Numérique, droit et vulnérabilités

Poullet, Yves

Published in:
L'étranger, la veuve et l'orphelin...Le droit protège-t-il les plus faibles ? Liber amicorum Jacques Fierens

Publication date:
2020

Document Version
le PDF de l'éditeur

Numérique, droit et vulnérabilités[1]

Yves Poullet

Cher Jacques, je te propose de parcourir les relations entre trois concepts : le concept de vulnérabilité, celui de droit et, enfin, celui de numérique. Mon invitation entend poursuivre un dialogue que nous avons entamé depuis que tu nous as rejoint dans cette faculté de droit qui nous est chère. Tu y es venu fort d'une passion, celle de la défense des « sans voix » et des libertés. Tu leur as donné une place dans ce monde juridique créé sur la fiction de l'égalité *a priori* de tous. Tu leur as prêté ta voix. Ton talent d'orateur et de juriste a porté bien loin leurs revendications. Aujourd'hui, à ton combat, j'apporte ma modeste contribution. Il m'apparaissait en effet d'emblée que les applications d'un numérique de plus en plus ubiquitaire et « intelligent » non seulement risquent de renforcer les vulnérabilités traditionnelles mais surtout d'en introduire d'autres plus essentielles qui touchent tout être humain. Dans le même temps, il était indéniable que le numérique peut offrir à chacun la chance de dépasser nos 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 justice et précisément, à l'intérieur de celle-ci, des « faibles », des handicapés, des « exclus » et des « sans voix » ?

Le propos s'articule comme suit. Il s'agit, tout d'abord, de circonscrire ce qu'est la vulnérabilité (Section 1), avant de s'interroger sur les relations que traditionnellement le droit entretient avec la vulnérabilité et décrire les tendances nouvelles de cette relation (Section 2). On relate, ensuite l'ambiguïté de l'impact des applications numériques sur le sort des « vulnérabilités », et, au-delà, de la vulnérabilité humaine. Il s'agit par-là de 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 (Section 3), avant de conclure.

[1] Cet article est une version abrégée de la conférence donnée au colloque ESPHIM, *L'identité en question : entre parcours de vulnérabilités et chemins d'autonomie*, organisé à Namur les 23, 24 et 25 janvier 2019.

SECTION 1. – La vulnérabilité – un concept en quête de définition

« 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 ». Cette définition de sociologues belges[2] me paraît intéressante à divers titres. Elle définit l'individu non comme une entité en soi, un « sujet de droit » autonome, conscient, vu comme une réalité abstraite mais le conçoit comme une capacité d'action sur ce qui l'entoure, capacité que diverses contraintes intrinsèques à l'individu ou extrinsèques limitent voire flétrissent et ne lui permettent pas de réaliser pleinement. Comment, par ailleurs, ne pas voir dans cette définition une allusion à la théorie des « *capabilities* » développée par A. Sen[3] ? Cette théorie généreuse exige de l'État qu'il offre à chaque citoyen 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 un rôle actif de l'État, qui doit rendre possible cette maîtrise. 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'eux-mêmes dans un contexte où des choix, certes parfois limités mais pleins de signification, restent possibles.

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 handicapés mentaux ou physiques, les enfants, les personnes âgées...). La seconde, les *vulnérabilités extrinsèques* ou relationnelles regroupent d'autres catégories de personnes, qui soit pour des raisons financières (les « pauvres ») ou de position économique défavorable (les consommateurs) soit au regard de considérations sociales (les femmes, les étrangers, aujourd'hui les LGBT...) sont 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

[2] P. Brotcorne, L. Damhuis, V. Laurent, G. Valenduc et P. Vendramin, *Diversité et vulnérabilités dans les usages des TIC*, Gand, Academia Press, 2010, p. 63.

[3] A. Sen, *Elements of a Theory of Human Rights*, *Philosophy & Public Affairs*, 2004, n° 32, pp. 315 et s.

de notre condition d'être humain, fragile et souffrant. 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 vulnérabilité extrinsèque et, plus récemment, elle entend couvrir notre vulnérabilité fondamentale.

SECTION 2. – Le droit et la protection de la vulnérabilité : une question de sens

L'essence du droit est, comme l'enseignait Lacordaire, de soutenir le faible contre le fort : « 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 »[4]. Cette attention particulière du droit vis-à-vis de la vulnérabilité s'explique aisément. Le droit poursuit une œuvre de libération des individus, non seulement en proclamant les libertés individuelles mais en veillant à ce que la justice sociale et la dignité de chacun, au sens le plus noble du terme, rendent possibles le vécu et l'expression de ces libertés. Le devoir de l'État de veiller ainsi à la dignité et à la justice sociale peut même justifier des discriminations positives[5].

La Cour européenne de Strasbourg a ainsi maintes fois rappelé les obligations positives des États et l'effet horizontal qu'implique la proclamation des libertés[6]. La protection des vulnérables y trouve une 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 critique de citoyen ? Le même souci explique que chacun puisse s'exprimer dans sa langue et bénéficie de traduction, 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

[4] D. Lacordaire, « Du double travail de l'homme », 52e conférence de Notre-Dame du 16 avril 1848, in *Œuvres du R.P. Henri-Dominique Lacordaire de l'ordre des Frères prêcheurs*, Paris, Poussielgue frères, 1872, 9 vol., vol. IV, *Conférences de Notre-Dame de Paris*, t. III, *Années 1846-1848*, pp. 471-495.

[5] Parmi bien d'autres auteurs, on cite J. Rawls, *Théorie de la Justice*, Paris, Seuil, 1997.

[6] 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, n° 63, Bruxelles, Bruylant, 2005, pp. 27 et s.

des principes rappelés ci-dessus. N'y voit-on pas la source de l'obligation des administrations de se rendre accessibles aux handicapés, 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 étrangers. 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 »[7].

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 de leur jeunesse, leur faiblesse de caractère ou leur handicap mental (les fous, les prodigues, mais également, jusqu'à 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 liée à cette vulnérabilité intrinsèque, la loi a entendu protéger les patients, notamment par des obligations d'information et de plus grande transparence imposées 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 XX^{e} siècle a étendu à de nouvelles catégories, cette fois caractérisées par leur vulnérabilité extrinsèque due à leur situation de dépendance économique, leur appartenance ethnique, voire à leur mode de vie.

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, de législations plus transversales 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 l'article 5.41 du projet de Code des obligations, la notion d'« abus de circonstances » définie 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 »[8] ; de son côté, la loi du 26 novembre 2011 introduit dans notre

[7] Sur cette extension, Y. POULLET, *La vie privée à l'heure du numérique*, coll. des cahiers du CRIDS, n° 45, Bruxelles, Larcier, pp. 60 et s. et l'analyse des décisions de la Cour de Strasbourg à propos du concept de vie privée.

[8] *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 *Vunérabilités*

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, par un arrêt du 7 novembre 2013, justifie 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 de chacun »[9]. La nécessité de prise en compte de la vulnérabilité de chacun dans notre société moderne exige cette extension.

En quoi le numérique modifie-t-il la conception de notre vulnérabilité ? Le numérique, aujourd'hui et chaque jour un peu plus, se caractérise par la dimension ubiquitaire de son infrastructure, par la capacité quasi illimitée de ses capacités de transmission, de traitement et de diffusion, par le caractère de plus en plus intrusif de ses applications et, enfin, par 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 voire de déterminer nos comportements. C'est à ce risque commun à tout homme qu'en particulier les législations de protection des données à caractère personnel entendent répondre. Cette réponse s'origine dans l'élargissement du concept de vie privée. Au départ, conçue comme une protection d'un espace clos dont nous pourrions écarter autrui afin de pouvoir nous retirer en nous-mêmes, les exigences de notre capacité de développement, d'une société de l'information de plus en plus envahissante, ont conduit à élargir la notion de vie privée et à la concevoir tant comme un droit à la séclusion ou au secret que comme un droit à la maîtrise de notre « image informationnelle » ou, selon l'expression souvent retenue, comme le « droit à l'auto-détermination informationnelle », c'est-à-dire de pouvoir contrôler : Qui détient des informations à notre propos ? Lesquelles ? Quelle utilisation entend-il en faire ?

---

et droits dans l'environnement numérique (H. Jacquemin et M. Nihoul coord.), actes du colloque tenu à Namur le 14 octobre 2018, coll. de la faculté de droit de Namur, Bruxelles, Larcier, pp. 241 et s. ; dans le même ouvrage, lire également F. George et J.-B. Hubin, « La protection de la personne en droit des obligations », pp. 67 et s.

[9] Voy. sur cette décision, la disposition légale et le débat autour de cette disposition, N. Colette-Basecqz, « La protection pénale des personnes vulnérables dans l'environnement numérique », in *Vunérabilités et droits dans l'environnement numérique*, *op. cit.*, pp. 135 et s.

L'importance de l'enjeu du numérique pour nos développements personnels, nos libertés et notre dignité est devenue telle que les autorités européennes l'ont consacré, à l'article 8 de la Charte européenne des droits de l'homme et à l'article 17 du Traité de Lisbonne[10], 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 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. »

SECTION 3. – La vulnérabilité aux risques du numérique

Soyons de bon compte : 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, la personne handicapée se réjouira, lorsqu'il dialogue dans les réseaux sociaux, de ne pas être aperçue 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

[10] Ce droit constitutionnel se traduit dans le 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, 4 mai 2016, pp. 1-88. Pour plus de détails sur les différentes dispositions dudit RGPD, nous renvoyons le lecteur à l'ouvrage : C. DE TERWANGNE et K. ROSIER (dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, coll. Cahiers du CRIDS, n° 44, Bruxelles, Larcier, 2018.

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. Enfin, on souligne la promesse de l'Homme mieux soigné voire augmenté que nous promettent les implants corporels et les progrès de la discipline dite NBIC, qui combine les développements de la nanotechnologie, de la biologie, de la science de l'information et des neurosciences (*Cognition science*).

À cette vision très positive, s'opposent des perspectives plus pessimistes : celle de l'internaute faisant face au « *Big Brother* »[11] 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 du *Procès* de Kafka, d'un sujet affrontant une machine dont le fonctionnement opaque et sans logique l'empêche d'anticiper les conséquences des actes qu'il pose. On évoque six types de risques : celui né du déséquilibre entre les pouvoirs respectifs[12] des responsables des traitements, d'une part, de la personne concernée, d'autre part ; celui 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[13] ; celui, ensuite, de la « décontextualisation », à savoir la distance entre la finalité pour laquelle la personne concernée « émet » ses données et celle de leur utilisation par le responsable du traitement ; celui de l'*opacité* du fonctionnement tant des *terminaux* (notamment, les *cookies*, les RFID présents dans l'Internet des objets), des *infrastructures* (voir les « agents distribués » de l'Internet des objets, voire des algorithmes de « *deep learning* » utilisés[14]) ; celui du *réductionnisme*, c'est-à-dire la réduction de la personne concernée

[11] La complémentarité des visions orwellienne et 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 pp. 7 et s.

[12] D. J. Solove, « Privacy and Power : Computer Data Bases and Metaphors for Information Privacy », *Stanford Law Review*, 2001, vol. 53, n° 6, pp. 1393 et s.

[13] Grâce à ce qu'il est convenu d'appeler l'« *affective computing* ».

[14] Le danger de « conformisme anticipatif », c'est-à-dire de l'adoption par la personne concernée du comportement qu'elle croit attendu par le responsable du traitement, né de l'opacité de nos sociétés de l'information comme menace pour notre démocratie et notre liberté d'expression, est mis en évidence dès 1983 par le fameux jugement constitutionnel dans l'affaire du recensement.

aux données collectées et traitées qui définissent à elles seules son « profil » et permettent de prédire son comportement futur[15] ; celui, enfin, de l'abolition de la distinction entre sphère publique et sphère privée[16].

Les développements des applications de l'IA et l'existence de méga-données de plus en plus riches quantitativement et qualitativement font craindre ce que ma collègue A. Rouvroy appelle la « gouvernementalité algorithmique » : 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[17], de nos comportements futurs et les influencent voire les dictent. À travers les « *nudge*s »[18], 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

[15] À cause de la capacité croissante de nos systèmes et d'un Internet des objets toujours plus ubiquitaires, les données collectées à propos des événements même les plus insignifiants de notre vie se multiplient. Les systèmes d'information nous analysent à travers ces données qui réduisent à des données factuelles et à leurs combinaisons pas 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 en fonction de nos systèmes d'intelligence « artificielle » et en vue de finalités définies par ceux qui utilisent ces données, voire directement par le dispositif technologique.

[16] 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.

[17] Sur la question de biais souvent dus mais non uniquement à la subjectivité des concepteurs de systèmes d'IA, voyez l'article « Biais » dans Wikipédia : « Un biais algorithmique se produit lorsque les données utilisées pour entraîner un système 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, malgré la neutralité présumée des données ».

[18] « 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, v° « Nudge »).

des chances de réussir leur parcours scolaire ; à vous juges, les risques de récidive d'une personne auteur 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 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.

SECTION 4. – Le droit en réponse à nos vulnérabilités face au numérique

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.

§ 1. Numérique et exclusion

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 convoqué en 2003 par les Nations unies : « une ressource publique mondiale »[19]. L'affirmation répétée par nombre de textes internationaux[20] trouve écho même en Belgique : des études récentes montrent

[19] 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.

[20] Parmi ces organisations internationales, on cite la résolution du Conseil des droits de l'homme des NU 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 « [g]arantir la liberté d'accès à internet à un coût abordable pour toutes les catégories de population, sans discrimination ».

que 14 % de la population belge reste privée de connexion à l'Internet et les chiffres sont bien plus élevés quand on envisage les catégories de personnes plus vulnérables[21]. L'accessibilité des personnes handicapées à l'Internet est exigée par la Convention de l'Organisation des Nations unies (ONU) relative aux droits des personnes handicapées[22]. La réponse du droit à cette exclusion consiste en la proclamation de ce qu'il est convenu d'appeler un « service universel » qui, dans un monde de libre concurrence, oblige à garantir l'accès de tous à « un ensemble minimal de services déterminés à tous les utilisateurs finaux à un prix abordable ». À cet égard, progressivement se dégage de certains textes européens l'idée d'élargir cette notion de service universel, en particulier à certaines plateformes dites infomédiaires (*search engines*) ou de communication (réseaux sociaux). Ces plateformes opèrent comme des « *gatekeepers* » dans la mesure où, en situation de position dominante sur le marché, elles offrent un service essentiel à la population dans une société de l'information et de la connaissance. Elles pourraient dès lors voir leurs services régulés par l'autorité publique afin d'offrir des services *minima* (engins de recherche, accès aux réseaux sociaux). La réglementation de ces plateformes viserait la sécurité offerte[23], les critères de *ranking* et leur transparence[24], modes de contrôle de l'atteinte par leurs « clients à la propriété intellectuelle d'autrui »[25] voire la qualité de l'information véhiculée (dans le cadre de

[21] 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 des personnes vulnérables », in *Vulnérabilités et droits dans l'environnement électronique*, *op. cit.*, p. 40 et les références reprises).

[22] Art. 9(2), al. g), de la Convention relative aux droits des personnes handicapées du 13 décembre 2006. À cette difficulté d'accès à l'Internet, s'ajoutent depuis d'autres textes sur l'accessibilité cette fois à des sites web ou à des applications mobiles ou, pour les personnes en particulier mal voyantes, l'accès aux services et aux informations offerts sur le web (voy. notamment, la 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).

[23] Directive dite NIS sur la sécurité du réseau et des systèmes d'information (directive (EU) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.*, L 194, 19 juillet 2016, pp. 1-30).

[24] Règlement sur le traitement loyal des utilisateurs professionnels des plateformes en ligne en cours de discussion au Parlement européen. 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.*

[25] ... que l'autorité publique déléguerait à ces plateformes, ainsi dans la directive du 26 mars 2019 sur le droit d'autrui dans le marché unique numérique, l'article 17 réclame

la lutte contre les *fake news)*[26]. Autre extension de la notion de service universel, l'obligation faite aux autorités publiques de mettre à disposition du public l'information détenue par elles sous une forme telle que le contenu puisse être réutilisé facilement (voir le principe d'*open data* de la directive dite PSI ou le droit à la portabilité consacré notamment par le RGPD). Cette reconnaissance de plus en plus élargie du droit de chacun à pouvoir bénéficier de services numériques toujours plus nombreux s'analyse à notre point de vue non comme la reconnaissance d'un « nouveau » droit de l'homme mais comme une conséquence de l'obligation positive de l'État de favoriser la liberté d'expression et l'épanouissement de chacun, cette obligation est traduite par la consécration de services universels, aujourd'hui encore en nombre limité mais que la reconnaissance des besoins de tout individu de pouvoir participer à notre société du numérique doit progressivement élargir.

Au-delà de cet élargissement se pose, à l'inverse, la question de l'exclusion par le numérique de certaines catégories de personnes, soit parce que ces services, pourtant de première nécessité, ne sont plus accessibles que par le numérique, soit parce que l'accès à ces services numériques ou créés par le numérique n'est possible qu'à des conditions financières qui excluent nombre de citoyens. Le premier concerne notamment l'accès aux services publics et souligne les dangers du « *all digital* » de l'administration publique. Les citoyens sont invités de manière pressante voire tenus d'utiliser la voie électronique désormais privilégiée pour l'accès aux services de l'administration[27]. Cette digitalisation tous azimuts soulève une difficulté croissante d'accès pour certaines catégories de population d'accéder à l'administration[28]. Le second cas 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

---

des plateformes qu'elles prennent à la demande des ayants droit des mesures raisonnables, « appropriés et proportionnées » pour prévenir des violations des droits de propriété intellectuelle.

[26] Voy. 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*, COM/2018/236 final).

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

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

corporels dont le fonctionnement décuple la mémoire ou lutte contre la vieillesse. Des manipulations génétiques modifient le bagage génétique de l'individu. Ces possibilités nouvelles ouvrent à terme la voie à une humanité à deux vitesses par définition discriminante si leur offre est réservée à ceux qui financièrement peuvent se les « payer »[29].

§ 2. Numérique et agression

Internet et ses applications deviennent l'instrument d'une multiplication sans précédent d'agressions contre les individus. Le message sur l'Internet, outre qu'il présente une apparence de vérité et de sincérité de son contenu[30], semble certifier son origine[31] et permettre ainsi d'abuser de notre fragilité psychologique[32]. La technologie permet à quiconque de s'introduire au cœur de nos systèmes d'information[33], notre intimité[34] voire de notre corps[35]. Cette constatation des risques créés par le numérique d'exploitation de nos faiblesses voire le renforcement de celles-ci justifient la définition de nouvelles infractions[36]. Nous n'aborderons pas la longue liste des dispositions nouvelles de notre Code pénal mais nous attarderons plutôt à la façon dont le droit, au risque de nos libertés, et plus particulièrement le Code de procédure pénale, s'est emparé de la technologie pour s'attaquer à ceux qui utilisent celle-ci pour agir contre eux.

---

[29] 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 », disponible à l'adresse : http://ec.europa.eu/european_group_ethics/publications/docs/avis20compl_en.pdf.

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

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

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

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

[34] 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 qui peut être particulièrement dangereux et dommageable (exemple : accès au système de conduite d'une voiture intelligente).

[35] 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 ?

[36] Sur cette question, pour un exposé plus complet, lire N. Colette-Basecqz, « La protection des personnes vulnérables dans l'environnement numérique », in *Vulnérabilités et droits dans l'environnement numérique*, *op. cit.*, pp. 133 et s.

Dans quelle mesure l'autorité publique peut-elle utiliser les moyens que lui offre la technologie pour combattre la criminalité informatique ? La règle générale fixée par l'article 8, paragraphe 2 (atteintes possibles à la vie privée) de la Convention européenne des droits de l'Homme exige que les méthodes d'enquête respectent 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[37] ? 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[38] et précisées par la jurisprudence de la Cour[39]. Ainsi, l'utilisation des méthodes de surveillance des communications 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 d'exécution, *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 ? Par ailleurs, la mémoire de nos ordinateurs est sans limite et les risques de stigmatisations à vie de certaines personnes suspectées voire condamnées doivent être écartés par des législations adéquates.

[37] Ainsi, les opérateurs et fournisseurs de réseau de communication (les Proximus, Orange mais aussi Skype, Facebook, WhatsApp...) 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 en outre 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 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.

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

[39] Voy. notamment la décision de la Cour européenne des droits de l'homme 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 *L'Europe des droits de l'Homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019.

§ 3. Numérique, stigmatisation, normalisation et manipulation

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 « nus » 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 ses données ; voilà l'homme manipulé insidieusement ; voilà, enfin, l'homme « prévu », gouverné par la magie d'une intelligence artificielle.

Face à ces risques majeurs, quelle réponse le droit peut-il donner ? Comme annoncé et décrit plus haut, le concept de vie privée a donné naissance aux nombreuses législations de protection des données et plus récemment au Règlement général de protection des données (RGPD). Ce règlement est-il à la hauteur des risques dénoncés ? Le sentiment dominant en réponse à cette question est certes positif mais il est cependant difficile de ne pas noter quelques lacunes ou insuffisances de la protection accordée et surtout de dénoncer l'approche suivie. Quelques limites en ce qui concerne l'application du RGPD sont à craindre, en particulier face aux développements des systèmes d'intelligence artificielle dont chacun reconnaît qu'ils représentent le plus « haut risque » d'atteinte à nos libertés individuelles[40]. Surtout, le RGPD repose sur une conception purement individualiste de l'autonomie, que traduit notamment la primauté du consentement, et néglige les risques collectifs nés du traitement de données à caractère personnel. Ainsi, dans la mesure où mon profil se construit à partir de mes données autant que de celles d'autrui, la décision par ou envers moi a un impact sur la décision prise envers d'autres[41]. Lorsque

[40] Ainsi, il peut être relevé les difficultés suivantes d'application du RGPD : 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 (exemples : 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. Enfin, le RGPD réclame qu'information soit donnée sur la « logique suivie », la transparence des algorithmes de *deep learning* est difficile voire impossible, elle se heurte aux secrets d'affaires et droits de propriété intellectuelle.

[41] 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 profilé

mon GPS m'indique à moi comme à d'autres conducteurs bloqués dans un trafic routier une voie de traverse peu indiquée pour un trafic intense, il doit être tenu compte que ce cumul de décisions individualisées a un impact sur une question d'intérêt général. Cette conception individualiste de la protection des données se heurte au fondement du principe éthique d'autonomie qui reconnaît que l'individu est d'abord un être social et donc que la norme libre de son action doit être estimée à l'aune de l'intérêt général et du respect de la liberté correspondante d'autrui. Au-delà de cette 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 et qu'une approche collective est nécessaire.

§ 4. Numérique et discrimination

L'utilisation du numérique et de ses applications par les administrations, entreprises ou autres organismes multiplie les risques de discrimination. Le premier type de discrimination naît de l'impossibilité ou de 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, en particulier ceux de l'administration, représentent pourtant un passage obligé pour l'exercice de droits. D'autres discriminations trouvent leur origine dans le fait que des organismes utilisent l'information collectée pour connaître l'internaute-client et adaptent leur message au « profil » ainsi dessiné : réservant l'accès à certains ou différenciant les modalités de la transaction en fonction de ce profil[42]. Ce risque est encore accru par les possibilités qu'offre l'IA de construire de tels profils.

Les risques de discrimination peuvent concerner bien d'autres catégories de personnes que celles qui se rapportent aux données sensibles dont le RGPD et la directive établissent la liste : la race, les opinions politiques, religieuses, philosophiques, l'appartenance syndicale ou la santé. Des

calculé suite aux 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, Mr Poullet – ma prime d'assurance. Si j'accepte, ce traitement, qui trouverait sa légitimité dans mon seul consentement, dans la mesure où d'autres consentements individuels d'autres conducteurs « modèle » suivront, remet en cause un principe fondamental de l'assurance qui est celui de la mutualisation des risques.

[42] Il s'agit des techniques d'« *adaptative pricing* », développées par certaines 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.

systèmes d'IA permettent d'identifier des groupes de famille à risque en ce qui concerne l'éducation des enfants, des zones d'habitat où la population est criminogène et celles où la chance de réussite scolaire est la plus forte. Bref, les discriminations suivent des critères variés, parfois non prévisibles, liés à l'utilisation de vastes bases de données et des systèmes d'IA. Tous ces risques justifient un devoir de vigilance, non seulement lors de l'élaboration de tels systèmes (audit[43] et lutte contre les biais et erreurs, avec obligation de tests avant démarrage effectif), mais de manière continue tout au long de la vie du système. Il s'agit d'impliquer dans cette évaluation des comités d'éthique[44] et de susciter des discussions publiques sur la légitimité de ces systèmes d'aide à la décision dont le fonctionnement doit être dans toute la mesure du possible transparent afin d'être critiquable.

§ 5. Numérique et 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 ces deux problématiques et justifie leur analyse dans un propos 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 sa vulnérabilité[45].

---

[43] Tout récemment, suite au 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.

[44] 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 ».

[45] 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. Voy. également, N. Le Devedec, « Humanisme, transhumanisme : deux conceptions antithétiques de la perfectibilité humaines », in *Généalogies et nature du transhumanisme – État actuel du débat* (F. Damour, S. Deprez et D. Doat dir.), Québec, Liber, 2018, p. 33 : selon cette dernière, 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 ».

Les premières apparitions des robots nés de l'IA, présents en santé (robots chirurgiens, aide-soignant, prescripteur de médicaments ou de soins...), sur nos routes (voitures intelligentes) dans nos entreprises (*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, une protection non des robots mais bien de leurs concepteurs ou de ceux qui les mettent sur le marché.

Quant aux manipulations génétiques, elles appellent les considérations suivantes : « Si la matière est de l'information (codage), écrit le philosophe et homme de sciences Magnin[46], 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 ceux que la nature nous révèle ». Récemment, des chercheurs ont mis au point, sous le nom de CRISP-Cas-9, une méthode d'édition de gênes qui permet de couper des gênes dits « fautifs » et de les remplacer par d'autres gênes. 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. Plus radicalement, il s'agit, selon certains transhumanistes, de concevoir « toutes les entités biophysiques comme un donné fonctionnel, manipulable et améliorable *ad vitam aeternam* »[47].

Ces développements des technologies du NBIC et en particulier la manipulation du bagage génétique des individus entraînent des réactions juridiques timides du droit. En matière de droit de propriété intellectuelle, l'UNESCO rappelle certes que le patrimoine génétique est le patrimoine de l'humanité et ne peut faire l'objet d'aucune appropriation mais sa

[46] T. Magnin, *Penser l'humain au temps de l'homme augmenté*, Paris, Albin Michel, 2017, pp. 34 et 35.

[47] *Généalogies et nature du transhumanisme – État actuel du débat*, *op. cit.* p. 9. « Dans cette perspective, le transhumanisme est parfois présenté comme l'instrument d'une manipulation des imaginaires sociaux, mobilisée et financées par de grands acteurs économiques – GAFA, Microsoft, IBM, TESLA, *etc.* soucieux de créer des besoins et attentes pour des produits et services en préparation ».

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. De telles données, par ailleurs, appartiennent non à une personne mais à plusieurs personnes. Enfin, est notée la question de la 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 et justifie le renvoi des autorités à une réflexion éthique. Ainsi, l'UNESCO, face aux développements de la biotechnologie, estimait dès 2003[48] : « 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 qu'entraîne ce développement »[49]. Ce « contrefort éthique »[50] 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.

Conclusions

Le numérique constitue tout à la fois une chance pour notre développement personnel et, 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 les principes éthiques « *do good* »

[48] UNESCO, *Déclaration internationale sur les données génétiques humaines*, 2003.

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

[50] Sur ce « contrefort éthique » et sa nécessité face à la montée du mouvement « eugéniste », lire P. GIORGINI, *La tentation d'Eugénie*, Paris, Bayard, 2018, pp. 301 et s.

et « *do not harm* »[51]. Le développement du numérique doit être guidé par ces deux principes, celui de l'apport bénéfique et, à l'inverse, celui du 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. Le rappel de ces principes a toute son importance à propos du développement des technologies du numérique et de leurs applications. 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.

Ainsi, le slogan « *AI for good* » a trouvé, dans de nombreux forums, un écho et a provoqué la réflexion sur l'application des principes éthiques de dignité, d'autonomie et de solidarité ou justice sociale[52] au développement du numérique. L'enjeu du numérique et de chaque technologie « disruptive » pour le développement non seulement de nos libertés, de la justice sociale mais au-delà de nos sociétés, de nos démocraties et des individus doit faire l'objet de discussions publiques « *multistakeholders* » qui doivent éclairer, le cas échéant, les choix réglementaires. Le thème de la vulnérabilité doit y être explicitement abordé, 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 la question de l'identité humaine. Vu l'imprévisibilité des applications des développements technologiques et l'ambiguïté de ceux-ci, il serait sans doute utile d'appliquer la méthode réglementaire du « bac à sable »[53], qui autorise des expérimentations d'applications technologiques tout en les soumettant à un devoir d'évaluation et d'accompagnement.

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. Pour ce faire, et ton action

[51] Voy. à ce propos mais en matière de biotechnologies et biomédecine, les travaux de T. L. Beauchamps et J.-F. Childress, *Principles of Biomedical Ethics*, 3e éd., New York, OUP, 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* ».

[52] Sur ces trois principes, leur signification et leurs applications aux technologies du digital, lire Y. Poullet, *Éthique et droits de l'Homme dans notre société du numérique*, Bruxelles, Académie Royale de Belgique (à paraître) et les nombreuses références reprises.

[53] Sur cette manière de procéder face à une innovation dont on a quelque peine à juger des risques et bénéfices, lire, notamment, N. Deviller, « Jouer dans le "bac à sable" réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne des blocs », *R.T.D. com.*, 2017, pp. 1037 et s.

Jacques l'a bien souligné, il importe que ces droits ne soient pas compris comme des dogmes affirmés solennellement mais, au contraire, comme des instruments d'action, une incitation à rechercher toujours plus leur traduction effective, dans une perspective non point individualiste mais bien comme l'affirme Arendt[54], dans l'affirmation de l'appartenance de chaque individu à la communauté. Au-delà, et nous en revenons au propos placé en exergue de cette contribution, il importe d'éviter de « basculer trop rapidement d'une présomption d'égalité à celle d'une capacité d'agir (*agency*)[55]. Mac Neil[56] et Castel[57] évoquent cette vulnérabilité des personnes, qui rend impossible 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 et être en mesure de s'engager dans ces revendications de droits qui ne peuvent suffire à circonscrire l'espace démocratique ». En d'autres termes, mettre les droits de l'homme au service d'une protection effective de nos vulnérabilités, singulièrement accrues par le numérique, rendre à chacun les conditions de son développement personnel, sa mise en capacité, son *empowerment* et, en particulier, refuser le mythe d'un dépassement de notre vulnérabilité ontologique par la machine. N'est-ce pas le combat de toute ta vie et pas seulement de celle académique, cher Jacques ? Voilà, en tout cas, des défis que les technologies lancent à notre société démocratique... pour le meilleur et pour le pire.

---

[54] « 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 garantie 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*, « Quarto », Paris, Gallimard, 2002, p. 873).

[55] J. Lacroix et J.-Y. Pranchere, *Le procès des droits de l'homme*, Paris, Seuil, 2016, p. 324.

[56] L. McNay, *The misguided search for the Political*, Cambridge, Policy, 2014.

[57] R. Castel, « L'autonomie, aspiration ou condition », in *La vie des idées*, 26 mars 2010, disponible à l'adresse : http://www.laviedesidées.fr/L-autonomie-aspiration-ou.html. L'auteur ajoute : « 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 ».