Le numérique et le droit à la rencontre des personnes âgées

Yves POULLET

Professeur émérite à l'Université de Namur,
Professeur associé à l'Université Catholique de Lille

Résumé : Le numérique constitue-t-il, pour les personnes âgées, une opportunité d'ouverture au monde et de santé augmentée ou, au contraire, un facteur d'exclusion, de manipulation et de surveillance ? Comment le droit aborde ou devrait-il aborder ces défis ?

Mots-clés : coffre fort électronique, testament numérique, robot et surveillance

La réflexion qui suit doit être considérée plus comme une introduction que comme une conclusion. Le numérique est devenu une dimension de notre société et surtout de nos vies, en particulier celles de nos aînés. Pour ces derniers, les innovations technologiques dites disruptives, fruit du numérique, nous apparaissent plus subies que maîtrisées. Ne nions pas les multiples avantages liés à ces innovations, en matière de santé (recherche contre l'Alzeihmer, robots aide-soignant, suivi à domicile, ...) certes mais également en matière administrative (calcul de la pension, accès automatique à divers formulaires, octroi automatique d'avantages, ...) mais également dans la vie de tous les jours (domotique, participation à des réseaux sociaux, ...). Le numérique permet de lutter contre l'angoisse de la maladie et la solitude. A tous ces avantages, on opposera la difficulté de plus en plus ressentie par nos aînés de s'intégrer dans un monde à la technologie sans cesse évolutive et dont ils se sentent exclus, faute de pouvoir manipuler l'outil ; on soulignera également le sentiment de déresponsabilisation ressenti par eux, face à une ubiquité du numérique qui dictent leurs comportements, les contrôlent voire les manipulent. Face à l'ambivalence de cette double réalité, quel rôle le Droit peut-il jouer ? L'essence du Droit est certes de protéger le faible contre le fort (Lacordaire) mais il reste aux juristes, d'une part, à prendre conscience des risques nouveaux voire des nouvelles vulnérabilités encourus par les individus et, en particulier, les personnes âgées, d'autre part, à imaginer comment intervenir au service des personnes vulnérables face à une technologie aux applications foisonnantes,

complexes et largement opaques. Tel sera le propos de la première partie. La seconde partie aborde directement quelques questions particulières auxquelles invite la réalité des applications du numériques lorsqu'elles sont vécues ou non vécues par les personnes âgées : les questions de l'accès aux applications du numérique, des robots aide-soignants, du testament numérique et des enjeux de l'intelligence artificielle seront abordés. Que le lecteur puisse au terme de ces réflexions saisir l'ampleur du défi que le Droit se doit de relever et poursuivre nos considérations. Il s'agit en effet, pour le juriste, de permettre à nos aînés, grâce et non nonobstant les technologies, de continuer à vivre dignement et à apporter à nos sociétés le plein apport de leurs personnalités.

1 Vieillissement, vulnérabilités, droit et numérique

La démarche que nous proposons peut se résumer comme suit [1]. Quelle définition donner à la notion et dans quelle catégorie ranger la vulnérabilité de nos aînés ? Ces clarifications nous permettent d'envisager les aspects nouveaux engendrés par le numérique et après avoir défini ces aspects d'envisager d'abord le rôle traditionnel du Droit, à travers en particulier les Droits de l'homme et, ensuite, d'envisager comment des législations récentes ont abordé les risques nouveaux liés au numérique.

La vulnérabilité peut être définie comme l'« *expérience influençant négativement la capacité d'agir des individus, leur capacité à créer des situations socialement valorisantes pour s'intégrer pleinement dans la société* » [2] « *En invitant à considérer tout à la fois les « fêlures » et les « blessures » des individus, mais aussi leurs capacités et « capabilités » à les surmonter, il n'a d'intérêt que s'il invite, avec empathie, « à être attentif aussi bien à ce qui peut éviter la concrétisation de la potentialité qu'à ce qui est mis en œuvre pour panser la blessure » ; et non à rendre les individus responsables de leurs échecs, « double peine » dont sont accablés les plus démunis. Dit autrement, les facteurs de vulnérabilité sont trop souvent plus extrinsèques qu'intrinsèques et appellent donc fondamentalement une lutte politique sur les causes (des inégalités économiques, d'accès au savoir, territoriales, etc.) . . . Bref, il convient de ne pas se tromper de combat : c'est d'abord la société qui vulnérabilise les individus, et non l'inverse.* » [3] De telles définition et approche peuvent être rapprochées de la théorie des

1. Le lecteur trouvera bien d'autres réflexions dans l'article : Y.POULLET, « Le droit de la vulnérabilité au risque du numérique », Colloque ESPHIM : *L'IDENTITÉ EN QUESTION : ENTRE PARCOURS DE VULNÉRABILITÉS ET CHEMINS D'AUTONOMIE*, L. Rizzerio (*sous la direction de*), Namur, les 23, 24 et 25 janvier 2018, en cours de publication.

2. P. BROTCORNE, L. DAMHUIS, V. LAURENT, G. VALENDUC et P. VENDRAMIN, *Diversité et vulnérabilités dans les usages des TIC,* Gent, Academia Press, 2010, p. 64). Cf. dans le même sens, « La vulnérabilité recèle ainsi, selon Soulet, plusieurs caractéristiques. Elle est universelle d'abord, puisque nous sommes tous vulnérables ; elle est aussi potentielle (par-là possible, mais non certaine, concrétisation d'un risque), relationnelle et contextuelle (nous ne sommes vulnérables que dans un contexte donné, et en fonction des protections dont nous bénéficions), individuelle (elle ne frappe pas tous les acteurs de la même façon : face à une même exposition, certains seront plus touchés que d'autres) et enfin réversible (il est possible d'agir sur les facteurs et le contexte). L'exposition à la vulnérabilité est donc commune à tous les individus, mais non égale. Par son universalité, cette notion a dès lors pour propriété d'être bien plus englobante que toutes les catégories antérieurement utilisées pour désigner les individus en difficulté, tout en s'appliquant aisément à l'action catégorielle. » (A. BRODIEZ-DOLINO, « Le concept de vulnérabilité, article publié in '*La vie des idées',* 11 février 2016, disponible sur le site https://laviedesidees.fr/).

3. A. BRODIEZ-DOLINO, « Le concept de vulnérabilité, article publié in '*La vie des idées',* 11 février 2016, disponible sur le site https://laviedesidees.fr/

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

« *capabilities* » développées par SEN [4]. Cette théorie met l'accent sur les conditions qui effectivement rendent les citoyens capables dans le contexte socio-économique et culturel qui est le leur, de devenir (ou rester) *'fuller social persons, exercising their own volitions and to interact with – and influence – the world in which they live'* et envisage le rôle de l'Etat et donc du Droit au service du développement des capacités de chacun. La notion de vie privée [5] apparaît centrale dans cette volonté du droit de reconnaître cette exigence pour l'Etat de veiller à ce que chacun puisse développer ses capacités, 'forger son identité' [6] ou exercer son auto-détermination [7].

Traditionnellement, les personnes âgées sont considérées à la fois comme cumulant des vulnérabilités tant intrinsèques (celles dues aux déficiences physiques ou mentales, à la précarité financière de la personne elle-même), qu'extrinsèques (celles portées par le regard social sur la situation de certaines personnes en fonction de leurs opinions, de leurs choix de sexualité, de leurs nationalités, etc.). A ce cumul vécu par la personne âgée, s'ajoute ce qu'il est convenu d'appeler la vulnérabilité ontologique, qui caractérise notre essence humaine. Les anthropologues ont l'habitude de distinguer des deux premières 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 vulnérabilité extrinsèque et, plus récemment, elle entend couvrir notre vulnérabilité fondamentale [8]. On le verra, le droit du numérique s'intéressera tant à des catégories particulières de vulnérabilités qu'à celle ontologique de l'Homme.

4. A. SEN, 'Economics, Law and Ethics'. In *Against Injustice the New Economics of Amartya Sen.* Cambridge University Press, 2009 ; du même auteur, 'Human Rights and Capabilities'. *Journal of Human Development, 2005/* 6, no. 2, p. 155 à 166.

5. Sur la signification du concept de vie privée, lire notre essai, *La vie privée à l'heure du numérique*, Larcier, Coll. des cahiers du CRIDS n° 45, Larcier, Bruxelles, 2019.

6. C'est ainsi que dans un arrêt récent de 2017 (Arrêt BARBULESCU), la Cour européenne des droits de l'homme définit la vie privée.

7. On connaît le célèbre attendu rendu par la Cour de Strasbourg dans l'affaire PRETTY (Affaire PRETTY c. Royaume-Uni, Requête n° 2346/02, – 61, 25 avril 2002 (attendu repris par la Grande Chambre de la Cour dans l'affaire C. GOODWIN, décision du 12 juillet 2002, 90)) : « *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, 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.* »

8. « Applicable aux divers publics couverts par l'action (médico-)sociale, le terme doit sans doute aussi son succès à sa congruence aux évolutions de l'action sociale contemporaine, lesquelles reposent pour partie sur la conviction dialectique, au principe des politiques dites d'*empowerment* et « d'État social actif » progressivement mises en œuvre depuis la fin des années 1980, que nous sommes tous vulnérables, mais disposant aussi de ressources mobilisables pour retrouver davantage d'autonomie. La vulnérabilité pourrait dès lors être considérée comme une notion-pivot au sein d'un parcours individuel réversible fait d'instabilité du présent et d'incertitude de l'avenir, conduisant soit à l'autonomie au fil de l'*empowerment*, soit à l'assistance au fil de la dépendance. En invitant à articuler dans l'action sociale deux injonctions pour partie contradictoires que sont le souhait d'autonomie de la personne et les réalités de ses dépendances, elle est aussi en lien étroit avec les thématiques du *care*. » (P. VIDAL-NAQUET,. Le travail de care : tact, ruse et fiction', in Brodiez A., von Bueltzingsloewen I., Eyraud B., Laval C. et Ravon B. *Vulnérabilités sociales et sanitaires. Approches sociologiques et historiques,* Presses Universitaires de Rennes, p. 1-14, 2014).

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

L'essence du droit est 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* » [9]. Son intervention s'appuie tant sur les principes de justice sociale chère à Rawls, qui doit garantir l'accès de tous à ce qui est jugé nécessaire pour une vie digne dans une société, un droit à contenu variable – une discrimination positive en vue de l'égalité mais au-delà sur les droits de l'homme consacrés tant par la Charte de l'Union Européenne (traité de Nice de 2000) que de la Convention européenne de 1950. Ces textes européens entendent assurer à chacun la protection de ses libertés individuelles, afin de permettre à chacun de jouer pleinement son rôle dans la société. Nous reviendrons en particulier sur le rôle joué par le 'droit à la vie privée' dont découle, dans nos sociétés du numérique, le droit à la protection des données. Sans vouloir revenir sur des écrits précédents [10], la notion unifie 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. Sans doute, le Droit s'est d'abord préoccupé des vulnérabilités particulières qu'elles soient intrinsèques ou extrinsèques et pour ce faire a multiplié de nouvelles 'branches » du droit : le droit de la jeunesse, des étrangers, des minorités, des patients, etc. Il semble que désormais, le droit, sans renier cette approche des vulnérabilités particulières, s'intéresse également à une prise en considération de notre vulnérabilité ontologique [11]. Nous citerons ici deux textes belges : l'un en projet, l'article 5.41 du projet de code des obligations qui consacre la notion d'abus de circonstances, défini comme « *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.* » et l'autre en droit pénal qui, sous la notion d'abus de la situation de faiblesse d'autrui, vise au-delà des catégories classiques de vulnérabilités, toute situation caractérisée par l'exploitation de la situation vulnérable d'autrui peu importe le moyen, l'objectif ou l'existence d'une vulnérabilité particulière de l'individu même si cette dernière entraînera présomption de faiblesse [12]. Le numérique constituera souvent ce moyen : les capacités de profilage liées à l'utilisation de systèmes d'intelligence artificielle offrent à celui qui souhaite exploiter autrui, à la fois les instruments de connaissance de ce dernier mais également de prédiction de son comportement ; la présence des terminaux au cœur même des lieux intimes de chacun, l'interactivité du dialogue et la confiance liée à l'apparence de vérité de la parole délivrée par l'ordinateur expliquent ce fait.

Le numérique et en particulier les services offerts par les plateformes de communication et d'information offrent des applications ressenties comme une nécessité première

9. 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, p. 471-495.

10. Y. POULLET, *La vie privée à l'heure du numérique*, Larcier, Coll. des cahiers du CRIDS n° 45, Larcier, Bruxelles, 2019

11. A ce propos, lire en particulier les contributions de F. GEORGES et J.B. HUBIN à propos du droit des obligations (en particulier, p. 67) et de N. COLETTE-BASECQZ en droit pénal (en particulier, p. 151, publiées dans l'ouvrage collectif, *Vunérabilités et droits dans l'environnement numérique*, Actes du colloque tenu à Namur le 14 octobre 2018, ouvrage sous la coordination de H. JACQUEMIN et M. NIHOUL, Larcier, Collection de la faculté de droit de Namur.

12. La loi belge s'est fortement appuyée sur un arrêt de la Cour Constitutionnelle belge du 7 novembre 2013 qui estimait que : « *dans une société démocratique, la protection des personnes en situation de faiblesse constitue une condition essentielle pour protéger les droits fondamentaux de chacun* »

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

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, ils 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.

Dans le même temps, il est difficile de nier le risque d'augmentation de la vulnérabilité de nos aînés du fait de la numérisation de notre société. La complexité et la perpétuelle évolution du fonctionnement de nos terminaux, le coût d'accès à certains services mettent hors-jeu les personnes âgées et créent le risque de leur exclusion d'une société où l'utilisation du numérique est devenu une condition de participation à la vie sociale et à un certain nombre de services y compris administratifs : c'est le risque d'exclusion qui est ainsi souligné. L'opacité du fonctionnement de nos systèmes d'information a une conséquence : la manipulation insidieuse des internautes. Cette possibilité de manipulation existe d'autant plus que l'intelligence artificielle permet ce que ma collègue A. ROUVROY (2014) appelle la « gouvernementalité algorithmique » [13]. Comme nous l'avons déjà souligné, les profils créés constituent des outils non seulement d'analyse du passé mais du fait de la 'vérité' que ces profils prétendent refléter, une vérité, certes, purement statistique et non exempte de biais. Il est donc intéressant d'utiliser ces profils comme un instrument de prévision de nos comportements futurs et à travers ce qu'il est convenu d'appeler les '*nudges*'[14] de l'inciter aux comportements souhaités par le prestataire de services ou de produits sur Internet. Le phénomène des *Fake news* constitue une autre manifestation des risques de manipulations : Internet véhicule des rumeurs, des fausses informations et nombre de messages de propagande, le tout sous couvert d'apparente vérité. Les internautes, en particulier les personnes âgées [15], sont d'autant plus appelés à accorder de la crédibilité à l'information reçue qu'elle provient d'un 'ami' sur le réseau social et les incite

13. 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,* 2013.

14. « La théorie du Nudge (ou théorie du paternalisme libéral), nous explique Wikipedia, 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. »

15. « Les internautes âgés de plus de 65 ans ont tendance à partager plus de fausses informations sur Facebook que les utilisateurs plus jeunes, selon une nouvelle étude américaine ... *(Université de Princetown*), nous indique une dépêche de l'Association France Presse en date du 11/01/2019, qui précise, « *Mais ceux l'ayant fait avaient plus de chances d'être âgés. Les utilisateurs de plus de 65 ans ont partagé "près de sept fois plus d'articles" issus de médias relayant de fausses informations que les personnes*

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

à la communiquer aussi rapidement que reçue, à leurs propres 'amis'. La dimension virale de la circulation de l'information s'explique alors par la volonté d'amplifier la 'nouvelle' dans ces groupes partageant au départ les mêmes convictions. Un second risque lié au profilage est celui de la discrimination liée à l'âge, ainsi l'offre de logement peut écarter les personnes âgées, le repérage d'un passé médical stigmatise la personne âgée et l'écarte de certains services ou produits que l'on désire offrir aux seules personnes jeunes et bien portantes. L'ubiquité des systèmes d'information mais également le robot aide-soignant permettent de suivre, voire d'épier, chacun dans ses déplacements, ses habitudes, ses goûts voire ses émotions [16] et agitent le spectre du *big Brother,* le risque d'une surveillance continue et sans limites. Enfin, on évoque les risques liés à l'automaticité des prises de décision qu'en particulier, l'intelligence artificielle propose. Cette automaticité s'opère sur base de données prises auprès de nombre d'individus voire de données anonymes au sein desquels des algorithmes opéreront des corrélations non nécessairement transparentes y compris pour l'opérateur du système [17] et proposeront des décisions voire décideront, sans qu'il soit nécessairement possible et encore moins facile de discuter les 'vérités sorties de l'ordinateur' à l'objectivité et la neutralité apparentes. Les risques de biais discriminants dus tant à des données non adéquates ou de mauvaise qualité qu'à des erreurs ou de mauvais choix d'algorithmes sont souvent dénoncés. On souligne, en outre, la conséquence de ce recours qui conduit à la 'déresponsabilisation' [18] des décideurs mais également des 'bénéficiaires' des décisions de ces systèmes, qui se fieront unilatéralement sans plus de réflexion critique à ces décisions automatisées. On dénonce ainsi le risque d'un homme normalisé, déresponsabilisé, renforcé dans ses dogmes et opinions, manipulable, stigmatisé par son passé et constamment surveillé, bref d'un homme vulnérable face au numérique.

On le pressent, le numérique soulève des questions éthiques essentielles, en particulier lorsque ses applications concernent nos aînés. Il met en cause la dignité [19] 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 les personnes

âgées de 18 à 29 ans (le groupe le plus jeune étudié) et ce, indépendamment de leur appartenance politique ».

16. Grâce à ce qu'il est convenu d'appeler l'« *Affective Computing »,* traitement de l'information qui analyse des données biométriques (reconnaissance faciale, données de déplacements, étude de l'écriture) pour en déduire les émotions ou la psychologie d'une personne déterminée par exemple lors de l'entretien d'embauche, lors d'un interrogatoire policier ou de surveillance de la sécurité dans un aéroport.

17. C'est le cas des systèmes dits de '*deep learning'.*

18. A cet égard, les experts AI nommés par la Commission européenne relèvent 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* » (HIGH LEVEL EXPERT GROUP on AI, 2017 – High Level Expert Group *on* Artificial Intelligence, *Ethical Guidelines for a Trustworthy AI*, projet de rapport publié le 18 décembre 2018 disponible sur le site : https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf)

19. 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.

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

âgées 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'eux 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 âgées.

Le Droit et la reconnaissance par lui des libertés et des droits fondamentaux qu'il confère constituent une condition de la possibilité pour chacun de mener une vie morale et de poursuivre le bien. En particulier, les droits de l'homme fixent les conditions essentielles du développement de l'homme dans une société respectueuse des libertés, du développement de chacun et de sa dignité et on ne sera pas étonné dès lors de retrouver leur affirmation comme moteur du développement d'un numérique et d'une société du numérique bons et justes. Comme le notent très justement OST et van de KERCKOVE [20], l'éthique pénètre le Droit par le biais des droits de l'homme et lui assure ainsi sa 'légitimité'. Le RGPD [21], qui fait suite à différentes générations de législations de protection des données, est sans doute l'illustration la plus éclatante du rôle que le Droit entend jouer de manière à mettre le numérique au service de l'homme. L'accroissement de nos vulnérabilités causé par le numérique et amplifié par la vieillesse justifie les législations de protection des données et, peut-être, la décision de la Charte de l'Union Européenne des droits fondamentaux d'ériger ce droit à la protection des données comme un droit quasi constitutionnel [22]. L'analyse des cas particuliers le montrera amplement. Montrons combien quelques principes de cette législation et au-delà la conception large de la notion de vie privée par la jurisprudence tant de la Cour de justice de l'union européenne (CJUE) que celle de la Cour européenne des droits de l'homme (CEDH) traduisent les revendications éthiques évoquées.

Nombre de limites ou plutôt de balises au développement des applications du numérique peuvent être trouvées dans les principes mis en avant par cette jurisprudence et le RGPD. Le droit à la vie privée proclame le 'droit d'être laissé seul', ce qui peut vouloir dire le droit, en l'occurrence pour la personne âgée, de pouvoir se déconnecter des terminaux qui, en leur corps (les implants corporels), sur leur table de nuit mais également des robots qui l'entoure. Ce droit à la vie privée s'entend également de la condamnation d'une surveillance continue qui constitue une atteinte tant à la dignité qu'à notre vie privée. Le RGPD énonce nombre de principes qui serviront d'une part à assurer la transparence et la loyauté des traitements à travers les droits à l'information et ceux d'accès ou de correction, qui imposent l'obligation de définir de manière

20. Sur la légitimité et le rôle des droits de l'Homme dans la validité du droit, lire F.OST et M. van de KERCKOVE, *De la Pyramide au réseau,* Ed. Presses Universitaires Saint Louis, Bruxelles, p. 375 et s. ; p. 489 et s.

21. 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, 4.5.2016, p. 1-.88, disponible à* http://data.europa.eu/eli/reg/2016/679/oj. Pour un commentaire complet du RGPD, lire : de TERWANGNE et ROSIER (direction), 2018 – *Le règlement général sur la protection des données (RGPD/GDPR),* sous la direction de C. de TERWANGNE et K. ROSIER, Coll. Cahiers du CRIDS, n° 44, Larcier, 2018

22. C'est l'article 8 de la Charte qui reconnaît de manière distincte du droit à la vie privée, le droit à la protection des données.

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

précise, la finalité des traitements opérés et de ne retenir que les données pertinentes à l'égard de cette finalité. Cette double exigence doit être rappelée à l'heure où la collecte des données laissées tous azimuts par nos aînés poursuivent des finalités d'ordre divers, tant administratives que de soins à prodiguer mais également de contrôle et suivi de leurs comportements, sans omettre les buts de recherche scientifique. Le profilage de nos personnes âgées exige de vastes bases de données où sont entreposées des éléments dont la pertinence ne sera jamais appréciée qu'*a posteriori* et souvent, *deep learning* aidant, sans vraie transparence même aux responsables de traitement.

La qualité des données y compris leur mise à jour nécessite que le responsable de traitement se préoccupe des données fournies et, de manière générale de toutes celles utilisées. Cette précaution permettra d'éviter des biais ou erreurs dans les résultats fruit de l'ordinateur. Précisément à ce sujet, le RGPD reprend mais, sans doute doit-on le regretter avec moult exceptions, le principe de non suffisance du traitement automatisé comme seule base de décision. L'objectif est précisément d'entendre la parole et les arguments de la personne concernée. Le RGPD entoure de précautions particulières le traitement de données sensibles. On note que la notion de données sensibles ne s'attache plus nécessairement à la nature en soi de la donnée mais bien à la finalité poursuivie par le traitement qui révèle la sensibilité de la donnée. Ainsi, le fait d'habiter tel adresse peut révéler une donnée psychiatrique dans la mesure où l'adresse correspond à celle d'un hôpital psychiatrique pour personnes âgées. La notion de sécurité est centrale dans les lois de protection des données : elle commande la prise de mesures de sécurité techniques et organisationnelles pour veiller à l'intégrité, la confidentialité et la disponibilité des données. Elle oblige en cas de 'brèche de sécurité' le responsable à avertir les autorités de protection des données et les personnes concernées (ainsi, les habitants d'un home qui se serait vu hacker et ainsi 'voler' l'ensemble des données et diagnostics sur ses pensionnaires) voire lorsque le risque susceptible d'être subi par les personnes concernées est important, de procéder à une évaluation du risque qui doit être communiquée à l'autorité de protection des données. Le RGPD réclame que la technologie soit mise au service de la protection des données : ainsi sont énoncés les principes du « *Privacy by design »,* du *« Privacy by default » mais, également, de la « Data Portability ».* Enfin, on souligne que désormais le recours contre toute infraction ou violation du RGPD peut-être aussi bien collective qu'individuelle. Certaines de ces avancées du droit à la vie privée seront reprises lors de l'examen des questions particulières, qui suit.

2 De quelques questions particulières : Personnes âgées, Numérique et Droit

La seconde partie analyse la réponse du Droit à certains défis particuliers soulevés par le numérique en ce qui concerne les libertés ou plutôt les 'capacités' de la personne âgée. Le premier est crucial : le numérique exclut nombre de personnes âgées et les prive ainsi d'un moyen d'intégration à notre société devenue de l'information. Le deuxième recense quelques questions relatives à la maîtrise par le 'vieux souffrant' de son environnement médical numérisé. Le troisième étudie la réponse du Droit à la question délicate du devenir de notre image et de nos biens numériques au-delà de la mort par la création de l'institution du testament numérique. Enfin, les possibilités

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

de l'intelligence artificielle méritent lorsqu'il est question de personnes âgées quelques inquiétudes.

2.1 Le numérique et l'exclusion des personnes âgées

L'accès à l'Internet et l'usage des services offerts par l'Internet posent difficulté pour nos aînés. La complexité de l'outil, la constante évolution de celui-ci, l'absence de culture du numérique, le prix de certains des services y liés, le jargon utilisé autant de raisons qui expliquent la difficulté de ces personnes à pouvoir bénéficier de l'ensemble des avantages du numérique. Le Rapport du 27 septembre 2018 du CSA établi pour la Fondation EMMAUS [23] sur l'exclusion numérique des personnes âgées souligne : « *Il existe désormais un noyau dur d'exclus du numérique et les personnes âgées y sont majoritaires, tout particulièrement, les plus fragiles d'entre elles. Il y a urgence à ne plus laisser une partie importante de la population en situation d'exclusion et à ne pas laisser nos aînés devenir les laissés-pour-compte du numérique* ». Ce même rapport cite des chiffres alarmants : 21 % des personnes âgées de 60 ans et plus n'ont toujours pas Internet à leur domicile tandis que 44 % n'ont pas de smartphone ; seulement 54 % savent regarder des vidéos sur Internet ; seulement 43 % utilisent les réseaux sociaux et uniquement 35 % utilisent leur smartphone pour aller sur Internet.

Face à cette situation et le constat suivant lequel l'utilisation du numérique devient et est ressentie y compris par les personnes âgées comme une condition de leur intégration sociale, que faire ? Sans doute, le premier impératif est de consacrer le principe de l'accès aux services universels [24] de communication et d'information, non pas simplement comme l'accès à une infrastructure de qualité mais au-delà, comme l'accès de tous aux services y compris offerts par les plateformes de communication et d'informations reconnus comme d'utilité publique dans notre société de l'information. 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

23. CSA, 2018, *L'exclusion numérique des personnes âgées,* Étude réalisée par CSA pour les petits frères des Pauvres, financée par la Fondation des petits frères des Pauvres, 27 septembre 2018, disponible sur le site : petitsfreresdespauvres.fr/informer/prises-de-positions/contre-l-exclusion. On rapprochera de ces chiffres ceux publiés et largement commenté par le rapport du CREDOC (CREDOC, *Baromètre du numérique (4^e édition*), rapport disponible sur le site : https://www.credoc.fr/publications/barometre-du-numerique-2017-17eme-edition) « Ce rapport présente les résultats des questions insérées par le CGE, l'Arcep et l'Agence du Numérique dans la vague de juin 2017 de l'enquête du CRÉDOC sur les "Conditions de vie et les Aspirations" Il s'organise en trois chapitres :
1.Le premier chapitre s'intéresse aux principaux taux d'équipements (en téléphone fixe, téléphone mobile, ordinateur à domicile et connexion internet à domicile) et présente la proportion d'internautes dans la population française.
2.Le second s'intéresse aux usages, en regardant tour à tour : les usages sur téléphone mobile (navigation sur internet, envoi d'e-mail et téléchargement d'applications) et notamment les échanges texte par messagerie instantanée ; puis plus largement, les usages sur internet (achats ,réseaux sociaux, loisirs, formation et recherche d'emploi, démarches administratives...). Un focus est réalisé sur l'e-administration, il permet d'identifier les difficultés ressenties par les adultes face à l'administration en ligne et de dégager des pistes pour accompagner au mieux la dématérialisation des services publics. Le temps passé sur les écrans (télévision, internet) et la façon dont les Français ressentent le temps qu'ils consacrent aux différents médias (télévision, radio, internet, presse écrite ...) sont également analysés.
3.Le dernier chapitre fait le point sur la place d'internet dans la société actuelle. Les Français sont interrogés pour savoir si internet est nécessaire pour se sentir intégré dans la société française. ». Ce rapport nous servira dans l'analyse qui suit

24. « 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.

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

2003 par les Nations Unies : « une ressource publique internationale » [25]. L'affirmation se heurte à la constatation de ce qu'il est convenu d'appeler la fracture numérique [26] ou pour être plus juste le fossé numérique et ce nonobstant 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) [27], 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 Etats membres de l'ONU d'*« accroître nettement l'accès aux technologies de l'information et des communications et 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 ou plutôt dans le même esprit, au plan européen, une Résolution du Parlement de 2008 [28] 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. La réponse du droit consiste en la proclamation d'un « service universel » [29] qui garantisse, selon l'expression de la Directive européenne [30],

25. 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 Etats, 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.* »

26. « *Avec la Déclaration universelle de l'UNESCO sur la diversité culturelle de 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.* » (Richard Delmas, « Internet et la diversité, le souci du passage à l'éthique », *Revue française des sciences de l'information et de la communication*, 2, 2013, mis en ligne le 01 janvier 2013, consulté le 18 novembre 2018. URL : http://journals.openedition.org/rfsic/278 ; DOI : 10.4000/rfsic.278

27. 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).

28. 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 »

29. « 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.

30. 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 l'IBPT le soin de prendre des mesures permettant de rencontrer les besoins de *'groupes sociaux particuliers notamment les utilisateurs finals 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

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

la fourniture '*d'un ensemble minimal de services déterminés*[31] *à tous les utilisateurs finaux à un prix abordable'.*[32] Cette notion de service universel ne devrait-elle pas s'étendre aux services de communication (réseaux sociaux) et d'information (moteurs de recherches) offerts en quasi-monopole par certaines plateformes considérées comme les '*gatekeepers'* de la société de l'information ? Ces services ne doivent-ils pas être considérés comme nécessaires pour le développement de chacun à l'heure du tout numérique ?

L'électronique pénètre rapidement nos administrations et de plus en plus certains services administratifs sont accessibles par voie électronique (déclaration d'impôt, introduction d'une demande d'aide sociale ou de logement. . .). Pour des raisons évidentes, l'administration privilégie le dialogue électronique avec les citoyens et y attache certains avantages. Les rapports du CREDOC et EMMAUS notent la difficulté pour certaines catégories, en particulier les vieilles personnes d'utiliser la voie électronique, non tant par défaut de connexion que du fait de la difficulté de comprendre le langage souvent sibyllin et administratif utilisé par nos administrations[33], y compris lorsqu'il s'agit de l'exercice de droits sociaux[34] A cette difficulté croissante, on note

2016, COM(2016) 590 final adoptée par les Etats –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. »*

31. Y compris, l'accès aux sites Web (Cf. les travaux du W3C et la directive 2016/2102/UE du 26 octobre 2016) : '*Toute personne, quelles que soient ses capacités sur le plan physique, psychologique ou technique, doit être capable de percevoir comprendre, naviguer et interagir*').

32. 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 (2) alinéa g) de la Convention relative aux droits des personnes handicapées du 13 décembre 2006 demande aux Etats 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* ».

33. Cf. à ce propos le rapport du Défenseur des droits de 2017 (disponible sur le site https://www.publicsenat.fr/article/politique/rapport-du-defenseur-des-droits-toubon-pointe-le-traitement-des-etrangers-en) : « *Le numérique est souvent présenté comme une avancée. Une évidence et un progrès. Pour l'État, c'est aussi une source d'économie. Pour les administrés, il peut être source de difficulté et, pointe le rapport, du recul des services publics. « Le recul de l'accueil dans les services publics à l'ère de la dématérialisation est une énorme difficulté pour le public et particulièrement pour les personnes âgées, précaires, en situation de handicap ou étrangères. La confiance, qui est un élément essentiel de la relation entre les usagers et les administrations, s'est dégradée du fait de procédures administratives de plus en plus dématérialisées et complexes » souligne l'autorité, qui remarque « la réduction de l'accueil des usagers et la difficulté d'obtenir des informations par téléphone avec un renvoi automatisé quasi systématique* ».

34. MISSION SOCIETE du NUMERIQUE, *LE NUMÉRIQUE, MENACE OU OPPORTUNITÉ POUR LE RECOURS AUX DROITS SOCIAUX ? UNE ENQUÊTE EN HAUTS DE France,* Rapport publié le 13 novembre 2018, disponible sur le site : https://labo.societenumerique.gouv.fr/2018/11/13/numerique-menace-opportunite-recours-aux-droits-sociaux-enquete-aupres-personnes-agees-situation-de-precarite-hauts-de-france/.

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

deux réponses : la première est celle du 'coffre-fort numérique' installé dans les lieux d'aide sociale, service, qui doit permettre de faciliter et faire gérer par un tiers de confiance, l'identification, l'accès, le stockage électronique des documents administratifs d'un individu vulnérable, qui le souhaite [35] ; la seconde est, au contraire, le droit de préférer l'accès non numérique. En juin 2018, le Rapport du Comité Action Publique 2022 (CAP 22) [36] constate que « *la présence physique des services publics sur le territoire est une source de cohésion nationale et de réduction des inégalités. C'est la raison pour laquelle chaque citoyen doit pouvoir avoir accès (physique) à un agent (en chair et en os), à proximité de chez lui* » et préconise une réforme pour « *développer les lieux d'accueil uniques. Il s'agit de mettre en place un seul lieu pour tous les services publics.* » Quid de la gratuité de cette intermédiation ? Ainsi, la Poste française demande 50 euros pour une déclaration fiscale en ligne.

Ces diverses considérations nous amènent à émettre deux recommandations sur le développement de notre administrations électronique et ce, au profit des exclus du numérique. D'une part, il est important de respecter le choix des irréductibles réfractaires et leur garantir, ainsi qu'aux personnes dont les difficultés (handicap, maladie, illettrisme...) ne permettront pas l'accès au numérique, un accompagnement humain, pour ne pas créer d'inégalités dans l'accès aux droits ; d'autre part, il est nécessaire de renforcer le cadre juridique (*via* un système d'agrément) pour sécuriser tant les personnes qui demandent de l'aide que leurs « aidants numériques » concernant la protection des données, la confidentialité et les risques d'erreur.

2.2 Le numérique et la maîtrise de l'environnement de soins

Les outils et applications du numérique constituent de plus en plus un appui pour la délivrance des soins de santé et facilitent grandement la tâche de ceux qui les

35. Le coffre-fort numérique a été institué par l'article L. 137 introduit par la loi sur la République numérique qui insère cette disposition dans le Livre III du Code des postes et des communications. Cette disposition fait suite à une expérience menée par l'UNCCAS et la DGCS. Selon le texte de la loi, les finalités de ce coffre-fort seraient les suivantes :
« 1° La réception, le stockage, la suppression et la transmission de données ou documents électroniques dans des conditions permettant de justifier de leur intégrité et de l'exactitude de leur origine ;
« 2° La traçabilité des opérations réalisées sur ces documents ou données et la disponibilité de cette traçabilité pour l'utilisateur ;
« 3° L'identification de l'utilisateur lors de l'accès au service par un moyen d'identification électronique respectant l'article L. 136 ;
« 4° De garantir l'accès exclusif aux documents électroniques, données de l'utilisateur ou données associées au fonctionnement du service à cet utilisateur, aux tiers autres que le prestataire de service de coffre-fort numérique, explicitement autorisés par l'utilisateur à accéder à ces documents et données et, le cas échéant, au prestataire de service de coffre-fort numérique réalisant un traitement de ces documents ou données au seul bénéfice de l'utilisateur et après avoir recueilli son accord exprès dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
« 5° De donner la possibilité à l'utilisateur de récupérer les documents et les données stockées dans un standard ouvert aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert ou non aisément réutilisable qui peuvent être restitués dans leur format d'origine, dans des conditions définies par décret. « Le service de coffre-fort numérique peut également proposer des services de confiance au sens du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/ CE.
« Ce service de coffre-fort numérique peut bénéficier d'une certification établie selon un cahier des charges proposé par l'autorité nationale de la sécurité des systèmes d'information après avis de la Commission nationale de l'informatique et des libertés et approuvé par arrêté du ministre chargé du numérique.»

36. Disponible sur le site : https://www.gouvernement.fr/action/action-publique-2022-pour-une-transformation-du-service-public

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

gèrent, généralement des institutions hospitalières, d'EHPAD et à qui est sous-traitée leur gestion. Ces outils permettent de maintenir le patient à domicile, ce qui est souvent à considérer comme un bénéfice pour la personne vulnérable, en particulier les personnes âgées. On cite ainsi, les nombreux outils de télésurveillance, logés dans des bracelets électroniques de manière à pouvoir facilement géolocaliser le patient et lui permettre de lancer une demande d'intervention, les piluliers intelligents, les outils de télédiagnostic (capteurs de température, de tension, etc.) ou les '*quantified self'*. Ces derniers temps, on a vu apparaître des robots aide-soignants, capables de prodiguer des soins adaptés aux besoins du patient et de répondre à ses demandes.

Ces outils et applications nécessitent dans leurs déploiements un respect scrupuleux des législations de protection des données et leur agrément comme dispositifs médicaux [37].

Nous parlerons peu du second type de réglementation mais nous nous concentrerons sur le premier et relèverons quelques points en les appliquant au suivi des personnes âgées.

— Selon le RGPD, le consentement du patient doit, dans toute la mesure du possible, être libre, spécifique, informé, univoque et, s'agissant de données de santé, explicite. Cette exigence n'est pas simple à rencontrer surtout lorsque le patient âgé est incapable d'exprimer sa volonté. On peut certes invoquer avec prudence d'autres causes de légitimité du traitement des données : l'intérêt vital, la nécessité tirée de la relation thérapeutique. On peut surtout réclamer l'institutionnalisation légale de la 'personne de confiance', choisie par la personne qui sent ses capacités s'affaiblir et souhaite ainsi pouvoir déléguer l'expression de son consentement.
— La donnée de santé est largement définie par le RGPD, mais peut-on y ranger des données issues de traitements à but non thérapeutique, qui constituent un simple confort aidant certes la personne âgée à se sentir mieux et en sécurité mais non destinée à des soins ? Par ailleurs, la distinction entre données de santé et données autres n'est pas simple. Une donnée de géolocalisation qui indique la position d'une personne qui nécessite des soins urgents n'est pas en soi une donnée de santé mais le devient dans le contexte du suivi d'un patient.
— Le RGPD exige que les traitements de données médicales soient opérés sous la surveillance d'un professionnel de santé, voire d'une « équipe de soins ». Ce terme _« [désigne] un ensemble de professionnels – et pas seulement de professionnels de santé – [...], ce qui permet un partage d'information_s ». Ce point est important dans la mesure où nombre d'applications de suivi à distance de santé sont gérées par des entreprises offrant des services d'alerte et qui doivent être considérés comme sous-traitants avec toutes les implications que le RGPD réserve à cette catégorie et en particulier aux obligations de ces derniers et des responsables de traitements vis-à-vis d'eux.

37. Cf. le RÈGLEMENT (UE) 2017/745 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, JOUE, 5 mai 2017, L 117/1

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

— Enfin, les institutions qui mettent en place seules ou ensemble de telles applications devront le cas échéant nommer un détaché à la protection des données et, dans la mesure où le traitement opéré constitue au vu de la nature des données traitées un 'risque élevé' pour les personnes concernées, procéder à une évaluation de l'impact en matière de vie privée. [38]

Avant d'aborder deux cas particuliers de suivi des personnes à distance et sans présence d'un agent personne physique, à savoir : le bracelet et le robot électroniques, une dernière réflexion à laquelle nous invitent deux psychologues du vieillissement, Van der LINDEN et JUILLERAT [39] : *« en l'absence d'une approche préventive et sociale du vieillissement (nous ajouterions en l'absence d'une « approche globale » de la personne âgée), les dispositifs de détection (téléassistance, bracelets de localisation, capteurs de toutes sortes) peuvent conduire, sous couvert de gestion des risques, à une surveillance permanente, une déresponsabilisation, une anxiété et une dépendance aux équipements (conduisant à davantage d'isolement et d'enfermement), ainsi qu'à une atteinte à la dignité des personnes et au sentiment de contrôle de leur existence ».* Cette réflexion rejoint notre remarque initiale sur la déresponsabilisation tant des personnes âgées que de ceux qui les entourent de leurs outils électroniques : elles appellent les recommandations suivantes : premièrement, concevoir des aides technologiques qui fournissent un appui à l'autonomie et qui permettent au maximum à la personne d'agir par elle-même face à ses difficultés, sans dépendre d'une intervention externe ; en second lieu, procéder sans doute à l'aide d'une discussion publique entre tous les porteurs d'intérêt (les professionnels de santé, les autorités de protection des données, les représentants des personnes âgées, les représentants des institutions de soins) à un arbitrage nécessaire entre, d'une part, la sécurité des patients et la responsabilité encourue par les institutions de soins (arguments avancés par les institutions de soins) et l'autonomie et la dignité de l'individu (leur responsabilisation). Ce débat est urgent [40] et nécessite d'être mené avec nos aînés, sous peine pour eux de subir la technologie et non de la maîtriser.

Le bracelet électronique et autres dispositifs de surveillance électronique ont fait l'objet de recommandations de la CNIL [41]. D'emblée, la CNIL refuse un système de surveillance continue et généralisée à l'ensemble d'une population, par exemple les résí-

38. RGPD art. 35 : « *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, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* »

39. M. Van der LINDEN et A.C. JUILLERAT, « Les personnes âgées et les nouvelles technologies, 6 octobre 2010, article disponible sur : http://www.mythe-alzheimer.org/article-les-personnes-agees-et-les-nouvelles-technologies-58960857.htm. Cet article a depuis fait l'objet de développements, lire M. Van der LINDEN et A.C. JUILLERAT, *Penser autrement le vieillissement*, Bruxelles, Mardaga, 2014.

40. Les deux auteurs cités à la note précédente montrent qu'il n'existe aucun consensus concernant une contribution, éthiquement acceptable, des technologies de surveillance à la qualité des soins et interventions proposées aux résidents. Ils indiquent également en quoi la question éthique est peu élaborée et aussi en quoi le point de vue des résidents est largement négligé. En fait, quand il y a débat, il se focalise essentiellement sur l'acceptabilité morale des effets des technologies de surveillance, quand il existe un conflit entre les intérêts de l'institution et les intérêts des résidants. Du point de vue de l'institution, on constate que la sécurité est le facteur clé qui conduit à décider de l'utilisation de ces technologies. Les auteurs en appellent à davantage de réflexion théorique et de recherche empirique (incluant le point de vue des résidents) sur ces questions.

41. Recommandation en date du 24 juillet 2013

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

dents d'une EHPAD et insiste sur la nécessité d'un examen de proportionnalité entre les besoins de surveillance révélés par l'état de chaque personne âgée et l'ampleur du contrôle et suivi. Cet examen doit, dans toute la mesure du possible, être opéré après avoir sondé les volontés et le cas échéant les réticences de chaque personne âgée. « Une telle décision pourrait s'appuyer sur un avis médical pris après une évaluation collégiale et pluridisciplinaire menée par l'équipe qui prend en charge la personne et donner lieu à des réévaluations régulières ». La CNIL insiste sur le droit à la déconnexion et souligne la nécessité d'une sécurité des systèmes d'alerte (fiabilité des dispositifs et sous-traitance agréée). La possibilité à travers ces dispositifs de surveiller l'activité des salariés et des aide-soignants mérite une information de ces derniers et leur droit à être consultés.

Les capacités des robots aide-soignants soulèvent des questions bien plus complexes encore [42]. Son indiscrétion, y compris le suivi de la personne aidée dans les lieux et l'accès aux conversations les plus intimes, est nécessaire si le patient souhaite disposer d'une aide tant soit peu personnalisée. Sous réserve de ce que nous dirons à propos de l'intelligence artificielle (*infra*, n° 21 et s.), il est patent que le fonctionnement du robot se nourrit de cette masse de données collectées afin d'y opérer les corrélations significatives. On s'inquiète dès lors du respect du principe de proportionnalité, affirmé par le RGPD, principe qui commande au responsable du traitement de ne traiter que les données pertinentes, nécessaires à assurer la finalité du traitement. La question de la collecte de données concernant des tiers (les infirmières, les proches de la personne âgée) pose le problème de leur acceptation de cette collecte des données dont le résultat du traitement pourrait leur être opposé. Que se passe-t-il lorsque la personne âgée souhaite que le robot soit déconnecté ? A-t-elle, la personne âgée le droit de l'exiger ? Si oui, que deviennent les données stockées par le robot ? Comment va s'exercer le droit d'accès du 'bénéficiaire' des soins du robot [43] ? Lors de leurs réflexions éthiques sur les robots, certaines commissions ont exigé que les robots ne soient pas trop humanoïdes, de telle sorte que la confusion entre un être humain et un outil artificiel comme le robot soit impossible [44] Peut-être, cette interdiction néglige-t-elle la vertu d'empathie qui peut exister entre le vieillard et son robot dans le contexte de solitude que celui-là peut vivre. Enfin quelle sera la responsabilité du constructeur en cas de dysfonctionnement du robot (par exemple, le robot frappe la personne âgée), sachant que ce dysfonctionnement peut-être dû au mauvais fonctionnement des algorithmes conçus par le constructeur ou concepteur du logiciel, à la mauvaise qualité des données

42. *Cf.* notamment, les réflexions du Groupe européen d'éthique des sciences et des technologies nouvelles, in *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*. 2018, Bruxelles, Commission européenne, disponible à l'adresse suivante : https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.

43. Sur toutes ces questions, lire l'excellent article d'A.DELFORGE et L. GERARD, « Notre vie privée est-elle réellement mise en danger par les robots ? », in *L'intelligence artificielle et le droit,* sous la coordination d'H.JACQUEMIN et A. de STREEL, Coll. Cahiers du CRIDS, n° 41, 2017, p. 143 et s.

44. Ce principe de 'non confusion' interdit toute utilisation non transparente des technologies pour faire croire artificiellement à l'action d'une personne, telle que stigmatisée par la Déclaration de Montréal (Principe d'intimité et de vie privée, n° 8) : « *L'intégrité de l'identité personnelle doit être garantie. Les SIA (Systèmes d'intelligence artificielle) ne doivent pas être utilisés pour imiter ni modifier l'apparence physique, la voix et d'autres caractéristiques individuelles dans le but de nuire à la réputation d'une personne ou pour manipuler d'autres personnes."* DECLARATION de Montréal : « *Pour une IA responsable* », Déclaration développée sous les auspices de l'université de Montreal (2017) disponible sur le site : https://www.declarationmontreal-iaresponsable.com/la-declaration.

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

introduites mais également aux apprentissages de la machine au hasard des situations rencontrées auprès de l'utilisateur ?

Au-delà de ces deux outils envisagés particulièrement, qu'en est-il des systèmes mis en place par des institutions de soins et utilisant divers instruments de collecte de données, caméras de vidéosurveillance, bracelets électroniques, sols intelligents, robots-animaux ou aide-soignants ? La crainte d'un sentiment de surveillance continue et d'absence totale d'intimité est dénoncée, plus encore, si les divers instruments de collecte sont interconnectés et, à la limite, assurent ainsi une surveillance globale du comportement des hôtes de l'institution. Sans doute, est-il utile de rappeler le principe énoncé par la loi du 2 janvier 2002, article L.311-3 du Code de l'action sociale et des familles : *« L'exercice des droits et libertés individuels est garanti à toute personne prise en charge par des établissements et services sociaux et médico-sociaux. »* On évoquera ainsi la nécessité de garantir la liberté de déplacement, celle d'expression et d'opinion comme celle du droit à la vie privée et en particulier le « droit à être laissé seul ». On regrettera que le droit à la dignité qui implique précisément une absence de surveillance globale n'ait point été rappelé par ce texte fondamental.

La délibération n° 2016-094 du 14 avril 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi des personnes handicapées et des personnes âgées (AU-047) rappelle les finalités 'autorisées' de mise en place de tels systèmes [45]. Il s'agit d'améliorer la sécurité des 'clients' et d'assurer un meilleur suivi des soins à prodiguer aux personnes de l'institution. Il ne peut être question par ces systèmes de prévenir des vols ou dégâts matériels. La finalité de surveillance du personnel doit faire l'objet d'une décision prise après concertation avec le personnel concerné. A titre liminaire, la commission rappelle que des données à caractère personnel ne peuvent être collectées que si elles sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie. L'ensemble des données n'ont pas vocation à être systématiquement recueillies et moins encore conservées. Seules les données strictement nécessaires à la mise en œuvre du suivi social et médico-social de la personne concernée, ou de son représentant légal, peuvent faire l'objet d'un traitement. Les tiers en particulier les proches qui visitent un ami ou un parent aîné doivent être avertis des mesures de surveillance mises en place (vidéosurveillance, enceintes, robots,...) En conséquence, le responsable de traitement doit être en mesure de justifier [46] du caractère nécessaire et proportionné des données à caractère personnel pour les besoins du travail et des soins fournis. Les questions de sécurité et de pseudonymisation des données, de même

45. Voilà une liste partielle : « Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes dites 'vulnérables', en qui concerne la collecte de données sensibles et traitements « de santé » mis en œuvre par les établissements de santé (hôpital, CHU, cliniques, etc.) :
- dossier « patients » ;
- algorithmes de prise de décision médicale ;
- dispositifs de vigilances sanitaires et de gestion du risque ;
- dispositifs de télémédecine ;
- gestion du laboratoire de biologie médicale et de la pharmacie à usage intérieur, etc.
Traitements portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ou par un établissement d'hébergement : .... »

46. On retrouve là le principe d'*accountability'* affirmé depuis par le RGPD (article 5. 2.). La délibération est d'ailleurs explicitement présentée comme une anticipation de l'application des dispositions du RGPD, alors déjà bien connues pour l'essentiel.

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

que le rappel du secret professionnel par le personnel de l'institution, sont soulignés et une évaluation des risques sur le modèle exigé par l'EDPB [47] sur base des exigences du RGPD (article 35 et s.) est réclamée.

Quelques recommandations émanent de cet ensemble de considérations : la première concerne l'encouragement à définir contractuellement entre l'institution et son 'client', de rédiger ce qu'il est convenu d'appeler un contrat de séjour et de règlement intérieur : « *On a parfaitement le droit de mettre en place des sols intelligents, de la vidéosurveillance dans les parties communes. Mais il faut l'inscrire dans le règlement intérieur, dans lequel le mode de fonctionnement de l'établissement est opposable aux résidents* ». En deuxième lieu, on laissera des zones de liberté, c'est-à-dire sans aucune surveillance. En troisième lieu, la procédure d'évaluation des risques doit être l'occasion pour les institutions d'un débat ouvert pour fixer la juste balance entre l'intérêt des responsables de traitement à limiter leur responsabilité en cas de survenance d'un incident par non détection d'un problème de santé et non intervention suffisamment rapide et la nécessité de préserver au maximum l'autonomie et la dignité de la personne concernée.

2.3 Le testament numérique

L'article 63 de la loi LEMAIRE sur la République numérique, qui attend toujours son décret d'application, ajoute un article 40-.1. à la loi Informatique et Libertés : « *Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières* » [48]. La motivation de cette innovation [49] répond à une double préoccupation bien réelle : la première concerne notre vie privée.

47. Sur l'obligation de "Privacy Impact Assessment" (PIA) requis et encadré par les articles 34 et s. du RGPD, lire l'excellent article de F.DUMORTIER, "La sécurité des traitements, les analyses d'impact et les violations de données", in Le RGPD, Analyse approfondie, C. de Terwangne et K. Rosier (eds), Cahier du Crids, No. 44, Bruxelles Larcier, 2018, p. 143 à 255 (en particulier, les pages 197 à 222) et outre les lignes directrices du Groupe de l'article 29 : Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679WP. 248, en date du 4 octobre 2017, disponibles sur le site de la CNIL à l'adresse : wp248_rev.01_fr (cnil.fr) et, plus récemment, la Recommandation 01/2019 sur le projet de liste du superviseur européen de la protection des données concernant les opérations de traitement soumises à l'exigence d'une étude d'impact sur la protection des données (article 39.4 du règlement (UE) 2018/1725)

48. « Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.
« Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation. »

49. A noter la reconnaissance également aux Etats Unis suite aux travaux de l'Uniform Law Commission. « *The Uniform Law Commission recently concluded its annual meeting where the commissioners approved 5 new acts including one on electronic wills... UETA and E-SIGN both contain an express exception for wills, which, because the testator is deceased at the time the document must be interpreted, are subject to special execution requirements to ensure validity and must still be executed on paper in most states. Under the new Electronic Wills Act, the testator's electronic signature must be witnessed contemporaneously (or notarized contemporaneously in states that allow notarized wills) and the document must be stored in a tamper-evident file. States will have the option to include language that allows remote witnessing. The act will also address recognition of electronic wills executed under the law of another state. For a generation that is used to banking, communicating, and transacting business online, the Uniform Electronic Wills Act will allow online estate planning while maintaining safeguards to help prevent fraud and coercion.*" (https://lawprofessors.typepad.com/elder_law/2019/07/uniform-law-commissioners-approve-new-act-on-electronic-wills.html.)

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

Les lois de protection des données ne protègent pas au-delà de la mort, c'est dès lors avec appréhension que je vois confier à l'inconnu les secrets confiés à l'ordinateur (messages e-mail, messages échangés sur les réseaux sociaux, images voire photos intimes confiées à l'ordinateur) ou des données plus triviales mais qui révèlent un aspect de ma personnalité (liste de contacts, consommation d'électricité ou relevé d'une facture, etc.). Cet inconnu peut être un proche ayant saisi ou connaissant mon mot de passe, mon employeur, l'opérateur du service de messagerie, du cloud où les données de mon smartphone ou de mon ordinateur voire de mon robot. La seconde est plus accessoire et s'attache à la valeur patrimoniale des biens immatériels présents sur mon ordinateur ou mes terminaux. Ne pensons pas simplement aux manuscrits inachevés laissés sur l'ordinateur ni aux droits que j'aurais pu toucher sur base de mes droits d'auteur mais bien plutôt aux copies de films obtenues sous licence, à l'enregistrement de mes musiques préférées ou à des abonnements m'offrant le droit à tel ou tel avantage sonnant et trébuchant.

Le testament [50], toujours révocable, consiste en la désignation d'un tiers de confiance, un mandataire à l'exécution des directives. Ce mandat est d'ordre public et prévaut sur toutes les dispositions insérées dans les conditions générales que le testateur pourrait avoir signé avec son prestataire de services. On sait en effet que ces prestataires se déclarent volontiers en droit de gérer les 'comptes' du défunt ouvert auprès d'eux [51]. Désormais leur incombe un devoir d'informer leurs 'clients' : « Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne ».

50. La loi prévoit en cas d'absence de testament numérique : « *En l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés à la présente section dans la mesure nécessaire :*
- à l'organisation et au règlement de la succession du défunt. A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ;
- à la prise en compte, par les responsables de traitement, de son décès. A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.
Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en application du troisième alinéa du présent III. »

51. Un article récent récapitulait comme suit les dispositions trouvées chez les opérateurs et prestataires les plus utilisés : « Selon la Commission nationale informatique et libertés (CNIL), un profil Facebook sur 100 appartiendrait à une personne décédée, soit 13 millions de profils dans le monde. En attendant, Twitter, Snapchat et LinkedIn peuvent supprimer les comptes d'une personne disparue à la demande d'un proche. Seule condition : il devra justifier de la mort en fournissant un certificat de décès. Sur Instagram, vous pouvez de votre vivant désigner une personne qui pourra demander la clôture du compte ou demander à le passer en compte "de commémoration". Ainsi, vos photos resteront visibles, mais plus aucune interaction sur votre profil ne sera possible. Sur Facebook, vous pouvez également choisir un légataire en indiquant son nom dans les paramètres du réseau social qui aura pour mission de gérer votre page commémorative pour permettre à vos proches de continuer à laisser des messages sur celle-ci. Google propose quant à lui un gestionnaire de compte inactif appelé "Inactive Account Manager" afin de gérer de son vivant toutes les données liées pour l'ensemble des services Google tels que Gmail, You Tube, Google Drive, Google+, etc. une fois que celui-ci sera inactif. Dans le cas où le défunt n'a pas laissé d'instructions, il s'engage à collaborer avec les familles afin de clôturer les comptes en ligne de ce dernier avec possibilité de récupérer certains contenus issus des comptes. Apple et Microsoft semblent se différencier quant aux données numériques possédées par l'utilisateur. Concernant Apple toutes les données achetées par le défunts (films, musiques, apps. . .) ne peuvent être léguées ou données. »

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

2.4 Les logiciels d'aide à la décision et en particulier d'intelligence artificielle

La puissance des logiciels d'aide à la décision, voire de décision, est telle que, tant les pouvoirs publics que ceux privés, sont tentés d'y recourir de telle manière que la décision soit proposée par l'ordinateur, voire décidée par ce dernier. L'ordinateur et son 'intelligence' tantôt donnent à ces pouvoirs l'illusion d'une décision parfaitement objective et neutre loin des préjugés qui habitent un décideur humain, tantôt permettent, en particulier aux entreprises privées de sélectionner une clientèle idéale et, le cas échéant, en fonction des profils des personnes de sélectionner les 'bons' profils. Les personnes âgées risquent de faire les frais de cette utilisation de ces systèmes d'aide à la décision, soit qu'ils soient exclus, soit que les critères retenus par la machine n'en excluent certains pour je ne sais quelle raison : biais informatique ou simplement manque de prise en considération du point de vue de la personne concernée [52]. Pour illustrer le propos, nous partirons d'un cas, celui du logiciel SIREVA et de la réaction de l'ANAS (Association Nationale des Assistants Sociaux) pour ensuite évoquer les enjeux de l'IA au service des politiques des pouvoirs publics et privés.

Dans le cadre de sa politique d'aide au maintien des personnes âgées au lieu de leur domicile, le ministère français de l'aide sociale avait décidé fin 2016, d'utiliser un logiciel d'aide à la décision : le logiciel SIREVA (Support Inter-Régimes d'EVAluation), système dit expert qui, en fonction de certains critères, déterminait les bénéficiaires de cette aide. Les assistants sociaux avaient été mis à contribution pour récolter, lors de visites domiciliaires, les données nécessaires à l'alimentation de cette banque de données. L'Association nationale des assistants de service social (ANAS), interpellée par des assistants de service social d'organismes de sécurité sociale s'interroge sur le questionnaire qui est demandé à ces assistants sociaux de fournir et, en particulier, de la grille « prédictive » FRAGIRE qui contient des tests cognitifs et de marche de même qu'une grille d'évaluation de l'autonomie (AGGIR). L'Association réagit [53] comme suit : « *Pour une politique efficiente des actions de prévention et de repérage des fragilités des personnes dans le cadre du maintien à domicile portée par la CNAV, il est indispensable :*

- *Qu'il y ait une clarification des formalités effectuées auprès... de la CNIL concernant le dossier SIREVA ;*
- *Que soit respecté le droit des personnes concernées à être aidées sans que des données personnelles et sensibles les concernant ne soient inscrites dans un fichier de façon obligatoire ;*

52. Sur le profilage, on se référera à la, recommendation du Conseil de l'Europe de 2010, actuellement en cours d'actualisation : The protection of individuals with regard to automatic processing of personal data in the context of profiling, *Recommendation CM/Rec(2010)13 and explanatory memorandum,* document disponible sur le site du Conseil de l'Europe. Le lecteur lira notre rapport récemment discutée au comité consultatif de la Convention n° 108 du Conseil de l'Europe : FRENAY B. et POULLET Y., *Rapport et propositions de recommandations sur le « Profilage et la Convention 108+ du Conseil de l'Europe*, Rapport présenté au Comité consultatif de la Convention n° 108, Strasbourg, 21 septembre 2019, rapport disponible sur le site du Conseil de l'Europe

53. ANAS, « Souriez, vous êtes fichés », Communiqué du 17 avril 2018, disponible sur le site : anas.fr/Avec-SIREVA-souriez-vous-etes-fiches*a1179.html

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

— *Que les professionnels soient reconnus dans leurs compétences à évaluer la situation des personnes et à proposer des plans d'aide par la relation d'aide plutôt que par des outils de scoring préétablis.* ».

On louera cette prise de position qui interdit de réduire les personnes à des données dont par ailleurs la fiabilité est loin d'être absolue et sur cette base suivant des raisonnements non contestables par les personnes 'objets' de ces décisions, Elle rejoint le principe du RGPD (article 22) qui interdit de se satisfaire d'une décision prise sur base du seul raisonnement automatisé : « *La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.* ». Cependant on note de nombreuses exceptions, en particulier pour les pouvoirs publics [54].

Les pouvoirs publics, précisément, ont tendance pour les raisons déjà décrites à recourir aux systèmes d'intelligence artificielle ou systèmes-experts. Le croisement de données en provenance des diverses administrations donne à ces autorités le gisement de données à partir duquel ils pourront sélectionner aisément qui peut bénéficier de tel ou tel régime préférentiel ou au contraire en être exclu. Il s'agit, suivant le principe du '*benevolent government*', de substituer, à l'exigence de démarches actives de la part du citoyen, une attitude proactive des autorités publiques qui, elles-mêmes, détecteront les situations particulières des citoyens et leur accorderont les droits liés à ces situations. En d'autres termes, il s'agit de faire le bonheur des citoyens sans initiative nécessaire de leur part. Autre application de l'intelligence artificielle : le tarif de remboursement de médicaments peut de même être décidé dans le cadre du fonctionnement de tels systèmes. De tels systèmes peuvent fonctionner de manière opaque, dans la mesure où les données sont collectées indirectement auprès d'une autre administration et non plus auprès de la personne concernée, dans la mesure où le raisonnement complexe n'est pas toujours aisé à comprendre et peut inclure des biais (par exemple, on prend en compte pour fixer le profil de celui qui aura droit à telle aide, les populations ayant bénéficié d'une aide similaire dans le cadre d'un régime légal ancien). A cette opacité, s'ajoute que le droit de la personne concernée à être entendu peut-être organisé de telle sorte qu'il soit peu effectif et ce, d'autant plus que l'agent en charge de cette audition osera difficilement engager sa responsabilité propre, en contestant la 'vérité sortie de l'ordinateur'. A cette opacité, répond la demande de nombre d'auteurs [55] d'exiger la parfaite transparence (ou, du moins, l'explicabilité des décisions rendues ou proposées par ces algorithmes) des algorithmes de décision utilisés par l'autorité publique. Le fonctionnement de ces algorithmes, les règles qui y préside, le choix des données utilisées, leur qualité deviennent, ainsi, objets possibles de débats avec les représentants des citoyens visés, en l'occurrence des associations luttant pour la défense des aînés. Doivent également être mises en œuvre des mesures organisationnelles et managériales qui permettent une contestation aisée

54. Voir l'article 22. 2 b) : « *est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou . . .* »

55. AI NOW Institute, « *Litigating Algorithms : Challenging Government Use of Algorithmic Decision Systems*", 2018, https://ainowinstitute.org/litigatingalgorithms.pdf

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

par la personne concernée et, enfin, il faut veiller à la réelle indépendance décisionnelle de l'agent public qui reçoit la contestation et entend la personne concernée.

En ce qui concerne les pouvoirs privés, on peut imaginer nombre d'applications utilisant les vastes réservoirs de données nées de la collecte ubiquitaire de données pour 'profiler' l'individu [56]. Ainsi, les compagnies d'assurance voiture peuvent utiliser les nombreuses données récoltées par les capteurs placés dans le véhicule (géolocalisation, type de conduite de la voiture, personnes présentes dans le véhicule, présence d'alcool dans l'haleine...) ou liées à des statistiques (risques d'accident pour telle catégorie d'âge, moyenne d'accident de conducteurs de tel type de véhicule ; etc.) pour déterminer avec précision les risques liés aux conduites individuelles et fixer la prime d'assurance en fonction de ces risques, voire d'exclure telle ou telle personne. La contestation de la décision de la compagnie d'assurances sera d'autant plus difficile que le 'raisonnement' sera peu transparent, s'appuiera, comme nous l'avons dit, sur l'apparente objectivité des données et de l'algorithme, qui ont conduit au résultat et, surtout, le mode de prise de décision aura été accepté comme condition du contrat d'assurance. L'incidence de ce type de profilage peut poser problème pour les personnes âgées qui seront facilement mises à l'index et ne pourront bénéficier du principe traditionnel de la mutualisation. Par ailleurs, le profil 'personnes âgées' peut conduire le prestataire à adopter des pratiques de manipulation des personnes ainsi étiquetées, plus désarmées devant l'outil et souvent plus ignorantes des pratiques du *Web*. On songe bien évidemment aux pratiques de '*phishing*' et de rançonnage auxquelles les personnes âgées sont plus facilement exposées [57]. Enfin, la crainte de biais volontaires ou non en défaveur des personnes âgées dans le fonctionnement des algorithmes appelle la nécessité de mettre en place, comme le recommandent plusieurs textes et recommandations à propos de l'intelligence artificielle [58], une évaluation multidisciplinaire et ouverte aux différents représentants d'intérêts, y compris les associations de défense des aînés. « *AI systems should not harm human beings. By design, AI systems should protect the dignity, integrity, liberty, privacy, safety, and security of human beings in society and at work. AI systems should not threaten the democratic process, freedom of expression, freedoms of identify, or the possibility to refuse AI services. At the very least, AI systems should not be designed in a way that enhances existing harms or creates new harms for individuals. Harms can be physical, psychological, financial or social. AI specific harms may stem from the treatment of data on individuals (i.e. how it is collected, stored, used, etc.). To avoid harm, data collected and used for training of AI algorithms must be done in a way that avoids discrimination, manipulation, or negative profiling. Of equal importance, AI systems should be developed and imple-*

56. Pour une discussion approfondie des enjeux de l'IA, lire CNIL, « *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle.* », synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une république numérique, https://www.cnil.fr/sites/default/files/atoms/.../cnil_rapport_garder_la_main_Web.pdf.

57. Voir *supra,* n° 5 , notre réflexion sur l'intérêt de la disposition pénale qui incrimine celui qui abuse des faiblesses d'autrui.

58. Notamment, Conseil de l'Europe, «Rapport sur l'intelligence artificielle», rapport établi par A. MANTELERO, T-PD(2018)09Rev., Strasbourg, le 25 janvier 2019, , https ://rm.coe.int/intelligence-artificielle-et-protection-des-donnees-enjeux-et-solution/168091f8a5 et « Lignes directrices » T-PD(2019)01, https://rm.coe.int/lignes-directrices-sur-l-intelligence-artificielle-et-la-protection-de/168091ff40

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

mented in a way that protects societies from ideological polarization and algorithmic determinism.[59]. »

3 Conclusions

L'appropriation par le monde des aînés du numérique est une urgence, à l'heure où de plus en plus le numérique conditionne leurs choix de vie, entoure leur comportement et, malheureusement, décide seul de l'action à prendre vis-à-vis d'eux sans nécessairement qu'ils puissent participer à ces décisions. Cette appropriation permettra à nos aînés de saisir et surtout de profiter de toutes les opportunités du numérique. La stratégie nationale pour un « numérique inclusif », dans son rapport de mai 2018 préconisait trois actions dues par les pouvoirs publics et qui s'appliquent particulièrement bien aux besoins des aînés, en fonction de leur 'niveau', d'appropriation du numérique. Il s'agit tantôt de 'faire à la place', tantôt d''aider à faire', tantôt, enfin d''aider à mieux faire' et notamment à critiquer l'outil mis à leur disposition et les informations que cet outil véhicule. La réalisation de ces trois tâches – la lutte contre l' « illectronisme », au sens le plus large, des personnes âgées – pourrait être confiée en particulier aux EHPAD et aux bureaux d'assistance sociale.

Cette lutte est une nécessité si on souhaite que vieillesse ne signifie pas exclusion de la société de l'information et de ses bénéfices. Au-delà, il s'agit de mettre les valeurs éthiques « Dignité », « Autonomie », « solidarité » au centre de la réflexion 'participative' d'une société numérique pleinement respectueuse de l'humain – fût-il vieux et sans doute diminué dans certaines de ses capacités. On évitera de tomber dans une confiance démesurée dans les potentialités de la gouvernementalité algorithmique et la valeur des prédictions et des décisions de la 'machine' et on en mesurera à l'aune des valeurs éthiques et des droits de l'homme à la fois l'apport mais également les risques encourus par ces personnes particulièrement vulnérables. A cet égard, le concept de vie privée joue un rôle important au service de l'autonomie de la personne y compris d'échapper à la surveillance de l'outil et de ses applications et comme lutte contre la déresponsabilisation tant des aînés que de ceux qui les entourent et les soignent. Voilà quelques réflexions qui, nous l'espérons, introduiront un débat essentiel. Quel rôle peut et doit jouer le Droit au service de nos aînés dans leur appropriation du numérique ?.

Références :

ANAS, 2018 – **ANAS**, « Avec SIREVA, souriez, vous êtes fichés », manifeste du 17 avril 2018, disponible sur le site de l'ANAS : https://www.anas.fr/Avec-SIREVA-souriez-vous-etes-fiches_a1179.html ;

ARENDT, 2002 - **H. ARENDT**, « En guise de conclusion », in *Les origines du totalitarisme,* Paris, Gallimard, « Quarto », 2002, p. 873 et s. ;

BEAUCHAMPS et CHILDRESS, 2001 - **T.L. BEAUCHAMPS & J.F. CHILDRESS**, *Principles of Biomedical Ethics*, 3ème éd., Oxford University Press, New York, 2001 ;

BECK, 1986 – **U. BECK**, *La société du risque*, Paris, Aubier, 2001 (1986 pour l'édition allemande) ;

BOUDON, 1975 - **R. BOUDON**, « *Justice sociale et intérêt général : à propos de la Théorie de la justice de Rawls* », *Revue française de science politique*, vol. 25, n° 2, 1975, p. 193-221 ;

59. High Level Expert Group on Artificial Intelligence, *Ethical Guidelines for a Trustworthy AI* (2019).

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

BROTCORNE et alii 2010 - **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 ;

BROTCORNE, 2017, **P. BROTCORNE**, « L'effectivité des libertés fondamentales des personnes vulnérables », in *Vulnérabilités et Droits dans l'environnement électronique*, », in *Vunérabilités et droits dans l'environnement numérique*, Actes du colloque tenu à Namur le 14 octobre 2018, ouvrage sous la coordination de H. JACQUEMIN et M. NIHOUL, Larcier, Collection de la faculté de droit de Namur, p. 33 et s. ;

BRODIEZ-DOLINO, 2016, **A. BRODIEZ-DOLINO**, « Le concept de vulnérabilité, article publié in '*La vie des idées',* 11 février 2016, disponible sur le site https://laviedesidees.fr/ ;

CASTEL, 2010 - **R. CASTEL**, « L'autonomie, aspiration ou condition » in *La vie des idées,* 26 mars 2010, disponible à l'adresse : http://www.laviedesidÃ¯es.fr/L-autonomie-aspiration-ou.html ;

CNIL, 2016 - ***Délibération n° 2016-094 du 14 avril 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de l'accueil, l'hébergement, l'accompagnement et le suivi des personnes handicapées et des personnes âgées (AU-047),*** disponible sur le site de la CNIL : https://www.cnil.fr/ ;

CNIL, 2017 - CNIL, *Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise*, disponible sur le site de la CNIL : https://www.cnil.fr/ ;

CNIL, 2013 – CNIL, Systèmes de suivi et d'assistance électroniques des personnes âgées ou désorientées : les recommandations de la CNIL, disponible sur le site de la CNIL : Systèmes de suivi et d'assistance électroniques des personnes âgées ou désorientées : les recommandations de la CNIL, 24 juillet 2013 : https://www.cnil.fr/fr/systemes-de-suivi-et-dassistance-electroniques-des-personnes-agees-ou-desorientees ;

COLETTE-BAZECQZ, 2017 - **N. COLETTE-BAZECQZ**, « La protection pénale des personnes vulnérables dans l'environnement numérique », in *Vunérabilités et droits dans l'environnement numérique*, Actes du colloque tenu à Namur le 14 octobre 2018, ouvrage sous la coordination de H. JACQUEMIN et M. NIHOUL Larcier, Collection de la faculté de droit de Namur, p. 135 et s. ;

COMMISSION EUROPEENNE, 2018 - 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) ;

CONSEIL des DROITS de l'HOMME - NU, 2014 - 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) ;

CONSEIL de l'EUROPE 2014 - 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) ;

CONVENTION 108+, 2018 - Convention n° 108 modifiée du Conseil de l'Europe 'pour la protection des personnes à l'égard du traitement des données à caractère personnel', adoptée à la 128ème session du Comité des Ministres, le 18 mai 2018, texte et le long rapport explicatif sont accessibles sur le site du Conseil de l'Europe : www.coe.int/dataprotection ;

CORTEZ, 2018 – A. CORTEZ, « Précaires, personnes âgées, ruraux... les naufragés de la "dématérialisation" des services de l'Etat », publié le 12 mars 2018, disponible sur le site : https://www.marianne.net/societe/precaires-personnes-agees-ruraux-les-naufrages-de-la-dematerialisation-des-services-de-l-etat ;

CREDOC, 2017 – **CREDOC,** *Baromètre du numérique (4ème édition*), rapport disponible sur le site : https://www.credoc.fr/publications/barometre-du-numerique-2017-17eme-edition ;

CSA, 2018 - L'exclusion numérique des personnes âgées, Étude réalisée par CSA pour les petits frères des Pauvres, financée par la Fondation des petits frères des Pauvres, 27 septembre 2018, disponible sur le site : petitsfreresdespauvres.fr/informer/prises-de-positions/contre-l-exclusion... ;

de TERWANGNE et ROSIER (direction), 2018 - *Le règlement général sur la protection des données (RGPD/GDPR),* sous la direction de C. de TERWANGNE et K. ROSIER, Coll. Cahiers du CRIDS, n° 44, Larcier, 2018 ;

DEVELEDEC, 2018 - **N. Le DEVEDEC,** « Humanisme, transhumanisme : deux conceptions antithétiques de la perfectibilité humaines, in *Généalogies et nature du transhumanisme – Etat actuel du débat,* ouvrage sous la direction de F. DAMOUR, S. DEPREZ et D.DOAT, Liber, 2018, p. 33 et s. ;

DOAT, 2016 - **D. DOAT**, « La vulnérabilité : esquisse d'une reconstruction conceptuelle », *Revue de théologie et de philosophie,* 2016, n° 48, p. 751 ;

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

DWORKIN, 1977 - **R. DWORKIN**, *Taking Rights Seriously,* Cambridge, Harvard University Press, 1977 ;

EDPS, 2015 - **EDPS**, « Towards a new Digital Ethics, Opinion 4/2015, 11 septembre 2015 ;

EDPS, Ethics Advisory Group,"*Towards a digital ethics*", Report 2018, Le rapport est disponible sur le site : https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf. ;

HERVEG, 2017 - **J. HERVEG**, « Réflexions autour ed la protection des données et des vulnérabilités », in *Vunérabilités et droits dans l'environnement numérique*, Actes du colloque tenu à Namur le 14 octobre 2018, ouvrage sous la coordination de H. JACQUEMIN et M. NIHOUL, Larcier, Collection de la faculté de droit de Namur, p. 33 et s. ;

HIGH LEVEL EXPERT GROUP on AI, 2017 - **High Level Expert Group *on* Artificial Intelligence**, *Ethical Guidelines for a Trustworthy AI* , projet de rapport publié le 18 décembre 2018 disponible sur le site : 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-) ;

LACORDAIRE, 1872 - **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, p. 471-495 ;

LACROIX, 2016 - **J. LACROIX et J.Y. PRANCHERE**, *Le procès des droits de l'homme,* Seuil, 2016, p. 324 ;

Mc NAY, 2014 - **L. McNAY**, *The misguided Search for the Political*, Cambridge, Policy, 2014 ;

MANTELERO, 2018 - **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. ;

MAGNIN, 2017 - **T. MAGNIN**, *Penser l'humain au temps de l'homme augmenté,* Albin Michel, 2017 ; MISSION SOCIETE du NUMERIQUE, 2018 - **MISSION SOCIETE du NUMERIQUE,** *LE NUMÉRIQUE, MENACE OU OPPORTUNITÉ POUR LE RECOURS AUX DROITS SOCIAUX ? UNE ENQUÊTE EN HAUTS DE France,* Rapport publie le 13 novembre 2018, disponible sur le site : https://labo.societenumerique.gouv.fr/2018/11/13/numerique-menace-opportunite-recours-aux-droits-sociaux-enquete-aupres-personnes-agees-situation-de-precarite-hauts-de-france ;

ORIS, 2017 – **M. ORIS**, « Les contours du concept de vulnérabilité », in *Les populations vulnérables Actes du XVI e colloque national de démographie*, CUDEP ;

POULLET, 2018, **Y.POULLET**, « Le droit de la vulnérabilité au risque du numérique », Colloque ESPHIM : *L'IDENTITÉ EN QUESTION : ENTRE PARCOURS DE VULNÉRABILITÉS ET CHEMINS D'AUTONOMIE*, L. Rizzerio (sous la direction de), Namur les 23, 24 et 25 janvier 2018, en cours de publication ;

POULLET, 2019 - **Y. POULLET**, *La vie privée à l'heure du numérique*, Larcier, Coll. des cahiers du CRIDS n° 45, Larcier, Bruxelles, 2019 ;

POULLET, 1995 - **Y. POULLET**, « Au-delà du service universel des télécommunications : le service universel dans la société de l'information », *Les consommateurs et la société de l'information, Bruxelles, Centre coopératif de la Consommation, 1998, p ; 41 et s. ;*

RAWLS, 1997 - **J. RAWLS**, *Théorie de la Justice*, Seuil, 1997 ;

REBOURG et BURDIN, 2014 - **M. REBOURG et E. BURDIN**, « La vulnérabilité dans l'espace juridique : la situation des personnes du grand âge », in BRODIEZ-DOLINO Axelle *et alii*, *Vulnérabilités sanitaires et sociales. De l'histoire à la sociologie*, Rennes, PUR, 2014, p. 65-76 ;

RGPD, 2016 - **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, 4.5.2016, p. 1-.88,* disponible à http://data.europa.eu/eli/reg/2016/679/oj ;

REPUBLIQUE FRANCAISE, 2016 - LOI No. 2016-1321 du 7 octobre 2016 pour une République numérique, disponible sur le site : https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829_type=general ;

ROUVROY- POULLET (2009) - **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 ? ,* Springer, Dordrecht, 2009, p. 159 et s. ;

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874

SENECHAL, *2017* - **J. SENECHAL**, Vulnérabilité et contrôle du contractant à l'ère numérique, in *Vunérabilités et droits dans l'environnement numérique*, Actes du colloque tenu à Namur le 14 octobre 2018, ouvrage sous la coordination de H. JACQUEMIN et M. NIHOUL, Larcier, Collection de la faculté de droit de Namur, p. 107 et s. ;

SEN, 1985 - **A.SEN**, *Elements of a Theory of Human Rights*, PHIL. & PUB. AFF., 2004, n° 32, p. 315 et s. ;

SEN, 1985 - **A. SEN**, *Commodities and Capabilities*. Amsterdam ; New York, Elsevier Science Pub. Co., 1985 ;

SEN, 2009 - **A. SEN**, 'Economics, Law and Ethics'. In *Against Injustice the New Economics of Amartya Sen.* Cambridge University Press, 2009 ;

SEN, 2009 - 'Human Rights and Capabilities'. *Journal of Human Development, 2005/* 6, no. 2, pp. 155 à 166 ;

SMSI, 2003 - **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 ;

SUDRE, 2005 - **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, Bruylant, Nemesis, 2005, p. 27 et s. ;

TIC- SANTE, 2016 – **TIC-SANTE**, « Ehpad : le numérique ne crée pas de nouveaux risques juridiques mais les démultiplie : compte rendu de la conférence de D. JAFAAR », 2 août, 2016, disponible sur le site : https://www.ticsante.com/story/3120/ehpad-le-numerique-ne-cree-pas-de-nouveaux-risques-juridiques-mais-les-demultiplie.html ;

Van der LINDEN et JUILLERET, 2010 – **M. Van der LINDEN et A.C. JUILLERAT**, « Les personnes âgées et les nouvelles technologies », 6 octobre 2010, article disponible sur http://www.mythe-alzheimer.org/article-les-personnes-agees-et-les-nouvelles-technologies-58960857.htm.

Published in : PIATTI, M.-C. ; GUILLERMIN, M. (dir.) (2020), *Intelligence(s) artificielle(s) et Vulnérabilité(s) : kaléidoscope. Les contreforts de l'éthique et du droit*, Editions des archives contemporaines, ISBN : 9782813003874, doi : https ://doi.org/10.17184/eac.9782813003874