de toute technologie dont le fonctionnement ou le design pourraient avoir un impact négatif sur la sécurité ou le bien-être des individus ou des collectivités.

15. De nombreuses explications sont avancées pour comprendre ce recours de plus en plus massif aux technologies les plus avancées du numérique – Sans prétendre à l'exhaustivité, on épingle chez l'utilisateur des services et des produits du numérique :

- la perte des repères traditionnels qui sécurisaient notre existence et nous faisaient exister. L'*extimacy*, en d'autres termes, la nécessité d'apparaître, technologie aidante, et de se raconter à longueur de blogs et de réseaux sociaux s'explique certes par cette volonté de retrouver une « ex-istence » en même temps qu'elle est une réponse à un besoin compulsif de communication de et avec l'autre dans un marché où chacun gagne et que l'on peut résumer ainsi : « Je te parle et me raconte si tu me parles et te racontes », besoin auquel l'individu résiste d'autant moins que ce service lui est offert gratuitement ;
- la lutte contre les sentiments d'insécurité et d'angoisse : être connecté, c'est pouvoir à tout moment se situer et espérer maîtriser ce qui fait notre angoisse : le succès des tests prédictifs *on-line*, l'utilisation des produits *quantified self* comme le bracelet permettant à chaque instant de connaître son pouls, sa tension, son état de stress, etc., ou du GPS, ange gardien de notre conduite, s'expliquent de la sorte ;
- le confort engendré par toute une série de technologies qui nous facilitent la vie (voy. les outils de domotique qui permettent la gestion à distance de l'immeuble), nos choix (la présélection opérée par nos moteurs de recherche ou nos plates-formes musicales), et qui répondent à nos injonctions (les robots, les enceintes connectées) ;
- le sentiment de maîtrise d'un environnement désormais fixé aux limites de la Terre, qu'il s'agisse de la culture, de l'information, de la consommation, etc. Nous sommes ubiquitaires, sentiment qui contraste avec celui d'une perte de la maîtrise du fonctionnement de l'outil technologique qui permet cette maîtrise de l'environnement.

---

autorités publiques, citoyens, concurrents, etc., qui, parfois, peuvent être contradictoires. Il importe de permettre l'expression de chaque acteur et de rechercher l'équilibre des différents intérêts exprimés à la lumière des valeurs éthiques et de la prudence qu'imposent les jugements, tant éthiques que juridiques. Enfin, le quatrième, au nom de ce principe de prudence et pour réaliser le vœu d'une construction éthique de la technologie, exige la mise en place de lieux d'évaluation, tant au sein des organisations privées que publiques. Sur ce point, le parallèle avec le droit du développement est inspirant.

Du côté des prestataires, le recours est aisément justifié par la diminution des coûts administratifs et salariaux, la meilleure performance par une meilleure connaissance du « client », la sécurité accrue, une meilleure gestion administrative des opérations.

16. Le numérique et l'accroissement de nos « capacités » – À force d'insister sur les menaces induites par les applications modernes du numérique, on en oublierait presque de souligner ce qui pourtant ne peut être contesté : l'utilisation des technologies de l'information fournit des ressources inédites à l'individu pour se développer et s'ouvrir à la société. Il est certain que l'outil, en particulier Internet, favorise au plus haut point la possibilité pour chacun de découvrir et discuter la pensée d'autrui, de collecter l'information nécessaire à son jugement et de participer à la formation de l'opinion publique. Au-delà, à l'ubiquité du numérique répond l'ubiquité de l'homme. On souligne que l'utilisation de l'outil lui permet d'échapper aux contraintes de lieu et de temps et, plus encore, aux entraves culturelles et sociales que peut lui imposer son milieu. Ainsi, le porteur de handicap se réjouira lorsqu'il dialogue dans les réseaux sociaux de ne pas être aperçu par autrui à travers son infirmité. Le pauvre louera la possibilité qui lui est offerte gratuitement de bénéficier d'une information riche à portée d'un clic. Enfin, l'internaute peut, sous couvert d'un pseudonyme, expérimenter plusieurs manières d'être lui-même au monde, d'y jouer différents rôles et d'exprimer diverses facettes de sa personnalité. L'Internet des objets lui permet d'agir à distance, de découvrir son environnement, voire de le transformer. Les applications des imprimantes 3D promettent la création d'objets, y compris de remplacer tel ou tel membre humain. Les robots nous aideront dans des tâches quotidiennes et nous en déchargeront. On ajoute que les nombreuses applications des systèmes d'intelligence artificielle en matière de santé, d'éducation, de définition de stratégies augurent de services meilleurs et d'une recherche facilitée.

Le numérique et en particulier les services offerts par les plates-formes de communication et d'information offrent des applications ressenties comme une nécessité première pour exister dans notre société dite de l'information et de la communication, en particulier pour les personnes âgées qui y trouvent l'opportunité de maintenir un contact facile avec les leurs ou leurs proches. Au-delà, elles y trouvent un remède à leur solitude et leurs angoisses, par exemple, d'affronter les incertitudes de la ville. La domotique autorise, pour une personne dont les déplacements peuvent être difficiles, la maîtrise de son environnement physique. En matière de santé, les outils de contrôle et de prédiction que le numérique offre grâce aux systèmes de *quantified self* peuvent calmer ses angoisses et permettre le maintien de la personne âgée dans son domicile. Mieux, l'utilisation d'implants corporels accessibles, voire activables à distance, permet dès

maintenant de lutter contre le stress, les déficiences de mémoire et d'agir, par exemple, en cas d'insuffisance d'insuline. On ajoute le rôle décisif joué par l'utilisation des nombreux services et applications du numérique pour asseoir le développement de nos personnalités, notre ouverture à la diversité du monde, la possibilité d'une prise de parole citoyenne collective ou individuelle, et ce, sans que cette parole soit accueillie par le destinataire avec les préjugés liés à l'âge de son émetteur.

Enfin, on souligne la promesse de l'homme mieux soigné, voire augmenté, que nous promettent les implants corporels et les progrès des NBIC, en particulier les développements, certes contestables, sur le plan de l'éthique de la manipulation génétique[23].

17. Le numérique comme renforcement de nos vulnérabilités ontologiques – À cette vision très positive s'opposent des perspectives plus pessimistes : celle de l'internaute faisant face au *Big Brother*[24] du roman d'Orwell, puissance sans visage qui amasse l'information et peut tout décider face à un internaute de plus en plus transparent ; celle, inspirée

[23] La technologie des NBIC, c'est-à-dire l'utilisation combinée des sciences nanotechnologique, biotechnologique, informatique et neurocognitive, ouvre la voie à des manipulations sur le génome humain. « Si la matière est de l'information (codage – écrit le philosophe et homme de sciences Th. Magnin [*Penser l'humain au temps de l'homme augmenté*, Paris, Albin Michel, 2017, p. 34-35]), le traitement de celle-ci permet de copier le vivant naturel, mais aussi de le reprogrammer. Désormais, on "façonne le monde atome par atome à cette échelle pour laquelle il n'y a pas de différence entre la matière inerte et la matière vivante"… Elle permet de modifier le comportement des vivants naturels, mais aussi de penser à d'autres formes de vivants que ce[lle]s que la nature nous révèle. » Récemment, des chercheurs ont mis au point, sous le nom de CRISP-Cas-9 (*Clustered Regularly Interspaced Short Palindromic Repeats*, c'est-à-dire « courtes répétitions palindromiques groupées et régulièrement espacées »), une méthode d'édition de gènes qui permet de couper des gènes dits « fautifs » et de les remplacer par d'autres gènes. On ajoute que cette méthode a connu une première application à l'être humain. Le mercredi 28 novembre 2018, le scientifique chinois He Jiankiu a affirmé avoir recouru à cette technologie pour modifier les gènes des embryons de deux jumelles qui présentaient du fait de leur hérédité un fort risque de sida. L'annonce de l'opération a provoqué un tollé, tant pour des raisons de doute scientifique que pour des arguments éthiques. Derrière de telles manipulations, il ne s'agira plus demain uniquement de réparer l'individu, mais, au-delà de le transformer, notamment dans un souci d'amélioration de ses performances physiques et/ou mentales, de permettre l'éclosion d'un surhomme.

[24] L'opposition entre la vision orwellienne et celle kafkaïenne est remarquablement décrite par l'ouvrage de D. J. Solove, *The Digital Person. Technology and Privacy in the Information Age*, New York, New York University Press, 2004, particulièrement p. 7 et s. : « *The dominant metaphor for modern invasions of Privacy is Big Brother… Big Brother oppresses its citizens, purges, dissenters, and spies everyone in their homes. The result is a cold, drab grey world with hardly any space for love, joy, original thinking, spontaneity or creativity. It is a society under total control. Although the metaphor has proven quite useful for a number of privacy problems, it only partially captures the problems of digital dossiers. Big Brother envisions a centralized authoritarian power that aims for absolute control, but the digital dossiers constructed by business aren't controlled by a central power, and their goal is not to oppress us but to get us to buy new products and services.* »

du *Procès* de Kafka[25], d'un sujet affrontant une machine dont le fonctionnement totalement opaque et sans logique l'empêche d'anticiper les conséquences des actes qu'il pose. Ainsi, on évoque les dangers nés :

- du déséquilibre des pouvoirs respectifs[26] des responsables des traitements, d'une part, et de la personne concernée, d'autre part. Ce déséquilibre des pouvoirs informationnels peut conduire à toutes les discriminations, mais également à toutes les manipulations, la transparence des individus se heurtant en outre à la non-transparence des responsables de traitement ;
- de l'ubiquité des systèmes d'information qui permettent de suivre, voire d'épier, chacun dans ses déplacements, ses habitudes, ses goûts, voire ses émotions[27] ;
- de la « décontextualisation »[28] : les données qui circulent sur la Toile ont été « émises » par les personnes concernées pour une finalité précise ou dans un contexte particulier ou ont été collectées à un temps donné. Les croisements de données de toutes sortes au sein des *Big Data* et la possibilité d'interroger les moteurs de recherche à partir de n'importe quel mot-clé engendrent la crainte que nous soyons jugés « hors contexte ». En particulier, la mémoire de l'ordinateur sans commune mesure avec celle de l'humain risque de stigmatiser à vie l'individu à raison d'un comportement passé ;
- de l'opacité du fonctionnement tant des terminaux (notamment, les cookies, les RFID présents dans l'Internet des objets) que des infrastructures (voy. les « agents distribués » localisés tout au long de systèmes d'information, comme ceux dits d'intelligence ambiante). Pire, la « logique », à l'œuvre dans les systèmes d'intelligence artificielle dits de *deep learning*, devient opaque, même à leurs concepteurs, et ce, au hasard des corrélations que les algorithmes découvrent

[25] *Cf.* D.J. Solove, *The Digital Person*, *cit.*, p. 9 : « *The trial captures an individual's sense of helplessness, frustration and vulnerability when a large bureaucratic organization has control over a vast dossier of details about one's life… The problem is not simply a loss of control over personal information nor is there a diabolical motive or plan for domination as with Big Brother… The problem is a bureaucratic process that is uncontrolled.* »

[26] *Cf.* D.J. Solove, « Privacy and power: Computer data bases and metaphors for information privacy », *Stanford Law Review*, n° 53/6, 2001, p. 1393 et s.

[27] Grâce à ce qu'il est convenu d'appeler l'*Affective Computing*.

[28] L'importance du respect des « contextes », c'est-à-dire des zones de confiance dans lesquelles une donnée à caractère personnel est transmise par la personne concernée, a été remarquablement mise en évidence par H. Nissenbaum, « Privacy as contextual integrity », *George Washington Law Rev.*, n° 79, 2004, p. 150 et s. L'auteure affirme : « *The freedom from scrutiny and zones of "relative insularity" are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide venues in which people are free to experiment, act and decide without giving account to others or being fearful of retribution.* »

dans les réservoirs de données qui leur sont donnés en pâture. Cette opacité entraîne la crainte de traitements non sollicités, non voulus et la tentation, pour celui qui, comme le prisonnier de Kafka dans le roman *The Trial*, ignore le quoi, le pourquoi et le comment des traitements qui l'entourent, de se conformer à un comportement qui est celui qu'il pense être attendu par ces nouveaux « lieux » invisibles de surveillance. Ce « conformisme anticipatif » entraîne le risque, selon une décision récente du tribunal constitutionnel allemand, d'une normalisation des comportements, peu favorable, selon le tribunal, à une démocratie qui exige que chacun s'exprime et agisse de manière originale et personnelle[29] ;

- du réductionnisme[30] : de plus en plus, les données collectées à propos des événements, même les plus insignifiants de notre vie, se multiplient et les systèmes d'information nous analysent à travers ces données qui réduisent, à des données factuelles et à leurs combinaisons pas

[29] Les dangers de l'opacité de nos sociétés de l'information comme menace pour nos sociétés de l'information, où les citoyens ne peuvent connaître de manière exacte le fonctionnement des systèmes d'information, les données collectées, les lieux de traitement, les finalités poursuivies par ceux qui traitent les données, sont mis en évidence dès 1983 par le fameux jugement constitutionnel dans l'affaire du recensement (Bundesverfassungsgerichtshof, 15 décembre 1983, *EuGRZ,* 1983, p. 171 et s.). La tentation des citoyens est alors d'adopter le comportement, qu'ils croient attendu par la société et de ne point oser s'exprimer librement, ce qui est dommageable pour nos démocraties : « *The possibility of inspection and of gaining influence have increased to a degree hitherto unknown, and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may be possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanent as information, or is applied or passed, he will try not to attract attention by such behaviour. If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would have also impact the common good ("Gemeinwohl"), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate.* »

[30] Ce danger de « réductionnisme » est déjà dénoncé en 1966 par Karst (« "The files": Legal control over the accuracy and accessibility of stored personal data », *Law and Contemporary Problems*, n° 31, 1966, p. 361) qui souligne le danger de « *a centralized, standardized data processing* » qui ne retient comme signifiants, à propos du sujet de la recherche, que les faits repris et traités par l'ordinateur. Dans le même sens, l'ouvrage de J. Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, New York, Random House Trade, 2000, cité par D.J. Solove, « Privacy and power, *cit*. », p. 424 : « *Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge.* »

toujours maîtrisées, nos vies humaines, de même que nos personnalités aux résultats tirés du croisement de telles données. La tentation est d'autant plus forte que la donnée ne ment pas, qu'elle représente, dès lors, une vérité factuelle plus crédible que nos énoncés verbaux. Ainsi, nous voilà aperçus à travers des « profils » créés grâce à des technologies de plus en plus puissantes pour la poursuite de finalités définies par ceux qui utilisent ces données, connus ou inconnus. Ces profils et les décisions prises en fonction de ces profils peuvent être générés directement par le dispositif technologique[31]. Dans les systèmes d'intelligence ambiante où l'homme est mis en réseau avec un ensemble d'objets qui l'entourent, il devient, au sein de ce réseau, un objet communicant parmi d'autres, dont certains vont entraîner telle ou telle réaction ;

- de l'abolition de la distinction entre sphère publique et sphère privée[32]. L'homme perdu dans la foule peut être suivi, tracé. À l'inverse, même chez lui, enfermé à double tour, l'homme se voit à travers le GSM qu'il a en poche, les RFID qu'il peut porter, à travers son utilisation de la TV interactive, de son ordinateur relié à Internet, espionné, poursuivi, et ses secrets d'alcôve, percés. La protection du domicile physique, lieu inviolable, apparaissait traditionnellement, et aux yeux du droit, comme quelque chose de fondamental pour la construction de la personnalité de l'individu. Cette notion-là se trouve, elle aussi, bouleversée à l'heure actuelle par les développements technologiques. Cet effacement des frontières permet à celui qui détient la puissance

[31] C'est précisément la raison de l'article 15 de la directive européenne 95/46 en matière de protection des données qui prévoit des dispositions en matière de systèmes automatisés de décision. La préoccupation majeure a trait à l'automatisation croissante des processus décisionnels à l'égard des individus. Comme le révèlent les travaux préparatoires, le législateur européen en est venu à s'inquiéter d'une telle automatisation, tant elle diminue le rôle joué par les personnes dans les processus de décision : « *This provision is designed to protect interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institution deprives the individual the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his "data shadow"*. » Une autre préoccupation concerne le fait que l'automatisation galopante des processus de décision engendre une acceptation quasi automatique de la validité et de la pertinence de ces décisions et, corrélativement, un désinvestissement et une déresponsabilisation de décideurs « humains ». À cet égard, la Commission relève que « *the results produced by the machine, using more and more sophisticated software, and even expert system, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities* ».

[32] Sur cette distinction classique et sa radicale remise en cause, J.A. Fichbaum, « Towards an autonomy-based theory of constitutional Privacy. Beyond the ideology of familial privacy », *Harvard Civil Rights – Civil Liberties Review*, n° 14, 1979, p. 361-384. Sur ce point, lire également D.J. Solove, « Conceptualizing privacy », *California Law Review*, n° 90, 2002, spéc. p. 1138 et 1139.

technologique de pénétrer les secrets de la personne concernée et, dès lors, de la manipuler.

Cette puissance de manipulation existe d'autant plus que l'intelligence artificielle permet ce que ma collègue A. Rouvroy appelle la « gouvernementalité algorithmique »[33]. Les profils créés constituent des outils non seulement d'analyse du passé, mais la « vérité » qu'ils contiennent, certes, purement statistique, utilise ces profils comme un instrument de prévision, parfois sinon souvent biaisée[34], de nos comportements futurs. Comme le dit le patron d'Amazon, « avant même que vous passiez commande, nous avons déjà préparé votre colis ». Et le patron de Google renchérit : « *It will become very difficult for people to see or consume something that has not in some sense been tailored for them.* » Les données génétiques permettent à leurs analystes de dessiner votre évolution de santé et celle de vos enfants. À travers les *nudge*s[35], les systèmes vous proposent, à vous conducteur, la meilleure route à suivre ; à vous chercheur, la façon dont votre indice H pourra évoluer ; à vous responsable d'une commune, les zones d'insécurité ou d'abandon où vous devez intervenir ; à vous ministre de l'Éducation, les critères selon lesquels, *a priori*, les enfants ont des chances de réussir leur parcours scolaire ; à vous juge, les risques de récidive d'une personne auteure d'une infraction ou la décision la plus conforme au droit ou plutôt ce qui a déjà été jugé comme conforme au droit ; à vous lecteur, les ouvrages qui doivent correspondre à vos goûts. Bref, les systèmes d'*IA* fixent insidieusement la « norme » de vos comportements non en vous les imposant, mais, de manière plus subtile, en vous les proposant comme une évidence qui vous rend la vie facile : « il suffit de cliquer ». Ces systèmes opèrent à la manière de ce que d'aucuns qualifient de « capitalisme libertarien ». La norme n'est ni obligatoire ni transparente, elle est proposée

[33] Sur la notion de « gouvernementalité algorithmique », lire A. Rouvroy et T. Berns, « Gouvernementalité algorithmique et perspective d'émancipation : le disparate comme condition d'individuation par la relation », *Réseaux*, n° 177/1, 2013, p. 163-196.

[34] Sur la question de biais, dus souvent, mais non uniquement, à la subjectivité des concepteurs de systèmes d'*IA*, voir l'article « Biais » dans Wikipédia (consulté le 6 janvier 2022) : « Un biais algorithmique se produit lorsque les données utilisées pour entraîner un algorithme d'apprentissage automatique reflètent les valeurs implicites des humains impliqués dans la collecte, la sélection ou l'utilisation de ces données. Les biais algorithmiques ont été identifiés et critiqués pour leur impact sur les résultats des moteurs de recherche, les services de réseautage social, le respect de la vie privée et le profilage racial. Dans les résultats de recherche, ce biais peut créer des résultats reflétant des biais racistes, sexistes ou d'autres biais sociaux ou culturel[s], malgré la neutralité présumée des données. »

[35] La « théorie du *Nudge* (ou théorie du "paternalisme libéral") est un concept des sciences du comportement, de la théorie politique et d'économie issu des pratiques de design industriel, qui fait valoir que des suggestions indirectes peuvent, sans forcer, influencer les motivations, les incitations et la prise de décision des groupes et des individus, au moins de manière aussi efficace, sinon plus efficacement que l'instruction directe, la législation ou l'exécution. » (Wikipédia, « Nudge », consulté le 30 août 2020).

comme un conseil et induite du fonctionnement des systèmes que vous « consentez » à utiliser, et aucune sanction n'est liée à votre transgression de la norme proposée comme une facilité.

Tous ces dangers se trouvent accrus par le développement des applications d'intelligence artificielle caractérisées notamment par leur opacité, leur réductionnisme, leur caractère prédictif et leur « non-contestabilité »[36].

18. On le pressent, le numérique soulève des questions éthiques essentielles, en particulier lorsque ses applications concernent des personnes vulnérables – Il met en cause la dignité[37] de ces personnes soumises à une surveillance continue des lieux occupés et des propos et conversations parfois les plus intimes, personnes considérées comme objets et non plus sujets, victimes de manipulations par des opérateurs qui considèrent ces personnes comme moyen, et non plus comme un but en soi, selon la définition kantienne de la dignité ou, à tout le moins, comme êtres dont la parole n'est plus prise en considération face à l'« infaillibilité » des systèmes de décision automatisée. L'autonomie des personnes âgées est mise en cause par les décisions automatisées tant prises vis-à-vis d'elles que décidées à leur place. Enfin, les enjeux de justice sociale sont soulevés en ce qui concerne tant l'exclusion d'accès que des profilages discriminants à propos de personnes en raison précisément de leur vulnérabilité

IV. Le droit en réponse à nos vulnérabilités face au numérique

19. Des différentes manières dont le numérique atteint nos vulnérabilités – La réflexion introduite dans les derniers paragraphes mettait en évidence les causes de notre fragilité ontologique face au numérique. Mon propos dans ce quatrième point est de structurer les différents risques que nos vulnérabilités, tant celles intrinsèques qu'extrinsèques, mais également ontologiques, courent du fait d'un numérique ubiquitaire, puissant et de plus en plus structurant nos actions, nos vies, nos relations et notre société. Le premier risque est certes l'exclusion, le risque d'une société à

[36] Nous ne pouvons développer ce point et renvoyons le lecteur aux nombreuses études sur ce sujet, en particulier notre ouvrage, *Le RGPD face à l'intelligence artificielle*, Coll. Cahiers du CRIDS, Bruxelles, Larcier, n° 49, 2020.

[37] On évoque ainsi le cas des stagiaires indélicates qui avaient posté sur le réseau social *Snapchat* des vidéos de résidents, comportement jugé comme une atteinte à la dignité de ces personnes âgées. Le principe du droit à l'image est de donner son accord sur la diffusion de [son] image. Mais le développement d'une jurisprudence plus spécifique et le défenseur des droits, dans une décision du 4 avril 2013, ont rappelé que l'utilisation de l'image du résident peut constituer un abus, si ledit résident n'est pas considéré comme un sujet de droit, mais comme un « simple objet », même s'il a donné son accord. La décision du défenseur des droits insiste sur le fait que l'image des résidents doit être utilisée à bon escient et « pas comme un élément de décor », par exemple, sur un site internet.

deux vitesses dont seraient exclues certaines catégories de population. Le deuxième risque est lié aux infractions liées aux potentialités d'agression que recèle un réseau qui pénètre au cœur de nos foyers pour surprendre notre confiance légitime ou dont les contenus véhiculés peuvent choquer nos personnes, en particulier les enfants. Le troisième risque a été décrit ci-dessus, il touche à nos personnalités en tant que telles, tantôt stigmatisées, tantôt manipulées, tantôt normalisées. La discrimination que permet la connaissance d'autrui est un quatrième risque. Enfin, le numérique peut modifier notre identité la plus profonde, la modifier, l'augmenter. La réponse du droit à ces cinq risques sera présentée succinctement, et ce, à travers différentes branches du droit.

A. Numérique et exclusion

20. L'accès universel – La ressource, que constitue l'espace universel de communication d'Internet, est, selon les termes mêmes du *Sommet mondial de la société de l'information* (SMSI) convoqué en 2003 par les Nations unies : « une ressource publique internationale »[38]. L'affirmation se heurte à la constatation de ce qu'il est convenu d'appeler la fracture numérique[39] ou, pour être plus juste, le fossé numérique, et ce, nonobs-

[38] Sommet mondial sur la société de l'information, *Déclaration de principes, Construire la société de l'information : un défi mondial pour le nouveau millénaire*, Genève, 2003, WSIS-03/GENEVA/DOC/4-F, Principe n° 48 : « L'Internet est devenu une ressource publique mondiale et sa gouvernance devrait être un point essentiel de l'ordre du jour de la société de l'information. La gestion internationale de l'Internet devrait s'exercer de façon multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales. Elle devrait assurer une répartition équitable des ressources, faciliter l'accès de tous et garantir le fonctionnement stable et sécurisé de l'Internet, dans le respect du multilinguisme. »

[39] « Avec la Déclaration universelle de l'UNESCO sur la diversité culturelle du 2 novembre 2001, les questions actuelles relatives à la diversité culturelle ou à "l'héritage commun de l'humanité" deviennent des priorités. Cette déclaration fait de la diversité culturelle un impératif éthique concret, inséparable du respect de la dignité humaine. Il est à regretter que[,] malgré l'importance et l'universalité de ce régime de droits reconnus par la communauté internationale, les technologies numériques qui catalysent aujourd'hui l'essentiel des flux d'information aient renforcé des inégalités préexistantes, en particulier, la prédominance de l'écriture en caractères latins. Des multiples fractures numériques issues de ce biais inhérent à l'architecture initiale de l'Internet découlent de ces incidences et cela sur trois plans : (i) la difficulté d'utiliser nombre de services en raison du manque de reconnaissance des codes de caractères linguistiques ; (ii) l'impossibilité d'adapter véritablement ces technologies à un contexte local ; (iii) la difficulté d'utilisation de ces technologies par des personnes ayant un faible niveau d'instruction. À l'évidence[,] le cyberespace est toujours dominé par les cultures qui l'ont façonné initialement, conduisant à la prégnance des instruments linguistiques occidentaux/latins et aux schèmes culturels dominants qui y sont associés. Il serait bon de faire retour à la maison commune d'un monde qui n'est pas seulement celui de l'objet technique[,] mais celui des hommes. » *Cf.* R. Delmas, « Internet et la diversité, le souci du passage à l'éthique », *Revue française des sciences de l'information et de la communication*, n° 2, 2013, mis en ligne le 1er janvier 2013, consulté le 18 novembre 2018. URL : http://journals.openedition.org/rfsic/278 ; DOI : 10.4000/rfsic.278.

tant les appels des organisations internationales. Ainsi, parmi les Objectifs de développement durable adoptés par les Nations unies en 2015 dans le prolongement des Objectifs du millénaire pour le développement (OMD)[40], on souligne l'objectif n° 9 : « bâtir une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation ». Cet objectif donne comme mission aux États membres de l'ONU d'« accroître nettement l'accès aux technologies de l'information et des communications et [de] faire en sorte que tous les habitants des pays les moins avancés aient accès à Internet à un coût abordable d'ici à 2020 ». De la même manière, sur le plan européen, une Résolution du Parlement de 2008[41] condamnait les dispositions de la loi française Hadopi qui autorisait la coupure de l'accès à l'Internet des internautes indélicats ayant violé les droits de propriété intellectuelle. Leur motivation est célèbre, le Parlement comparait le besoin de la connexion au réseau à l'heure actuelle, à celui éprouvé vis-à-vis du pain par la population au XIX^e^ siècle. L'affirmation répétée par nombre de textes internationaux[42] trouve écho même en Belgique : des études récentes montrent que 14 % de la population belge restent privés de connexion à l'Internet et que les chiffres sont bien plus élevés quand on envisage les catégories de personnes plus vulnérables[43]. La réponse du droit consiste en la proclamation de ce qu'il est convenu d'appeler un « service universel »[44] qui garantisse l'accès de tous à l'infrastructure ou plutôt, selon l'expression de la directive européenne[45],

[40] AGONU, Résolution 70/1 adoptée le 25 septembre 2015, « Transformer notre monde : le Programme de développement durable à l'horizon 2030 », A/RES/70/1, objectif 9, alinéa c. Le document est disponible en format PDF à l'URL suivante : https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E).

[41] Le 10 avril 2008, le Parlement européen adopte une résolution qui engage les États membres à « éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telles que l'interruption de l'accès à l'Internet ».

[42] Parmi ces organisations internationales, on cite la Résolution du Conseil des droits de l'homme de l'ONU sur la promotion, la protection et l'exercice des droits de l'homme sur l'Internet du 26 juin 2014 (A/HRC/26/L.24, p. 3) et la recommandation du Conseil des ministres du Conseil de l'Europe sur un Guide des droits de l'homme sur Internet (16 avril 2014, CM/Rec, 2014, p. 4) qui affirme la nécessité de « garantir la liberté d'accès à internet à un coût abordable pour toutes les catégories de population, sans discrimination ». Pour d'autres références, lire P. Brotcorne, « L'effectivité des libertés fondamentales des personnes vulnérables », *in* H. Jacquemin et M. Nihoul (dir.), *Vulnérabilités et droits*, *cit.*, p. 38.

[43] Le chiffre monte à 27 % pour les femmes seules et 33 % pour les RMI ; 11 % de la population (29 % pour les RMI et 34 % pour les personnes de plus de 64 ans) avouent ne s'être jamais connectés. Il est à noter que l'obstacle financier explique souvent cette absence de connexion (P. Brotcorne, « L'effectivité des libertés fondamentales », *cit*., p. 40 et les références reprises).

[44] « Universel », et non « public », dans la mesure où le service est offert non par une entreprise ou administration publique, mais en concurrence par des entreprises sur un marché libéralisé.

[45] Directive 2002/22/CE du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services. Lors de la transposition de la directive en droit belge par la loi belge du 13 juin 2005 (*M.B*., 20 juin 2005, art. 8, 5°), le législateur a confié à

la fourniture « d'un ensemble minimal de services déterminés à tous les utilisateurs finaux à un prix abordable ». Par ailleurs, l'accessibilité des personnes relevant de catégories de personnes vulnérables intrinsèquement est réclamée par la Convention de l'Organisation des Nations unies (ONU) relative aux droits des personnes handicapées. L'article 9 demande aux États parties la prise de mesures appropriées pour « promouvoir l'accès des personnes handicapées aux nouveaux systèmes et technologies de l'information et de la communication, y compris l'internet »[46].

21. L'extension de la notion de service universel – À cette difficulté d'accès de base à l'Internet s'ajoutent, depuis, d'autres considérations sur l'accessibilité, cette fois à des sites web ou à des applications mobiles. Là encore, des initiatives sont prises pour permettre à chacun de bénéficier de l'espace public mondial. L'organisation mondiale de normalisation du Web, le W3C, dont les travaux sont largement reconnus par les acteurs de l'Internet, voire par les gouvernements, mais sans personnalité juridique, a établi un référentiel pour l'accessibilité des sites web, qu'il définit comme la possibilité pour toute personne, quels que soient ses besoins particuliers sur le plan physique, physiologique ou technique, de percevoir, comprendre et interagir avec le contenu des sites web, ce qui suppose l'ergonomie, la portabilité et le référencement des sites en ligne[47]. Cette initiative trouve écho dans la directive européenne relative à l'accessibilité des sites web et des applications mobiles des organismes du secteur public,

l'IBPT le soin de prendre des mesures permettant de rencontrer les besoins de « groupes sociaux particuliers, notamment les utilisateurs finaux handicapés, âgés ou présentant des besoins sociaux spécifiques ». Cette directive est sur le point d'être remplacée par une directive établissant le Code des communications électroniques européen (26 octobre 2016, *COM*[2016] 590 final, adoptée par les États membres le 29 juin 2018). « La proposition (art. 37) vise à moderniser le régime de service universel en supprimant de son champ d'application l'inclusion obligatoire, à l'échelle de l'UE, de services traditionnels (téléphones publics payants, annuaires complets et services de renseignements téléphoniques), et en mettant l'accent sur le haut débit en tant que service universel de base, qui serait défini par référence à une liste de base dynamique de services en ligne utilisables grâce à une connexion haut débit. L'intervention des États membres devrait porter plus particulièrement sur le caractère abordable de la connectivité disponible plutôt que sur le déploiement de réseaux, pour lequel de meilleurs outils existent. Le caractère abordable du service universel doit être assuré au moins en position déterminée, mais les États membres jouiront d'une certaine marge de manœuvre pour étendre les mesures d'accessibilité financière aux services mobiles également, en faveur des utilisateurs les plus vulnérables. L'article 79 impose aux États membres une obligation de garantir un accès abordable à tous les utilisateurs finaux aux services d'accès fonctionnel à l'internet haut débit et de communications vocales au moins en position déterminée. Afin de garantir ce caractère abordable, l'article 80 autorise les États membres à imposer aux entreprises d'avoir des formules tarifaires spéciales pour les utilisateurs finaux recensés comme ayant de faibles revenus ou des besoins sociaux particuliers et/ou de fournir à ces utilisateurs finaux un soutien direct, et instaure un droit d'acquisition pour les consommateurs bénéficiant de tarifs universels spéciaux. »

[46] Art. 9 (2), al. g), de la Convention relative aux droits des personnes handicapées du 13 décembre 2006.

[47] Le dernier référentiel du WCAG (*Web Content Accessibility Guidelines*) date d'avril 2018.

adoptée en 2016[48]. De plus, afin d'assurer le droit à la liberté d'expression et d'opinion, les États parties doivent, en application de l'article 21 de la Convention des Nations unies relative au droit des personnes handicapées, déjà citée, demander « instamment aux organismes privés qui mettent des services à la disposition du public, y compris par le biais de l'internet, de fournir des informations et des services sous des formes accessibles aux personnes handicapées » et encourager « les médias, y compris ceux qui communiquent leurs informations par l'internet, à rendre leurs services accessibles aux personnes handicapées »[49].

Progressivement se dégage, de nombreux textes européens, l'idée que les plates-formes dites infomédiaires (*search engines*) ou de communication (réseaux sociaux), qui opèrent comme des *Gatekeepers* dans la mesure où, en situation de position dominante sur le marché, elles offrent un service essentiel d'utilisation de l'Internet, voient leurs services régulés par l'autorité publique afin d'offrir une qualité de service sur le plan de la sécurité[50], sur leurs critères de *ranking* et leur transparence[51], sur les modes de contrôle de l'atteinte à la propriété intellectuelle[52] ou de qualité de l'information véhiculée (cas des *Fake News*)[53], demain sur l'obligation de fournir

[48] Directive 2016/2102/UE du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public, L. 327/1.

[49] Art. 21, al. c) et d), de la Convention précitée.

[50] Directive dite NIS sur la sécurité du réseau et des systèmes d'information (« Directive EU 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union », *J.O.*, L 194 du 19 juillet 2016, p. 1-30). Cette directive impose aux opérateurs de services essentiels et aux fournisseurs de services numériques des obligations telles que l'obligation d'informer les autorités publiques des incidents de sécurité.

[51] Proposition de règlement sur le traitement loyal des utilisateurs professionnels des plates-formes en ligne en cours de discussion au Parlement européen. À noter la déclaration du vice-président de la Commission chargé du marché unique numérique, Andrus Ansip : « Des millions de commerçants dans l'UE, de petite taille pour la plupart, dépendent désormais des plateformes en ligne pour atteindre leurs clients dans l'ensemble du marché unique numérique. Ces nouvelles places de marché en ligne sont porteuses de croissance et d'innovation dans l'UE, mais nous avons besoin d'un ensemble de règles claires et fondamentales pour garantir un environnement économique durable et prévisible. La proposition présentée ce jour accroît la transparence de l'économie en ligne, elle offre aux entreprises la prévisibilité dont elles ont besoin et elle profitera en définitive aux consommateurs européens. » Les obligations sont nombreuses : transparence des systèmes de *ranking*, des conditions objectives de suspension ou résiliation des services offerts, obligation d'information et de motivation en cas de différenciation de traitement, offre d'un service indépendant de médiation en cas de litige, etc.

[52] Que l'autorité publique déléguerait à ces plates-formes, ainsi dans le cas du projet de *Digital Copyright Act* dont l'article 13 réclame des plates-formes qu'elles prennent à la demande des ayants droit des mesures raisonnables, « appropriées et proportionnées », pour prévenir des violations des droits de propriété intellectuelle.

[53] *Cf.* la Communication de la Commission européenne (« Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, « Tackling online disinformation: A European approach »,

des services minimaux de base conformes aux exigences de protection des données. Faut-il y voir une nouvelle forme de service universel, cette fois non plus lié à l'« abordabilité » financière (*affordability*) de l'accès aux services, voire leur gratuité, mais débordant sur d'autres aspects de la qualité du service offert ? Je le crois[54]. Autre extension touchant cette fois au contenu de l'information, l'obligation faite aux autorités publiques, voire plus largement aux organismes détenus par ces autorités, de mettre à la disposition du public l'information détenue par eux sous une forme telle que le contenu puisse être réutilisé facilement (voy. le principe d'*open data*)[55]. On ajoute dans le même esprit, la demande du Conseil de l'Europe[56] que certains événements qui sont estimés représenter un enjeu ou un intérêt public (un match de football, mais surtout un débat parlementaire ou l'information sur une catastrophe nationale) soient l'objet d'une diffusion gratuite ou, en tout cas, sans acquittement d'un droit d'accès[57].

22. Le droit d'accès à l'Internet – Un droit de l'homme ? – Certains voient dans la reconnaissance de ces droits d'accès, hier à l'infrastructure, aujourd'hui à certains services de l'Internet, tant de communication, d'accès à l'information que de contenu, les prémices, voire la reconnaissance, d'un droit de l'homme nouveau, celui de l'accès à l'Internet. Dans un article récent, Mme Turgis[58] reprend notamment les propos de la Cour constitutionnelle française dans l'affaire *Hadopi*[59], mais également les propos du rapporteur spécial à l'Assemblée générale de l'ONU : « Dans

COM/2018/236 final) qui en appelle à l'autorégulation, tout en soulignant certains principes pour lutter contre les *Fake News*.

[54] *Cf.* Y. Poullet, « Au-delà du service universel des télécommunications : le service universel dans la société de l'information », *in Les consommateurs et la société de l'information*, Bruxelles, Centre coopératif de la consommation, 1998, p. 41-43. (le document en format PDF se trouve à l'URL suivante : http://www.crid.be/pdf/public/4640.pdf). Dans le même sens, *cf.* les réflexions de J. Senechal, « Vulnérabilité et contrôle du contractant à l'ère numérique », *in* H. Jacquemin et M. Nihoul, *Vulnérabilités et droits*, *cit.*, p. 107 et s.

[55] *Projet de directive du Parlement européen et du Conseil concernant la réutilisation des informations du secteur public* (refonte), Bruxelles, le 25 avril 2018, *COM*(2018) 234 final. Le texte a fait l'objet d'un accord (22 janvier 2019) par l'ensemble des pays européens : « *Data is increasingly the lifeblood of today's economy and unlocking the potential of public open data can bring significant economic benefits. The total direct economic value of public sector information and data from public undertakings is expected to increase from €52 billion in 2018 to €194 billion by 2030. With these new rules in place, we will ensure that we can make the most of this growth.* »

[56] Sur ces différents textes, C. Lamouline et Y. Poullet, *Des autoroutes de l'information à la démocratie électronique*, *Rapport au Conseil de l'Europe, octobre 1995*, Coll. Droit et Justice, Bruxelles, Bruylant, Nemesis, 1997.

[57] Sur ces différents textes, *cf.* C. Lamouline et Y. Poullet, *Des autoroutes de l'information à la démocratie, cit.*

[58] S. Turgis, « Les droits de l'homme à l'heure d'internet et du numérique : rupture ou continuité ? », *in* C. de Terwangne et Q. van Enis (dir.), *L'Europe des droits de l'homme à l'heure de l'Internet*, Bruxelles, Bruylant, 2019, p. 93-128.

[59] Conseil constitutionnel, *Loi favorisant la diffusion et la protection de la création sur Internet (loi Hadopi I)*, décision 2009-580 DC du 10 juin 2009, cons. 12.

certains États économiquement développés, l'accès à Internet a été reconnu comme un droit » et ce dernier conclut que, « bien que l'accès à Internet ne soit pas encore un droit de l'homme en tant que tel […] les États ont pour obligation positive de promouvoir ou de faciliter l'exercice de la liberté d'expression et de fournir les moyens nécessaires à l'exercice de ce droit, notamment Internet »[60]. Le rapporteur spécial souligne que l'accès à Internet déborde le cadre de l'exercice de la liberté d'expression, puisqu'il est aussi indispensable à l'exercice « d'autres droits, dont le droit à l'éducation, le droit de s'associer librement avec d'autres et le droit de réunion, le droit de participer pleinement à la vie sociale, culturelle et politique et le droit au développement économique et social »[61]. Faut-il suivre ces auteurs ? Comme Mme Turgis, je les mets en garde contre la tentation de l'efflorescence de nouveaux droits de l'homme liés à l'Internet, tant en matière de liberté d'expression (droit d'accès à l'Internet, droit à la culture, droit à la transparence, etc.) que de protection de la vie privée (droit à l'anonymat, droit à l'oubli, droit à la portabilité, etc.). De tels droits, que Mme Turgis qualifie de simples droits subjectifs « gigognes », s'articulent et dérivent des droits fondamentaux. Il faut craindre – s'inquiète-t-elle comme nous, la propension des législateurs et de certaines doctrines à les qualifier de droits fondamentaux, au risque d'un affaiblissement de la notion : « Envisager une modification de la liste des droits de l'homme, en y consacrant de nouveaux droits[,] pose la question de l'utilité, voire du caractère contre-productif d'une telle démarche [...] lorsque tout devient fondamental, rien ne l'est plus vraiment. » En particulier, le droit d'accès à l'Internet doit s'analyser non comme un droit de l'homme, mais comme une conséquence de l'obligation positive de l'État de favoriser la liberté d'expression de chacun, obligation traduite aujourd'hui par la création d'un service universel encore limité, mais que les besoins de l'individu dans une société du numérique toujours plus nécessaire à notre épanouissement élargiront certainement comme je l'ai indiqué. La reconnaissance d'un droit constitutionnel risque, au contraire, de rendre plus difficile cette évolution[62].

23. Le droit à l'éducation – La robotisation et l'obligation de chacun d'utiliser dans son travail les ressources des technologies du numérique posent d'autres problèmes : celui de l'accès au marché du travail et celui de la disqualification de certains métiers. Le droit à l'éducation affirmé par la Charte européenne des droits fondamentaux ne crée-t-il pas une obligation positive des États de veiller à l'éducation, y compris « tout au

[60] Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, F. La Rue, AGONU, A/66/290, 10 août 2011, § 61 et 65.
[61] *Ibid.*, § 61.
[62] Sur ce point, nos réflexions qui rejoignent celles de Mme Turgis. *Cf.* Y. Poullet, « Quelques réflexions d'avant-propos », *in* C. de Terwangne et Q. van Enis (dir.), *L'Europe des droits de l'homme à l'heure de l'Internet*, *cit.*, p. 7-39.

long de la vie » de chacun et, en particulier, des travailleurs, à l'utilisation des technologies du digital ? Différents textes le précisent. Ainsi, le Conseil de l'Union européenne se fonde sur le premier principe du Pilier européen des droits sociaux, en l'occurrence, le droit à une éducation de qualité et inclusive, à une formation et à un enseignement tout au long de la vie, pour reconnaître que les « *competence requirements have changed with more jobs being subject to automation* » et pour recommander[63] le développement de bonnes pratiques à cet égard[64]. Au niveau international, l'Organisation internationale du travail (OIT) s'appuie sur l'article 26 de la Déclaration universelle des droits de l'homme pour affirmer que l'éducation permanente à l'utilisation des technologies du digital constitue la clé de la participation de tous aux bénéfices des nouvelles technologies et des emplois qu'elles offrent[65]. La participation des représentants des travailleurs est vivement recommandée, de même que l'obligation pour les États de prévoir des systèmes d'« assurance-emploi » et des fonds sociaux destinés à financer cette éducation continue.

B. Numérique et agression[66]

24. Des risques multipliés – Qu'Internet et ses applications deviennent l'instrument d'une multiplication sans précédent d'agressions contre les individus s'explique aisément[67]. Le message sur l'Internet, outre qu'il présente une apparence de vérité et de sincérité de son contenu[68], semble certifier son origine[69] et permettre ainsi d'abuser de notre fragilité psychologique[70]. La technologie permet à quiconque de s'introduire au cœur de nos systèmes d'information[71], de notre intimité[72], voire de notre

---

[63] Recommandation du 22 mai 2018 relative aux compétences et à l'éducation permanente, *J.O.*, 4 juin 2018, n° 189, p. 1.

[64] *Ibid*. La recommandation énumère huit compétences : « *literacy competence, digital competence, personal, social and learning to learn competence and entrepreneurship competence* ».

[65] Global Commission on the Future of Work, *Work for a Brighter Future, Report*, Genève, International Labour Office, 2019, p. 30-32.

[66] Sur cette question, pour un exposé plus complet, lire N. Colette-Bazecqz, « La protection des personnes vulnérables », *cit*., p. 133 et s.

[67] *Ibid*.

[68] C'est tout le phénomène de la cyberprédation, dissimulation d'identité, d'âge ou de qualité, permettant de faire miroiter un avantage.

[69] Ainsi, le *phishing*, qui reproduit le site d'une entreprise pour soutirer des données à caractère personnel, voire de l'argent.

[70] Ainsi, le *grooming*, infraction qui consiste en l'envoi de textes ou d'images d'incitation à caractère sexuel.

[71] Ainsi, le *skimming,* qui consiste en une copie illégale des données reprises sur une carte électronique.

[72] On songe ainsi aux *spywares*, mais également à toutes les possibilités de *hackin*g des communications permises par l'Internet des objets et de manipulation de leur fonctionnement, ce

corps[73]. Les quelques considérations qui suivent s'interrogent sur, d'une part, la manière dont cette constatation des risques créés par le numérique d'exploitation de nos faiblesses, voire le renforcement de celles-ci, justifie la définition de nouvelles infractions et, d'autre part, la façon dont le droit s'est emparé de la même technologie pour s'attaquer à ceux qui utilisent les ressources offertes par le digital pour agir contre ces derniers.

25. La réponse du droit – La création de nouvelles infractions au risque de la « sécurité juridique » – Il me semble qu'à cet égard, on peut relever les tendances suivantes.

a) La première a déjà été citée : la criminalité informatique touche sans doute plus sensiblement certaines catégories de personnes de par leur vulnérabilité et justifie que, pour ces catégories, de nouvelles infractions soient créées ou des concepts élargis afin de protéger ces catégories. Je pense en particulier aux enfants dont la protection lors de leur utilisation de l'Internet justifie, en particulier en matière sexuelle, la création de dispositions pénales nouvelles. Sans prétendre être exhaustif, je cite le *grooming* (art. 377, 4°, du Code pénal [C. pén.]) ou la pédopornographie (art. 383*bis*, § 1er, C. pén.) où la disposition vise désormais également « des images réalistes représentant un mineur qui n'existe pas… ».

b) Si ce qui est puni *off-line* doit également être puni *on-line*, on note que tantôt, les définitions ont dû être adaptées, tantôt, le plus souvent, des dispositions ont été adoptées afin de viser la réalité comparable du vécu dans le monde digital. Ainsi, l'utilisation d'une carte de crédit volée aux fins de retirer l'argent ressemble furieusement à l'escroquerie, sauf que la disposition relative à cette dernière infraction vise le fait de tromper une personne, et non une machine. Il a donc été nécessaire de créer une disposition relative à la fraude informatique. Bien d'autres exemples (voy. le faux en informatique ou le voyeurisme [art. 371/1 C. pén.]) peuvent ainsi être donnés. Parfois, il suffit d'ajouter à des dispositions déjà existantes un paragraphe consacré à la circonstance particulière de sa commission via la technologie du numérique. Ainsi, les dispositions relatives à la cyberprédation (art. 433*bis* C. pén.) ou le cyberharcèlement (atteinte à la tranquillité des personnes) (art. 442*bis*

qui peut être particulièrement dangereux et dommageable (p. ex., accès au système de conduite d'une voiture intelligente).

[73] Ainsi, récemment, le cas de *sextoys* fonctionnant en ligne en connexion avec l'accès à des sites web à caractère pornographique, l'entrée d'un hacker dans le système de connexion à distance lui permettait de prendre le contrôle du fonctionnement de ceux-ci. Dans un tel cas, peut-on parler de viol au sens juridique du terme ? On retient que la cour d'appel de Liège, le 7 avril 2011, par une décision inédite, a condamné pour viol l'internaute qui avait contraint une mineure observée par webcam à introduire un crayon dans ses parties génitales.

C. pén.). La prise en compte comme circonstance aggravante de la vulnérabilité de la victime ou de la volonté de discrimination est parfois reprise. Ainsi, la loi du 26 novembre 2011 a précisé, à propos du cyberharcèlement, la circonstance aggravante que celui-ci soit commis envers une personne vulnérable (*en raison de son âge, de son état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale*) (art. 442*bis* C. pén.) ou s'appuie sur un mobile discriminatoire (orientation sexuelle, race, sexe…) (art. 442*ter* C. pén.).

c) Enfin, et ce point a déjà été relevé (*supra*, n° 4), c'est la vulnérabilité ontologique de l'homme qui est mise à mal par l'exploitation de l'outil numérique. On ne peut donc que saluer l'introduction en droit pénal, par la loi du 26 novembre 2011, d'une infraction portant sur l'« abus de la situation de faiblesse d'autrui », même si, comme le relèvent certains auteurs, cette reconnaissance méconnaît peut-être le principe de légalité qui régit le droit pénal et exige la précision des infractions dont l'interprétation doit être stricte[74].

26. La réponse du droit – L'utilisation de l'informatique au secours de la protection des personnes et les dangers du dogme de la sécurité – Ici, également, le propos sera bref[75]. La règle générale fixée par l'article 8, § 2 (atteintes possibles à la vie privée), et l'article 52 de la CEDH affirme que les méthodes d'enquête doivent respecter les principes de légalité, de nécessité et de proportionnalité. Ces principes, en particulier ceux de la proportionnalité, voire de la nécessité, justifient-ils la longue liste des obligations nouvelles imposées à certains acteurs et les nouvelles prérogatives des autorités judiciaires ou de police accordées généreusement par le Code d'instruction criminelle ? Ainsi, les opérateurs et fournisseurs de réseaux de communication (les Proximus, Orange, mais aussi Skype, Facebook, WhatsApp, etc.) doivent aider à l'identification, au repérage et à l'interception de toute communication. Certes, la demande doit émaner du procureur du Roi ou du juge d'instruction. La saisie des ordinateurs et, de manière générale, de tout équipement terminal peut être ordonnée par un officier de police judiciaire et, outre que sa « fouille » peut révéler des informations sans lien avec l'infraction pour laquelle la saisie a été ordonnée, elle peut de plus mettre à mal le secret professionnel de certains acteurs (avocats, médecins…), dont les communications avec l'auteur supposé de l'infraction sont ainsi révélées. L'accès au contenu chiffré ou protégé

[74] Sur ce point, l'article déjà cité de N. Colette-Bazecqz, « La protection des personnes vulnérables », *cit*., en particulier p. 135 et s. ; p. 175 et 176 et les nombreuses références y reprises.

[75] Je renvoie le lecteur à l'article de C. Forget, « Méthodes d'enquête pénale et protection des personnes vulnérables dans l'environnement numérique », *in* H. Jacquemin et M. Nihoul (dir.), *Vulnérabilités et droits*, *cit*., p. 179 et s.

par un code d'accès peut être obtenu grâce à l'installation via spyware de dispositifs techniques permettant cet accès ou le décryptage ou le décodage des données. On s'inquiète de ne pas retrouver, en droit belge, certaines garanties de protection des libertés, pourtant énoncées par la Convention n° 181 du Conseil de l'Europe sur la cybercriminalité[76] et précisées par la jurisprudence de la Cour[77]. Ainsi, la décision de mise en surveillance exige que l'on s'interroge sur la gravité des infractions, sur les catégories de personnes mises sur écoute, sur la fixation de limites à la durée de cette surveillance, etc. Dernière réflexion, demain, grâce à l'*IA*, les « vérités » sorties de nos ordinateurs permettront de détecter les potentiels criminels, terroristes ou non. Autorisera-t-on sur cette base nos autorités judiciaires ou policières à prendre des mesures vis-à-vis de ces « potentiels » criminels, à prévenir le crime et non plus simplement à le réprimer ?

V. Numérique, stigmatisation, normalisation et manipulation (les *nudges* ou le paternalisme libertarien)

27. Le numérique, comme outil de sujétion de l'homme : d'Orwell à Kafka – Notre vulnérabilité face au numérique est ontologique. C'est l'homme et non une catégorie ou des catégories spécifiques d'individus qui se trouvent à la fois multipliés, augmentés, ubiquitaires grâce à la machine, mais également « nous » devant la machine. Voilà, désormais, l'homme suivi et surveillé… En permanence, le voilà transparent au moment même où, de plus en plus, le fonctionnement des systèmes de collecte, de traitement et de transmission de l'information s'opacifie ; voilà l'homme mémorisé et stigmatisé, réduit à son profil et aperçu à travers ses données ; voilà l'homme manipulé insidieusement ; voilà, enfin, l'homme « prévu », gouverné par la magie d'une intelligence « artificielle », celle du numérique.

Face à ces risques majeurs, quelle réponse le droit peut-il donner ? Comme annoncé et décrit ci-dessus (n° 9), le concept de vie privée a donné naissance aux nombreuses législations de protection des données et récemment au Règlement général de la protection des données (le RGPD). Ce Règlement, présentant un modèle européen à la face du monde, élargissant encore les droits de la personne concernée, les obligations des responsables de traitement, et renforçant les moyens de contrôle et les sanctions

[76] *Cf.* Convention n° 181 du Conseil de l'Europe sur la cybercriminalité.

[77] *Cf.* not. la décision de la CEDH du 4 décembre 2015, *Zacharov c. Russie* (aff. n° 47143/06, § 231). Sur ce point, lire C. Forget, « Procédure et méthodes d'investigation sur Internet », *in* C. de Terwangne et Q. van Enis (dir.), *L'Europe des droits de l'homme*, *cit*., 2019.

à disposition des autorités, est-il à la hauteur des risques dénoncés ? Voilà l'objet des paragraphes qui suivent.

28. RGPD – Une réponse adéquate ? – Le sentiment dominant en réponse à cette question est certes positif, il est cependant difficile de ne pas noter quelques lacunes ou insuffisances de la protection accordée et surtout de dénoncer l'approche suivie. Ainsi, il est certain que l'élargissement considérable des droits de la personne concernée permet cette protection individuelle, mais encore faut-il exercer ces droits, ce qui, je le crains, ne sera pas le fait des groupes de personnes vulnérables[78]. Les paragraphes précédents ont également noté l'importance du principe de non-suffisance qui, même si on déplore les exceptions sans doute trop généreusement libellées, apparaît comme un bon rempart contre les décisions automatisées fondées sur les seules vertus de l'algorithme. Les obligations de sécurité, renforcées par les règles en cas de « brèches de sécurité », préviendront les accès illégitimes ou non autorisés[79]. La portée extraterritoriale du RGPD l'impose aux entreprises étrangères lorsque celles-ci développent une offre de biens ou services à des personnes sises en territoire européen ou suivent leur comportement.

Quelques limites sont cependant à craindre, en particulier, face aux développements des systèmes d'intelligence artificielle. En bref, ces systèmes obligent à repenser l'objet même des législations de protection des données, dans la mesure où ils travaillent tant sur des données à caractère personnel que non personnel (p. ex., les statistiques de réussite scolaire, de revenus par quartier, etc.) ; le hasard des corrélations peut révéler au responsable l'intérêt de la poursuite d'autres finalités que celle envisagée au départ, et ce, au mépris du principe de finalité spécifique et déterminée ; ces systèmes d'IA travaillent sur des données *a priori* et souvent *a posteriori* non pertinentes, là où le RGPD réclame qu'on ne peut utiliser que les données strictement nécessaires pour l'obtention de la finalité poursuivie ; si le RGPD réclame qu'une information soit donnée sur la « logique suivie », la transparence des algorithmes de *deep learning* est difficile, voire impossible. Par ailleurs, l'obligation de transparence, même légale, se heurte au secret d'affaires ou aux autres droits de propriété intellectuelle, élevés par la Charte européenne des droits de l'homme au

[78] À noter cependant premièrement que la plainte à l'Autorité de protection des données peut suffire à déclencher l'enquête sur les pratiques du responsable de traitement et que le RGPD a consacré la possibilité d'une *Class Action*, qui permet un recours non plus individuel, mais collectif, mené par des associations de consommateurs ou de libertés civiles.

[79] On ajoute que l'article 5.3 de la *directive e-Privacy* (en cours de révision) soumet au consentement des personnes concernées l'introduction de *spywares* ou *cookies* à l'intérieur du terminal de la personne concernée, protégeant, selon l'expression du Tribunal constitutionnel allemand (BVerfG, 2008), nos terminaux à l'instar d'un « domicile » (certes, virtuel), comme le prescrit l'article 8.1 de la CEDH.

rang de droits de l'homme. Ensuite, la question de la légitimité de la prévision des comportements n'est pas abordée en tant que telle et, pourtant, elle soulève des défis majeurs pour la vulnérabilité des individus : la police peut-elle utiliser des systèmes d'IA pour prévenir des crimes ? Les internautes ont-ils le droit de ne pas être soumis à un profilage ?

Enfin, et cette critique me paraît essentielle, le RGPD repose sur une conception purement individualiste de l'autonomie, que traduit la primauté du consentement que certains estiment en définitive la cause ultime de la légitimité des traitements. Sans doute, reconnaît-on que l'exigence d'un consentement libre, éclairé, spécifique et univoque est purement illusoire à l'heure où celui-ci est au bout d'un simple clic donné d'autant plus rapidement que le service présenté comme gratuit apparaît comme nécessitant une réponse urgente ? En outre et plus fondamentalement, cette conception individualiste du consentement se heurte à celle d'une autonomie qui affirme que l'individu est d'abord un être social et, donc, que son action doit être estimée à l'aune de l'intérêt général. Prenons un exemple : comme d'aucuns, j'ai été approché par ma compagnie d'assurances auto me recommandant d'accepter que mon risque individuel ou plutôt profil calculé à la suite des données communiquées (localisation, vitesse, parcours habituel, kilométrage parcouru, voire état d'alcoolisme…) par un mouchard installé dans mon véhicule fixe à la baisse – cela va de soi, M. Poullet – ma prime d'assurance. Ce traitement, qui trouverait sa légitimité dans mon seul consentement, généralisé par le consentement d'autres conducteurs dits « modèles de bonne conduite », remet en cause un principe fondamental de l'assurance qui est celui de la mutualisation des risques. Au-delà de cette première considération, il me semble que l'individu n'est pas en mesure de se protéger efficacement contre la puissance de certains prestataires majeurs dans l'économie du secteur des services du Net et vu la complexité et non-transparence des traitements et des flux de collecte et de communication des données. L'enjeu des opérations, qui se cachent derrière le consentement individuel, concerne non seulement la personne concernée, mais également d'autres personnes qui pourraient être discriminées[80], voire des choix de société. Comme l'écrivent Mmes Lobet

[80] Dans la mesure où leur profil construit à partir de leurs données, mais également des miennes comme d'autres utilisateurs, conduirait à prendre des décisions désavantageuses pour elles. Le CCPA accorde une importance particulière à ces risques de discrimination, non relevés en revanche dans les textes européens. *Cf. (a) (1) A. business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:(A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title. (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level*

et Cohen[81], ne s'agit-il pas d'un *privacy bug* des lois de protection des données, c'est-à-dire d'un cadre juridique qui affirme l'importance de la vie privée pour l'autonomie des sujets et, partant, la démocratie, mais qui, à travers le concept de « consentement individuel, laisse le poids de la défense de la protection des données aux individus ? » Et ce, j'ajoute, au risque de renforcer la vulnérabilité des individus.

A. Numérique et discrimination

29. Les risques envisagés – L'utilisation par les administrations, entreprises ou autres organismes multiplie les risques de discrimination. Le premier type de discrimination est la conséquence de l'impossibilité ou la difficulté pour certaines personnes d'utiliser correctement les systèmes d'information mis à leur disposition par ces organismes. Cette difficulté est liée à l'absence de convivialité de certains sites, dont certains représentent pourtant un passage obligé pour l'exercice de droits, en particulier ceux de l'administration. D'autres discriminations trouvent leur origine dans le fait que des organismes utilisent l'information collectée pour connaître l'internaute client, voire prédire son comportement, et adaptent leur message au « profil » ainsi dessiné. Sur la base de ce profilage, ces organismes réserveront l'accès à certains, différencieront les modalités de la transaction en fonction de ce profil[82] ou, dans le cas de la police, repéreront de manière systématique les présumés auteurs d'infraction. Ces risques de discrimination sont encore accrus par les possibilités qu'offre l'intelligence artificielle de construire de tels profils. Des textes récents prévoient des dispositions de manière à limiter ces risques. On citera certaines dispositions du RGPD, obligeant à informer du profilage et à en expliquer la logique. Une recommandation en cours de révision du Conseil de l'Europe va plus loin encore[83]. Dans le domaine du profilage policier, l'article 11 (3)

---

or quality of goods or services. Les paragraphes consacrés à la discrimination reviendront sur ce point.

[81] C. Lobet-Maris, « Le fétichisme de la donnée à caractère personnel – Relecture politique et critique de la vie privée », *in* C. de Terwangne, E. Degrave, S. Dusollier et R. Queck (dir.), *Law, Norms and Freedoms in the Cyberspace. Liber amicorum Yves Poullet*, Bruxelles, Larcier, 2018, p. 696, et J. Cohen, « Privacy, ideology and technology », *Georgetown Law Journal*, n° 89, 2001, p. 20-29. Voy. également les réflexions de A. Vedder et L. Naudts, « Accountability for the use of algorithms in a big data environment », *International Review of Law, Computers & Technology*, n° 31-2, 2017, p. 206-224, et de A. Vedder, KDD, « The challenge to individualism », *Ethics and Information Technology*, n° 1, 1997, p. 275-281.

[82] Il s'agit des techniques d'*adaptative pricing*, développées par certains prestataires de biens et services qui déterminent le prix en fonction, notamment, de l'intérêt pour le bien ou le produit présumé conformément au profil de l'internaute.

[83] Sur le profilage et les dispositions en matière de profilage, tant du RGPD que des recommandations en cours ou projetées du Conseil de l'Europe, Y. Poullet et B. Frenay, *Profilage et la Convention 108+. Rapport sur l'évolution de la situation après l'adoption de la*

de la directive relative à la protection des données (à caractère personnel par les autorités judiciaires ou de police [directive (EU) 2016/680]) interdit explicitement tout profilage qui contiendrait ou conduirait à des discriminations sur la base de catégories spécifiques de données, comme la race, l'origine ethnique, l'orientation sexuelle, les opinions politiques et les convictions religieuses[84].

30. Discrimination et IA – Les risques de discrimination liés à l'utilisation de vastes bases de données et des systèmes d'intelligence artificielle nécessitent la recherche de critères qui permettraient de distinguer les inégalités de traitement non discriminantes parce que justifiées de celles qui sont inacceptables[85]. La réponse est difficile dans la mesure où les critères de différenciation qui sont à la base des profils évoluent dans le cadre du fonctionnement de systèmes d'intelligence artificielle dits de *deep learning* et que l'essence même des *Big Data* est d'offrir aux corrélations le maximum de possibilités, en multipliant donc les sources et les types de données sans considération de leur pertinence *a priori*. Sans doute, des précautions doivent être prises d'emblée pour éviter les biais qui pourraient *a priori* discriminer des catégories d'individus ou aboutir à des résultats non fiables ou erronés. La question de la sélection des données est également posée : par exemple, dans un système de recherche policière, peut-on admettre d'inclure des données relatives à des infractions anciennes, des données sur la religion ou sur l'origine sociale qui pourraient conduire à des résultats non fiables (cas 1) ou des discriminations (cas 2 ou 3). On

---

Recommandation (2010)13 sur le profilage, Strasbourg, 7 novembre 2019, Comité consultatif de la protection des données, T-PD (2019) 07rev.

[84] On retrouve la même mise en garde en considérant le n° 71 du RGPD : « *In order to ensure fair and transparent processing in respect of the data subject, [...] the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons [...]* » (RGPD, recital 71). Et, plus récemment, le rapport du Parlement européen, *Fundamental Rights Implications of Big Data*, Sept. 2017 (P8_TA-PROV, 2017, 0076).

[85] À cet égard, Naudts (A. Vedder et L. Naudts « Accountability, *cit*. », n° 3 et s.) propose de retenir le critère de Dworkin (« What is equality? Part 2: Equality of resources », *Philos Public Aff.*, 1981, n° 10, p. 283-345) : sont justes les inégalités de traitement qui correspondent à des différences dont la personne qui les subit peut être tenue responsable ; à l'inverse, la discrimination existe si la différence se fonde sur des critères dont la personne ne peut être tenue responsable. « *Dworkin states that individuals are treated equally (with regard to the distribution of resources) only if that distribution is "sensitive towards 'ambition' or 'option luck', i.e. the traits and choices for which individuals should be held responsible, but insensitive to endowments and brute luck, i.e. those things for which the individual should not be held responsible" (Dworkin, 1981; Hausman 2009). Whereas inequalities due to option luck are just, inequalities due to brute luck are unjust (Dworkin 1981; Barry 2008). Option and brute luck can also inform us about the fair (or unfair) character of inequalities*. »

souligne également le devoir du responsable de traitement d'analyser les risques liés à l'implémentation de tels traitements[86]. Tout récemment, à la suite du scandale *Cambridge Analytica*, le 23 octobre 2018, le Parlement européen a réclamé l'audit par l'ENISA et l'*European Data Protection Board* du système de *ranking* et d'évaluation de leurs clients, mis en place par Facebook. Tous ces risques justifient un devoir de vigilance[87] non seulement à l'élaboration du système (avec obligation de tests avant démarrage effectif) et de manière continue, devoir qui pourrait impliquer l'intervention de comités d'éthique[88]. Sans doute, ces devoirs et ce principe de non-discrimination devront-ils être inscrits dans une prochaine législation, que nous appelons de nos vœux.

31. Discrimination et accès à certaines applications – Je me limite à deux points même si je suis convaincu que d'autres points soulèveront rapidement des difficultés. Ainsi, on pourrait pointer les questions de

---

[86] L'obligation est instituée par l'article 35 du Règlement : « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, d'effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ». Pour une application aux traitements dits de *social scoring*, lire : « *We value the freedom and autonomy of all citizens. Normative citizen scoring (e.g., general assessment of "moral personality" or "ethical integrity") in all aspects and on a large scale by public authorities endangers these values, especially when used not in accordance with fundamental rights, or when used disproportionately and without a delineated and communicated legitimate purpose. Today, citizen scoring – at large or smaller scale – is already often used in purely descriptive and domain-specific scorings (e.g. school systems, e-learning, or driver licenses). However, whenever citizen scoring is applied in a limited social domain, a fully transparent procedure should be available to citizens, providing them with information on the process, purpose and methodology of the scoring, and ideally providing them with the possibility to opt out of the scoring mechanism. This is particularly important in situations where an asymmetry of power exists between the parties. Developers and deployers should therefore ensure such opt-out option in the technology's design, and make the necessary resources available for this purpose.* »

[87] « *For the purposes of these Guidelines, the principle of justice imparts that the development, use, and regulation of AI systems must be fair. Developers and implementers need to ensure that individuals and minority groups maintain freedom from bias, stigmatisation and discrimination. Additionally, the positives and negatives resulting from AI should be evenly distributed, avoiding to place vulnerable demographics in a position of greater vulnerability and striving for equal opportunity in terms of access to education, goods, services and technology amongst human beings, without discrimination. Justice also means that AI systems must provide users with effective redress if harm occurs, or effective remedy if data practices are no longer aligned with human beings' individual or collective preferences* » (*Draft Report of the High Level Experts Group*, *cit.*, p. 11).

[88] Sur ce point, lire A. Mantelero, « Artificial Intelligence and data protection: Challenges and possible remedies – Report, », Comité consultatif de la Convention n° 108 du Conseil de l'Europe, 3 décembre 2018, T-PD (2018) 09Rev. La Déclaration de Montréal exige même que « [l]a découverte d'erreurs de fonctionnement des SIA, d'effets imprévus ou indésirables, de failles de sécurité et de fuites de données doit être impérativement signalée aux autorités publiques compétentes, aux parties prenantes concernées et aux personnes affectées par la situation ».

l'accès à l'éducation, à l'emploi, à la santé, au logement… dont seront privées des personnes en raison du profil auquel elles « appartiennent ». Le premier concerne l'accès aux services publics. Dans leurs rapports respectifs, E. Degrave et P. Brotcorne soulignent les dangers du *All Digital* de l'administration publique, en d'autres termes, le fait que, de plus en plus, les citoyens sont invités de manière pressante à utiliser la voie électronique désormais privilégiée pour l'accès aux services de l'administration[89]. Cette digitalisation tous azimuts soulève une difficulté croissante d'accès pour certaines catégories de population d'accéder à l'administration[90]. Par ailleurs, le rapport de Mme Degrave souligne les risques pour la vie privée et l'autonomie des citoyens liés à une politique dite de « *Benevolent e-government* » qui, sur la base de croisement de données à caractère personnel détenues par diverses administrations, repère les personnes ayant droit à telle prestation et les contacte systématiquement afin de leur offrir le bénéfice d'une prestation (p. ex., la fourniture de mazout de chauffage, ou l'octroi d'une réduction de redevance pour le ramassage des déchets), sans qu'il y ait eu déclaration d'intérêt de la part du citoyen.

Le second cas que j'évoque est l'irruption du numérique dans le domaine de la santé. Des applications nées des technologies du numérique permettent d'augmenter les capacités de l'homme via des implants corporels permettant, par exemple, de décupler la mémoire ou de lutter contre la vieillesse ou, par des manipulations génétiques, de modifier le bagage génétique de l'individu. Ces possibilités nouvelles ouvrent à terme la voie à une humanité à deux vitesses par définition discriminante, si l'offre de telles possibilités est réservée à ceux qui financièrement peuvent se les « offrir »[91].

B. Numérique et identité humaine

32. La mise en cause de l'identité humaine – Dans ce dernier point, il s'agit de faire écho à deux problématiques nouvelles : l'existence de robots et celle des manipulations génétiques grâce aux NBIC. Ce qui rapproche

[89] Déclaration fiscale en ligne, accès au dossier pension, déclaration de naissance, etc. À l'origine de cette digitalisation des relations entre citoyens et administration, la volonté de diminuer les coûts pour l'administration et de meilleure efficacité pour le citoyen.

[90] *Cf.*, à cet égard, les références commentées par P. Brotcorne (« L'effectivité des libertés fondamentales, *cit*. », p. 45) au *Rapport du défenseur des droits de la République française* de 2017, à l'étude CREDOC et à celle d'Emmaüs, qui dénoncent également la question du langage utilisé par ces sites web de l'administration et leur complexité d'utilisation, écartant de leur usage ceux qui en ont le plus besoin.

[91] Sur ce point, dès 2005, les réflexions du Groupe européen d'éthique des sciences et des technologies nouvelles, « Aspects éthiques des implants TIC dans le corps humain », disponibles à l'adresse : http://ec.europa.eu/european_group_ethics/publications/docs/avis20compl_en.pdf. *Cf.* également Y. Poullet, *Éthique et droits de l'homme*, *cit.*

ces deux problématiques et justifie leur analyse dans un ouvrage relatif aux vulnérabilités est la conviction suivante : le robot et les NBIC constituent, aux yeux de l'imaginaire social, la maîtrise quasi parfaite scientifique et technique du monde, une maîtrise qui permet le dépassement des limites humaines, de la vulnérabilité de chacun de nous[92]. Comme le note N. Le Devedec[93], le transhumanisme évacue la dimension sociale, affective et culturelle de l'homme au profit d'une perfectibilité seulement technique. « La figure humaniste de l'homme révolté, qui fonde son humanité sur sa capacité à transformer la société, cède sa place à celle de l'homme adapté, modifié par la technologie pour se conformer à la société existante »[94]. Bref, dans les deux cas, c'est l'affirmation et le rejet de notre vulnérabilité ontologique au profit d'un « monde meilleur » à la Aldous Huxley, qui traversent l'idéologie transhumaniste à l'œuvre dans le développement de ces deux technologies.

a) Le robot

33. Des robots au rêve du transhumanisme – Les développements récents de la technologie du numérique, en particulier grâce à l'intelligence artificielle, laissent accroire l'idée que l'homme pourrait trouver dans la machine un substitut à lui-même dans l'accomplissement de tâches bien humaines, substitut par ailleurs plus performant que lui-même, comme en témoigne le robot joueur de poker américain : Libratus, programme informatique d'intelligence artificielle auto-apprenant ayant battu à Pittsburgh, en 2017, les meilleurs joueurs de poker américain. Le robot Nao aide les malades. Sofia est devenue une ambassadrice de charme du royaume d'Arabie saoudite, répondant avec aisance aux questions des journalistes et, demain, certains voudraient voir les juges remplacés par des robots au profit d'une justice, plus efficace et « plus juste ». Au-delà, il est permis d'espérer que le cerveau humain dialogue avec la machine, voire soit transvasé vers celle-ci ou vice versa et que, progressivement, notre intelligence devienne de plus en plus « artificielle » (transhumanisme), entraînant la disparition de la race humaine ou son asservissement à ces êtres supérieurs (posthumanisme).

34. Le droit au secours des robots – Les premières apparitions des robots nés de l'IA, présents dans la vie de tous les jours en santé (robots chirurgien, aide-soignant, prescripteur de médicaments ou de soins…), sur

[92] On ajoute que ces limites sont, aux yeux des transhumanistes, liées au corps. Libérer l'homme des limites de son enveloppe charnelle est le propos de nombre d'entre eux.

[93] N. Le Devedec, « Humanisme, transhumanisme : deux conceptions antithétiques de la perfectibilité humaine », *in* F. Damour, S. Deprez et D. Doat (dir.), *Généalogies et nature du transhumanisme – État actuel du débat*, Montréal, Liber, 2018, p. 33.

[94] F. Damour, S. Deprez et D. Doat (dir.), « Introduction », *in Généalogies et nature du transhumanisme*, *cit*., p. 11.

nos routes (voitures intelligentes), dans nos entreprises (les chatbots)… ont été accueillies par le droit de manière bienveillante au regard des bénéfices que leur action pouvait apporter à la société. Ainsi, la Commission européenne s'interroge sur l'intérêt d'accorder un droit de propriété intellectuelle aux « créations » nées des systèmes robotiques ; le droit des contrats envisage des contrats noués via des robots et, récemment, le Parlement européen s'est interrogé sur l'octroi de la personnalité juridique aux robots, ce qui leur permettrait, on peut rêver, de réclamer comme les individus le bénéfice des droits de l'homme, ainsi le droit à la vie, à la non-discrimination et à la liberté d'expression. Sans doute, faut-il voir dans l'octroi de telles prérogatives aux robots assimilables à celles des humains, une protection non des robots, mais bien de leurs concepteurs ou de ceux qui les mettent sur le marché.

b. Les manipulations génétiques

35. De la manipulation génétique à l'eugénisme – « Si la matière est de l'information (codage), écrit le philosophe et homme de sciences Magnin[95], le traitement de celle-ci permet de copier le vivant naturel, mais aussi de le reprogrammer. Désormais, on façonne le monde atome par atome à cette échelle pour laquelle il n'y a pas de différence entre la matière inerte et la matière vivante [...]. Elle permet de modifier le comportement des vivants naturels[,] mais aussi de penser à d'autres formes de vivants que ce[lles] que la nature nous révèle. » Récemment, des chercheurs ont mis au point, sous le nom de CRISP-Cas-9[96], une méthode d'édition de gènes qui permet de couper des gènes dits « fautifs » et de les remplacer par d'autres gènes. Il ne s'agit pas uniquement de réparer l'individu, mais, au-delà, de le transformer, notamment dans un souci d'amélioration de ses performances[97]. Plus radicalement, il s'agit, selon certains transhumanistes, de concevoir « toutes les entités biophysiques comme un donné fonctionnel, manipulable et améliorable *ad vitam aeternam*. Dans cette perspective, le

[95] T. Magnin, *Penser l'humain*, *cit.*, p. 34-35.

[96] Désigné sous le nom de CRISPR pour « *Clustered Regularly Interspaced Short Palindromic Repeats* », c'est-à-dire « courtes répétitions palindromiques groupées et régulièrement espacées ». Sur cette innovation majeure, lire E. Charpentier, « CRISP-Cas-9, l'outil qui bouleverse la génétique ? », *Pour la Science*, n° 456, 2015, et le débat juridique sur la brevetabilité d'une telle innovation, lire « Qui sera le maître de l'outil génétique CRISP-Cas 9 ? », *OMPI Magazine*, avril 2017, p. 26 et s.

[97] Sur ces possibilités, lire B. Duarte, « Entangled agencies: Non identified practices of human – Technology hybridation through body hacking », *Nano Ethics*, VIII/3, 2014, p. 275-285. Lire également D. Lambert, « Le transhumanisme peut-il être l'avenir de l'Homme ? », *Urbaniana University Journal*, n° 3, 2016, p. 45-59 : « Du point de vue de leurs applications à l'être humain, on pourrait classer les technologies en trois catégories : celles qui réparent (entre autres, celles qui guérissent ses pathologies ou pallient certains handicaps), celles qui cherchent à l'"améliorer" (l'"augmenter") et, enfin, celles qui pourraient le transformer » et, du même auteur, *La Robotique et l'intelligence artificielle*, Paris, Lessius, 2019.

transhumanisme est parfois présenté comme l'instrument d'une manipulation des imaginaires sociaux, mobilisée et financée par de grands acteurs économiques – GAFA, Microsoft, IBM, TESLA, etc. – soucieux de créer des besoins et attentes pour des produits et services en préparation »[98]. Dans ce contexte, on soulignera tout l'enjeu des droits de propriété intellectuelle, dont les développeurs des technologies dites du NBIC pourraient se prévaloir pour s'approprier les résultats de leurs recherches.

36. La réponse hésitante du droit et le renvoi à l'éthique – Les développements des technologies du NBIC et en particulier la manipulation du bagage génétique des personnes entraînent des réactions juridiques timides du droit. En matière de droits de propriété intellectuelle, certes l'UNESCO rappelle que le patrimoine génétique est le patrimoine de l'humanité et ne peut faire l'objet d'aucune appropriation, mais sa protestation s'efface lorsqu'il est question des méthodes de manipulations des données génétiques. Conformément aux législations de protection des données, il est souligné que la donnée génétique est, depuis le RGPD, une donnée sensible, dont le traitement est donc soumis à des règles plus strictes. En outre, de telles données appartiennent non à une personne, mais à plusieurs personnes, dans la mesure où ces données sont partagées. Enfin est notée la question des risques de discrimination entre individus à la fois par les conséquences de l'analyse des données génétiques, mais également par le coût de l'accès aux soins permis par les manipulations génétiques et la possibilité de création d'une société où se côtoieraient les hommes augmentés et les autres.

Cette timidité des interventions juridiques s'explique sans doute par la nouveauté des applications de ces technologies NBIC et la crainte d'encadrer trop tôt une innovation dont on ignore les réelles potentialités. Cette crainte justifie le renvoi par les autorités publiques à une réflexion éthique : ainsi, l'UNESCO, face aux développements de la biotechnologie, estime dès 2003[99] : « Chaque individu a une constitution génétique caractéristique. Toutefois, l'identité d'une personne ne saurait se réduire à des caractéristiques génétiques, puisqu'elle se constitue par le jeu de facteurs éducatifs, environnementaux et personnels complexes, ainsi que de relations affectives, sociales, spirituelles et culturelles avec autrui, et qu'elle implique un élément de liberté » et, dans sa Déclaration universelle sur la bioéthique, en appelle à ce débat : « Convaincue que la sensibilité morale et la réflexion éthique devraient faire partie intégrante du processus de développement scientifique et technologique et que la (bio)éthique devrait jouer un rôle capital dans les choix qu'il convient de faire, face aux problèmes

[98] F. Damour, S. Deprez et D. Doat (dir.), « Introduction », *in Généalogies et nature du transhumanisme*, p. 9.
[99] UNESCO, *Déclaration internationale sur les données génétiques humaines*, octobre 2003.

qu'entraîne ce développement »[100]. Ce « contrefort éthique »[101] face à l'eugénisme suffira-t-il face aux forces de l'imaginaire collectif entretenu par de puissants opérateurs économiques et qui fonde la revendication de plus en plus forte d'un droit à l'homme non plus simplement réparé, mais bien augmenté ? Je crains que non et que des balises réglementaires doivent être réfléchies dès maintenant.

Conclusion

37. Une technologie au service de notre vulnérabilité – Affirmer l'ambivalence du numérique à la fois outil de renforcement des capacités de l'individu et instrument d'accroissement des vulnérabilités des individus, voire de notre société, oblige à rappeler un des principes éthiques essentiels : « *Do good and do not harm.* » Il s'agit de militer et de veiller au développement de technologies « bienveillantes » (*benevolent = do good*) et de rejeter les technologies « dommageables » (*maleficent = do not harm*). Il s'agit d'affirmer le devoir à la fois de ceux qui développent de telles technologies ou des applications dérivées de ces technologies, mais également de ceux qui en exploitent l'utilisation, devoir de veiller à ce que leurs développements technologiques et leur mise sur le marché apportent à la société et aux individus des bienfaits et évitent toute atteinte à leurs capacités de développement personnel. Le rappel de ce principe a toute son importance à propos du développement des technologies du numérique et de leurs applications. Certes, le principe éthique de bienveillance s'applique à tout développement technologique, mais en particulier à ces dernières, tant le déploiement du numérique envahit nos vies et les influence. À l'heure de l'eugénisme que nous proposent les NBIC, de la « gouvernementalité algorithmique » que nous assure l'intelligence artificielle, il est évident que la réflexion sur l'*ethical values design* de nos infrastructures, logiciels et applications est nécessaire.

38. La nécessité d'un débat public – L'appel à respecter ce principe éthique amène à s'interroger sur la signification théorique, mais surtout concrète, des autres principes éthiques. Le slogan « *AI for Good* » a trouvé dans de nombreux forums[102] un écho et a provoqué, sans qu'elle semble

[100] UNESCO, *Déclaration universelle*, 2005.

[101] Sur ce « contrefort éthique » et sa nécessité face à la montée du mouvement « eugéniste », lire P. Giorgini, *La Tentation d'Eugénie*, Montrouge, Bayard, 2018, p. 301 et s.

[102] EDPS, « Towards a new digital ethics », *Opinion*, 4/2015, 2015 ; EDPS, Ethics Advisory Group, « Towards a digital ethics », *Report*, 2018. Le rapport est disponible à l'URL suivante : https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf ; High Level Expert Group on Artificial Intelligence, « Ethical guidelines for a trustworthy AI », projet de rapport publié le 18 décembre 2018, disponible à l'URL suivante : https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf. European Parliament Resolution, « Fundamental rights implications of big data », Sept. 2017 (P8_TA-PROV, 2017,

être close, loin de là, la réflexion sur les principes éthiques de dignité, d'autonomie et de solidarité ou justice sociale[103]. Que l'enjeu du numérique pour le développement de nos sociétés, de nos démocraties et des individus fasse l'objet, dans un premier temps, de discussions publiques multidisciplinaires et où se retrouvent des représentants des différents intérêts concernés et, dans un second temps, au niveau du Parlement. On ajoute, premièrement, qu'il importe que ces discussions soient éclairées par les travaux d'un Comité d'avis de *Technology Assessment*, comme l'est le STOA, au niveau européen[104] ; deuxièmement, que le thème de la vulnérabilité y soit explicitement abordé et qu'il soit clairement reconnu à la fois les vulnérabilités particulières de groupes identifiés, mais, au-delà, la vulnérabilité ontologique de tout individu vis-à-vis du numérique, y compris celle de l'identité humaine. Enfin, vu l'imprévisibilité des applications qui caractérise le développement des technologies du digital et leur ambiguïté, il serait sans doute utile d'appliquer le modèle réglementaire du bac à sable[105], qui autorise des expérimentations d'applications

---

0076) ; « Déclaration de Montréal pour une IA responsable », 2017, déclaration développée sous les auspices de l'Université de Montréal, disponible à l'URL suivante : https://www.declarationmontreal-iaresponsable.com/la-declaration ; « General principles of the IEEE's second version of ethically aligned design: A Vision for prioritizing human well-being with autonomous and intelligent systems », 2017, document disponible à l'URL suivante : https://ethicsinaction.ieee.org/ ; European Group on Ethics in Science and New Technologies de la Commission européenne, « Statement on artificial intelligence, robotics and autonomous systems », 2018, disponible à l'URL suivante : https://ec.europa.eu/info/research-and-innovation/strategy/support-policy-making/scientific-support-eu-policies/european-group-ethics-science-and-new-technologies-ege/european-group-ethics-science-and-new-technologies-ege-news_en ; enfin, le rapport de la CNIL de décembre 2017, « Comment permettre à l'homme de garder la main ? – Les enjeux éthiques des algorithmes et de l'intelligence artificielle », disponible sur le site de la CNIL.

[103] Sur ces trois principes, leur signification et leurs applications aux technologies du digital, lire Y. Poullet, *Éthique et droits de l'homme*, *cit.*, et les nombreuses références reprises.

[104] STOA (Science and Technology Option Assessment – Scientific Foresight Unit – European Parliament). Le STOA a analysé ainsi différentes technologies, comme le robot : « How will robots change our lives? New study on the ethics of cyber-physical systems 3 », rapport disponible à l'adresse suivante : https://epthinktank.eu/2016/06/30/how-will-robots-change-our-lives-new-study-on-the-ethics-of-cyber-physical-systems-published/ ou la *blockchain* : « How blockchain technology can change our lives », *Rapport*, février 2017, PE 581.948.

[105] Sur cette manière de procéder face à une innovation dont on a quelque peine à juger des risques et bénéfices, lire l'excellent texte de M. Finck, « Blockchain regulation », Max Planck Institute for Innovation and Competition Research, *Paper*, n° 17-13, 2017. Lire également les réflexions de J. Maupin, « Mapping the global legal landscape of blockchain and other distributed ledger technologies », CIGI, Center for International Innovation Governance, *Paper*, n° 149, Oct. 2017 : « *The term sandbox here takes its cue from the Financial Conduct Authority's (FCA's) recent initiative to set up a UK regulatory sandbox: a safe space in which fintech companies targeting UK markets can test out new technologies within a "light touch" regulatory environment under close government supervision and for a defined period*. » En langue française, mêmes réflexions, *in* N. Deviller, « Jouer dans le "bac à sable" réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne des blocs », *RTD com.*, 2017, p. 1037 et s.

technologiques, tout en les soumettant à un devoir d'évaluation et d'accompagnement par un comité reprenant les différents *stakeholders*, des personnes représentant non seulement les opérateurs et prestataires, mais également la société civile, l'Autorité de protection des données, les groupes de personnes vulnérables.

39. Les droits de l'homme – Une référence incontournable – Le fondement juridique de la protection de nos vulnérabilités est à trouver dans les droits de l'homme : ainsi, la liberté d'expression, la vie privée, la dignité humaine, l'égalité ont été évoquées comme droits fondateurs de la lutte contre les vulnérabilités. Ceci dit, il importe de souligner qu'il s'agit non de droits de l'homme affirmés solennellement comme des dogmes, mais, au contraire, comme l'incitation à rechercher toujours plus leur traduction effective, dans une perspective non point individualiste, mais bien, comme l'affirme Arendt[106], dans l'affirmation de son appartenance à la communauté. Au-delà, Lacroix et Pranchère[107] mettent en garde : il importe d'éviter de « basculer trop rapidement d'une présomption d'égalité à celle d'une capacité d'agir (*agency*). Il a peu à nous dire sur les conditions sociales, qui rendent possibles les revendications radicales qui forment le cœur du politique ». Ces auteurs se réfèrent à Mac Nay[108] et Castel[109] évoquant la vulnérabilité des personnes, rendant impossibles précisément leur capacité d'agir et leur participation à la mobilisation démocratique, et concluent : « Il faut bien être "protégé pour être autonome", et donc disposer d'un minimum de ressources pour être affranchi de l'obligation de vivre au jour le jour la journée et être en mesure de s'engager dans ces revendications de droits qui ne peuvent suffire à circonscrire l'espace démocratique »… « Un argument qui ne plaide certes pas pour l'abandon du vocable des droits de l'homme[,] mais pour la reconnaissance du fait que la revendication de droits doit s'insérer dans une réflexion d'ensemble sur la recomposition de l'action publique susceptible de garantir les capacités sociales et politiques des personnes concernées. » En d'autres termes, mettre les droits de l'homme au service d'une protection effective de nos vulnérabilités, rendre à chacun les conditions de son développement personnel, sa mise en capacité, son *empowerment* et, en particulier, refuser

[106] « Le concept des droits de l'homme ne peut retrouver tout son sens que s'ils sont redéfinis comme le droit à la condition humaine elle-même, qui dépend de l'appartenance à une communauté humaine, le droit de ne jamais dépendre d'une dignité humaine qui, si elle n'est pas garantie *de facto* par les autres hommes, non seulement n'existe pas[,] mais est le dernier mythe, vraisemblablement le plus arrogant que nous ayons inventé dans toute notre histoire », H. Arendt, « En guise de conclusion », *in Les origines du totalitarisme*, Coll. Quarto, Paris, Gallimard, 2002, p. 873.

[107] J. Lacroix et J.-Y. Pranchère, *Le Procès des droits de l'homme*, Paris, Seuil, 2016, p. 324.

[108] L. McNay, *The Misguided Serach for the Political*, Cambridge, Polity Press, 2014.

[109] R. Castel, « L'autonomie, aspiration ou condition », *in La vie des idées*, 2010, disponible à l'URL suivante : https://laviedesidees.fr/L-autonomie-aspiration-ou.html.

le mythe d'un dépassement de l'homme par la machine, voilà les défis que les technologies lancent à notre société démocratique… pour le meilleur ou pour le pire.