LES VULNÉRABILITÉS INHÉRENTES À L'APPROCHE INDIVIDUALISTE DES DONNÉES DE SANTÉ DANS L' « ÈRE BIG DATA »

Fabien LECHEVALIER[1]

1 L'auteur est candidat au doctorat (LL.D) en Droit (Université Laval) / (Ph. D) Droit privé & sciences criminelles (Université Paris-Saclay).

Résumé

Le phénomène Big Data multiplie les pratiques de recueil de données dans tous les secteurs, mais c'est certainement dans le domaine de la santé, que celles-ci suscitent le plus de questions sur leur statut et sur leur partage. En effet, ces données relevant à la fois du bien commun de l'humanité et du plus profond de l'intime, nous poussent à nous interroger sur le régime juridique le plus adapté à leur appliquer afin préserver au mieux la vie privée des personnes. En France, le régime érigé par le RGPD institue le principe d'une interdiction générale de la collecte desdites données qui peut être levée par le consentement éclairé et exprès du patient. Cependant l'efficacité de ce cadre juridique est déjà contestée en doctrine et en pratique.

Alors que la réalité du partage et de l'analyse des données a changé, les théories dominantes de la vie privée limitent leurs analyses à une approche individualiste. Partant, nos objectifs spécifiques sont de discuter du surinvestissement de la théorie de la vie privée dans les théories centrées sur l'individu et de la nécessité pour les décideurs politiques de s'engager pleinement dans le débat d'une gestion collective des droits qui y sont attachés afin d'apporter une solution idoine aux vulnérabilités crées par l'« ère big data ».

Introduction

[1] «Big Data» sont deux petits mots avec une énorme signification sociétale[2]. Ces mots signifient un phénomène complexe qui a fini par définir la deuxième décennie du XXIe siècle. Les mégadonnées sont de vastes quantités d'informations susceptibles d'être collectées, stockées et analysées à grande échelle. À l'aide de ces données, les entreprises et les chercheurs peuvent déployer des algorithmes complexes et des technologies d'intelligence artificielle pour révéler des modèles, des connexions, des comportements, des tendances, des identités et des connaissances pratiques autrement inconnus. Dans le domaine de la santé, le big data correspond à l'ensemble des données socio-démographiques et de santé, disponibles auprès de différentes sources qui les collectent pour diverses raisons[3]. Ces informations proviennent des pratiques gouvernementales et commerciales, des transactions des consommateurs et des applications numériques[4]. Les individus contribuent de manière invisible au Big Data chaque fois qu'ils vivent des modes de vie numérique ou participent à l'économie numérique, comme lorsqu'ils effectuent une transaction à l'aide d'une carte de crédit, se font soigner à l'hôpital, utilisent une application mobile reliée à une montre connectée, recherchent un sujet sur Google ou publient sur Facebook[5]. Le phénomène Big data multiplie ainsi les pratiques de recueil de données dans tous les secteurs, mais c'est certainement dans le domaine de la santé que celles-ci suscitent le plus de questions sur leur statut et sur leur partage. L'exploitation de ces données présente, en effet, de nombreux intérêts dans le cadre de la médecine personnalisée : identification de facteurs de risque de maladie, aide au diagnostic, au choix et au suivi de l'efficacité des traitements, pharmacovigilance, épidémiologie... Mais à côté de ces perspectives très bénéfiques pour la santé publique, il est à craindre que, malgré les contrôles prévus, les données soient exploitées dans un intérêt économique au détriment de l'intérêt public. L'exploitation de nos données de santé pose de nombreux défis techniques et humains, et pose autant de questions éthiques que juridiques. Ces données relevant à la fois du bien commun de l'humanité

2 David Bollier, *The promise and peril of Big Data,* The Aspen Institute, (2010), https://www.emc.com/collateral/ analyst-reports/ 10334-ar-promise-peril-of-big-data.pdf [https://perma.cc/CD6F-ACYZ].

3 Rodolphe Theibaut, Big data en santé: Des défis techniques, humains et éthiques à relever, INSERM, (1er Juin 2016).

4 Jacob Morgan, « A Simple Explanation of « The Internet of Things », *Forbes,* (13 Mai 2014, 12:05 am), http:// www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/ #4a6ee29b6828.

5 Anita Allen, « Protecting One's Own Privacy in a Big Data Economy », (2016), 130:71 *Harvard Law Review Forum* 71.

et du plus profond de l'intime, nous poussent à nous interroger sur le régime juridique le plus adapté à leur appliquer afin de préserver au mieux la vie privée des personnes.

[2] Alors que la réalité du partage et de l'analyse des données a changé, on pourrait craindre que les théories de la vie privée prennent du retard au regard des enjeux colossaux auxquels elles doivent faire face. Cela est d'autant plus le cas dans un contexte où les théoriciens de la vie privée diffèrent notoirement et largement sur la conception appropriée à leur donner[6]. Pourtant, on s'aperçoit que ces nombreuses doctrines ont tendance à partager une hypothèse théorique sous-jacente. Les théories dominantes de la vie privée analysent, en effet, cette notion à travers la lentille de l'individualisme[7]. Elles peuvent, donc, toucher à la dimension sociale de la vie privée[8], mais ne l'engagent pas fortement. Nos objectifs spécifiques sont de discuter du surinvestissement de la théorie de la vie privée dans les théories centrées sur l'individu (I) et de la nécessité pour les décideurs politiques de s'engager pleinement dans le débat d'une gestion collective des droits qui y sont attachés (II).

I. L'INFLUENCE HISTORIQUE DE L'INDIVIDUALISME DANS L'AVIS ET LE CHOIX MODERNE

[3] ILe droit traditionnel à la vie privée envisage le contrôle d'un individu sur les informations qui proviennent de ou portent sur cet individu. Les approches modernes de la vie privée ont développé et intensifié l'accent mis sur la notification individuelle, le choix et le contrôle des flux d'informations[8]. C'est ainsi qu'en France, le régime érigé par le Règlement Général sur la Protection des Données (RGPD) institue le principe d'une interdiction générale de la collecte des données[9] de santé qui ne peut être levée que par le consentement éclairé et exprès du patient[10] (ou bien pour des intérêts de santé publique[11]). La vie privée en tant que

6 Daniel J. Solove, « Conceptualizing Privacy », (2002), *90 California Law Review 1087*, pp. 1099–1123.

7 Robert C. Post, « The Social Foundations of Privacy: Community and Self in the Common Law Tort », (1989), *77 California Law Review 957*, pp. 958.

8 Paul M. Schwartz, « Privacy and Democracy in Cyberspace », (1999), *52 Vanderbilt Law Review. 1609*, pp. 1664.

9 Priscilla M. Regan, L Legislating privacy: technology, social values and public policy 228, University of North Carolina Press, Chapel Hill, (1995), pp. 231.

10 Article 9 Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 96/46/CE (règlement général sur la protection des données).

11 Article 6 Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 96/46/CE (règlement général sur la protection des données).

contrôle est devenue une théorie dominante de la vie privée informationnelle, en partie parce qu'elle promet aux individus (à tort ou à raison) la possibilité de divulguer et de contrôler la diffusion d'informations en ligne[12]. Bien que la vie privée en tant que contrôle ne soit pas une approche incurablement centrée sur l'individu, le développement ultérieur de la théorie et, surtout, son régime opératoire de notification démontrent la dominance de l'individualisme dans le droit moderne de la vie privée[13]. L'avis et le choix dépendent entièrement et explicitement des individus.

[4] Ces régimes tentent de faire en sorte que les individus sachent ce qui est fait de leurs informations et aient le choix quant à la manière dont ces données sont utilisées. Même les critiques de l'avis et du choix tendent à adhérer au paradigme individuel, plutôt qu'à remettre en cause l'hypothèse de base de l'individualité. La réponse traditionnelle aux défauts des régimes de notification et de choix a été que la notification et le choix ne sont pas encore suffisamment solides[14]. En effet, la critique courante est que les consommateurs ne sont pas suffisamment informés de ce qui est fait de leurs informations et qu'ils ne disposent pas de suffisamment de pouvoir discrétionnaire pour contrôler leur vie privée. Une solution idoine consiste donc à faire valoir que la qualité de l'avis et du choix doit s'améliorer. Partant, les conditions d'utilisation et les accords de licence d'utilisateur final sont de plus en plus explicites à la demande des tribunaux et des régulateurs. L'accent mis sur la compréhension et le contrôle est censé permettre au consommateur de mieux comprendre et contrôler les conséquences de la révélation d'informations qu'il propose sur lui-même[15]. À son tour, la tendance réglementaire en matière de protection de la vie privée dès la conception (« Privacy by design ») vise à inciter les entreprises à créer des outils permettant une compréhension et un contrôle individuel[16]. Notre critique ne consiste pas à soutenir que l'avis et le choix ne sont pas utiles, mais simplement que l'éducation et l'autonomisation axées sur l'individu semblent donner des rendements décroissants[17]. Les consommateurs ne

12 *Ibid*.

13 Mark MacCarthy, « New Directions in Privacy: Disclosure, Unfairness and Externalities », (2011), *6 I/S: Journal of Law & Policy for Information Society 425*, pp. 429.

14 Priscilla M. Regan, *op. cit*., note 9.

15 Jeff Sovern, « Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information », (1999), *74 Washington Law Review 1033*, pp. 1094.

16 Kenneth A. Bamberger, Deirdre K. Mulligan, « Privacy on the Books and on the Ground », (2011), *63 Stanford Law Review 247*, pp. 301–02.

17 Ann Cavoukian, Information & Privacy Commissioner of Ontario Privacy by design: The 7 Fundamental principles S 1–2, (2011).

lisent pas assez rationnellement les politiques de confidentialité soigneusement formulées[18]. Dans une étude menée par la Commission européenne, en 2015, seulement 7% des internautes français disaient lire *toujours ou fréquemment* les conditions d'utilisation (comprenant les politiques de confidentialité)[19]. Avec l'arrivée du Big data et du deep learning, la situation s'est encore aggravée puisque tout internaute désirant bénéficier d'un service personnalisé n'a plus la possibilité à l'heure actuelle de s'opposer à la collecte et au traitement de ses données personnelles en raison des configurations techniques des algorithmes. Quand bien même ils les liraient, les audits produits par les entreprises en réponse aux incitations à la protection de la vie privée dès la conception sont souvent mis de côté en raison des coûts, du temps que cela nécessite ou de la complexité de la tâche[20]. Des théoriciens ont toutefois proposé une approche plus relationnelle du consentement dans laquelle la collecte des données serait soumise à un principe de réciprocité qui inviterait les collecteurs à mettre en place des moyens de contrôle intelligents tels que des instruments permettant un paramètrage personnalisé de la confidentialité et un retour intelligible des données sous formes d'alertes, des recommandations ou encore des tableaux de bord de suivi. Ce principe de réciprocité astreint les collecteurs à une obligation de rendre compte à la fois de ce qu'il font pour respecter la vie privée mais aussi des effets sociaux qu'induisent l'usage agrégé de ces données. La réciprocité est ce système de paiement symbolique qui maintient la confiance, tourné vers l'intérêt de l'autre. La question est désormais de savoir quels types de dispositifs permettent de l'exprimer.

[5] Même dans l'hypothèse où l'avis et le choix individualisés produiraient les résultats escomptés – et ce n'est actuellement pas le cas – un problème subsisterait. L'approche individuelle de la vie privée suppose à tort que la personne est l'unité prédominante dans la conversation sur la vie privée, et donc que chaque personne peut et doit gérer les informations uniquement sur elle- même[21]. C'est un oubli[22]. En consentant à la collecte d'informations, un utilisateur devient un canal de

18 Daniel J. Solove, *op. cit.*, note 6.

19 Daniel J. Solove, Woodrow Hartzog, « The FTC and the New Common Law of Privacy », (2014), *114 Columbia Law Review 583*, pp. 667.

20 En 2014, dans le même ordre d'idée, une étude Ipsos France révélait que 67% d'entre eux assuraient lire que *rarement ou jamais* ces conditions d'utilisation. Voir « Les français et le Big Data », *Ipsos-France, Enquête auprès des consommateurs, (2015),* pp. 16 et pp. 28.

21 Emil Protalinski, « Survey: Facebook, Google Privacy Policies Are Incomprehensible », *ZDNET,* (4 Mai 2012).

22 Bamberger, Mulligan, *op. cit.*, note 16.

collecte d'informations sur l'ensemble de son réseau social, qu'il ait ou non consenti de sorte que les données ne sont plus de simples données personnelles, mais des « données en réseaux » qui lient plusieurs personnes les unes avec les autres. En effet, nous interagissons constamment les uns avec les autres de sorte qu'il est de plus en plus difficile d'identifier des données qui sont vraiment « personnelles ». Aujourd'hui, les utilisateurs des nouvelles technologies divulguent constamment des informations, et sur le moindre de leurs mouvements[23] notamment au travers des réseaux sociaux[24]. Les consommateurs le font dans la croyance erronée que les données sont éphémères, ou en raison de promesses trop souvent rompues que les données des consommateurs peuvent être conservées à l'abri d'autres consommateurs ou de tiers malveillants[25]. Les smartphones ou autres appareils intelligents, omniprésents, permettent aux utilisateurs de fournir des informations sur eux-mêmes mais aussi sur les autres à longueur de temps[26]. Les possibilités de contourner les médias sociaux s'amenuisent à mesure que d'autres les emportent avec eux[27]. S'engager avec les médias sociaux n'est donc plus un choix purement individuel mais un résultat inévitable dans presque toutes les situations sociales. L'interconnexion des données va de mise avec leur interdépendance. Par consentement, un individu autorisant la collecte ou le traitement de ses données personnelles empièterait alors sur le droit à la vie privée de ses proches en raison de la nature même de la donnée. Les dérives issues du commerce de données extraites des tests génétiques récréatifs commercialisés à bas coûts sur Internet en sont un exemple flagrant. En 2017, la CNIL publiait son premier « Point CNIL : Les données génétiques »[28], où elle indiquait : *« les données génétiques présentent aussi la particularité d'être non seulement personnelles mais aussi pluripersonnelles car transmissibles et partagées. »*[29]. En effet, les données génétiques sont liées à l'ADN de son porteur et permettent de le

23 Mark MacCarthy, *op. cit.*, note 13.

24 Ils le font sur les commerces qu'ils visitent, les itinéraires qu'ils empruntent, les activités qu'ils réalisent, la nourriture qu'ils ingèrent et les personnes qu'ils rencontrent. Voir Michael Birnhack, « Reverse Engineering Informational Privacy Law », (2013), *15 Yale Journal of Law & Technology 24*, p. 86.

25 Les utilisateurs des réseaux sociaux *taguent* des photos les uns des autres sur Facebook et se référencent dans des publications géolocalisées. Voir James Grimmelmann, « Saving Facebook » (2009), *94 Iowa Law Review 1137*, pp. 1145–46; Voir aussi Nick BILTON, « Disruptions: Indiscreet Photos, Glimpsed Then Gone », *N.Y. Times: Bits,* (6 mai 2012, 5:24 pm); Voir aussi Jason Mazzone, « Facebook's Afterlife », (2012), *90 North Carolina Law Review 1643,* p. 1653.

26 Catherine Shu, « Confirmed: Snapchat Hack Not A Hoax, 4.6M Usernames And Numbers Published », *Techcrunch* (31 Décembre 2013).

27 Thomas H. Chia, « Fighting the Smartphone Patent War with Rand-Encumbered Patents », (2012), *27 Berkeley Technology Law Journal 209*, p. 231.

28 Peter Swire, « Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment », (2012), *90* North California Law Review 1371, pp. 1381–82.

29 Rapport CNIL, *Point CNIL: Les données génétiques,* La documentation française, CNIL, (2017).

distinguer parmi tous les autres êtres humains, mais elles sont également partagées pour partie par plusieurs personnes. Ainsi, même si les régulateurs réussissaient à donner un sens au consentement individualisé à la collecte de données, ils manqueraient l'essentiel. Les individus éduqués et responsabilisés n'ont toujours pas leur mot à dire, car même s'ils sont parfaitement informés et responsabilisés, ils ne contrôlent que leurs propres données et ne peuvent pas influer sur la montagne d'informations à partir desquelles les algorithmes de Big Data fonctionnent. Tant que des informations sont fournies par des tiers, personne ne peut vraiment s'en écarter. Si une personne ne fait pas elle-même partie du réseau, elle abandonne son avantage individuel, tout en supportant (la majeure partie du temps) son coût individuel[30].

[6] Le parti pris de l'individualisme n'est pas exclusif à la législation européenne, il traverse également les principales divisions culturelles et juridiques du droit à la vie privée. Par exemple, les approches de la vie privée semblent à première vue différentes de chaque côté de l'Atlantique[31]. Selon James Q. Whitman, si l'Amérique du Nord se concentrent sur la liberté[32], l'Union européenne, elle, s'appuie sur le concept de dignité humaine[33]. Pourtant, les deux philosophies considèrent la vie privée comme une question qu'il est préférable de résoudre en informant et en responsabilisant les individus[34]. En Europe comme en Amérique du Nord, l'objectif présumé est d'informer les individus sur le consentement à l'utilisation de leurs données personnelles. Néanmoins, le problème demeure : les données n'ont pas d'incidence sur cette personne seule. Sans avoir la prétention de proposer une analyse exhaustive des deux traditions, cet argument souhaite démontrer que l'apparente fracture transatlantique dans la théorie de la vie privée masque une similitude de fait sous-jacente[35]. Dans les deux ordres juridiques, les individus consentent à l'utilisation de données ayant un impact sur des tiers non consentants[36]. Les approches

30 *Ibid*.

31 Joshua A.T. Fairfield, Christoph Engel, « Privacy as a Public Good », (2015), *65:3 Duke Law Review 38.*

32 James Q. Whitman, « The Two Western Cultures of Privacy: Dignity Versus Liberty », (2004), *113 Yale Law Journal 1151*, pp. 1167.

33 *Ibid,* p.1158.

34 *Ibid*, p.1161.

35 Omer Tene, Jules Polonetsky, « To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising », (2012), *13 Minnesota Journal of Law, Science & Technology 281*, p. 287.

36 James Q. Whitman, *op. cit.*, note 32.

de la liberté et de la dignité se concentrent sur l'autonomisation et l'information des individus, plutôt que sur l'amélioration de la coordination de groupe[37]. Les lois nord-américaines et européennes diffèrent selon que les individus doivent accepter ou refuser la collecte et le traitement des données ainsi que sur la portée et le moment du consentement de la personne. Bien qu'héritières d'approches normatives différentes, les deux traditions situent le problème et sa solution autour de l'individu décidant de manière isolée: l'individu doit accepter ou refuser[38] à des utilisations bien souvent hors contexte. C'est en effet le cas puisqu'il devra poursuivre la suppression des données qui le concernent aux différentes phases de la vie de cette donnée. Ceci apparait d'autant plus dérangeant qu'il s'agit de données aussi sensibles que les données personnelles de santé.

[7] La discussion ci-dessus tente de souligner le sérieux parti pris en faveur de la conceptualisation de la vie privée en termes d'informations individuelles, de droits et d'actions. De plus, une succincte comparaison des approches nord- américaine et européenne montre que, malgré d'apparentes différences, ces approches se concentrent toutes les deux sur l'individualisme. En conséquence, cette théorie juridique occulte le dilemme social de la vie privée, comme nous allons, à présent, le développer.

II. L'INFLUENCE ÉMERGENTE DU COLLECTIVISME DANS LE DROIT DES DONNÉES DE SANTÉ

[8] Face à cette conception individualiste de la relation de la personne à ses données et du consentement, certains proposent une vision différente. En effet, les données personnelles, notamment celles relatives à la santé, même si elles relèvent pour chacun d'entre nous de la sphère privée la plus intime, deviennent aussi – par leur mise en commun – les composantes d'un réseau d'informations utiles à l'intérêt général[39]. Ce réseau constituerait un bien « public » ou « commun » relevant d'une protection collective de la vie privée. La justification découle du fait que, dans un réseau, les données deviennent « relationnelles » et ne pourraient donc pas être considérées comme relevant d'un enjeu

37 Omer Tene et Jules Polonetsky, *op. cit.*, note 35.

38 James Q. Whitman, *op. cit.*, note 32.

39 Omer Tene, Jules Polonetsky, « Big Data for All: Privacy and User Control in the Age of Analytics », (2013), *11 Northwestern Journal of Technology & Intellectual Property 239*, pp. 60–62.

purement individualiste. La donnée étant intégrée à un réseau, la protection du réseau serait alors plus adaptée que celle des données de chaque personne composant ce réseau. Pour être efficace[40], une protection relevant d'une conception individualiste imposerait en effet des limites sévères au partage des données, sauf anonymisation pouvant provoquer une dégradation qui priverait le traitement d'une partie de son efficacité. Dans cette approche, les « *données de santé, ne peuvent pas être protégées avec une approche* libérale concentrée sur la maximisation des libertés individuelles mais il serait plutôt nécessaire d'adopter une optique plus communautaire ou collective, qui pourrait exiger une limitation de certaines libertés individuelles, au nom de l'intérêt général et du bien commun »[41].

[6] Au nom de l'intérêt général et de la nécessité de favoriser le progrès, il pourrait être permis de remettre en cause la nécessité même d'un consentement au traitement des données, jugé comme pouvant être un obstacle excessif. D'autres plaident pour un contrôle plus laxiste et estiment que le consentement individuel pourrait être écarté s'il existe une forte probabilité que le traitement contribue à l'amélioration de la santé de la personne et, au-delà, à celle de la collectivité, lorsque le risque d'atteinte est proportionnellement plus faible. Une troisième conception intermédiaire fut proposée, celle d'une forme d'autonomie interactive et relationnelle, dans laquelle la personne gère ses données mais est intégrée dans une collectivité qui met en oeuvre un projet collectif qui la protège[42]. Cette dernière conception se fonde sur une littérature américaine florissante[43] qui propose d'explorer la valeur collective de la vie privée, proposant des exégèses originales des notions tirées de l'économie publique pour la qualifier de bien collectif à part entière.

[7] Néanmoins les concepts regroupés sous le vocable de biens collectifs sont polysémiques et ne recouvrent pas *de facto* les mêmes définitions selon qu'ils sont analysés par des philosophes, des politologues, des juristes ou des économistes. Certains auteurs soutiennent que la vie

40 *Loi n° 2016-1321* du 7 octobre 2016 pour une République numérique pose les premiers jalons d'une reconnaissance de la valeur collective des données.

41 Yann Joly, *et al, «* Are data sharing and privacy protection mutually exclusive? », (2016), *Cell 167,* p. 1150.

42 Danièle Bourcier, Primavera De Filippi. « Vers un droit collectif sur les données de santé », (2018), *Revue de Droit sanitaire et social*, pp. 444-56.

43 Voir nos travaux sur les fiducies de données qui offrent de belles perspectives d'une gestion collective des données: Fabien Lechevalier, *Les fiducies de données personnelles de santé*, Mémoire de maitrise, Université Laval, 2020.

privée serait un véritable bien public[44] car sans intervention mesurée, les décisions relevant de la vie privée personnelles d'individus pleinement informés tendent à réduire la vie privée d'autres individus. La littérature juridique n'est pas entièrement exempte de la suggestion selon laquelle la vie privée peut être étudiée de manière rentable comme un véritable bien public[45]. Par exemple, Paul Schwartz ou encore Joshua A.T. Fairfiel et Christoph Engle notent que la confidentialité des informations fonctionne comme tout autre type de bien public, à savoir comme l'air pur ou la défense nationale[46] et que la vie privée, d'un point de vue constitutif, est aussi un « bien public ». Schwartz ajoute que les informations privées sont en quelque sorte des « biens communs » qui nécessitent un certain degré de contrôle social[47]. Dans cette formulation il instaure cependant un doute sur la qualification qu'il donne auxdites informations : bien public pur ou bien commun[48] ? C'est dans cette même perspective que Priscilla Regan discute de la « *valeur collective* » de la vie privée, qu'elle tire quant à elle du concept des économistes de biens communs[49]. Elle suggère plus largement que la reconnaissance du fait que la vie privée possède certaines caractéristiques d'un bien commun rendrait plus clair d'une part, les intérêts institutionnels dans les informations personnelles et d'autre part, les faiblesses d'une solution de marché pour fournir une meilleure protection de la vie privée[50]. L'analyse de Regan pourrait trouver son positionnement dans le mouvement des *communs*[51] qui s'est développé ces dernières années au sein de la communauté scientifique. Pour le chercheur américain David Bollier, il s'agit d'une *« nouvelle manière de penser et de prendre soin des ressources qui n'appartiennent ni à un acteur*

44 Stefaan G. Verhulst, « Leveraging Private Data for Public Good. A Descriptive Analysis and Typology of Existing Practices », *GOVLAB*, (2019). En ligne: https://thelivinglib.org/leveraging-private-data-for-public-good- a-descriptive-analysis-and- typology-of-existing-practices/ ; Pricilla M. Regan, « Privacy as a Common Good in the Digital World », (2002), *5:3 Information, Communication & Society 382* ; Anita Allen, « Protecting One's Own Privacy in a Big Data Economy », (2016), *130:71 Harvard Law Review Forum 71* ; Joshua A.T. Fairfield, Christoph Engel, « Privacy as a Public Good » (2015), *65:3 Duke Law Review 38* ; Priscilla M. Regan, « Response to Privacy as a public good », (2016), *65 Duke Law Review 51* ; Mariana Mazzucato, « Let's make private data into public good », (27 Juin 2018), *MIT Technology Review,* En ligne: https:// www.technologyreview.com/s/ 611489/lets-make-private-data-into-a-public-good/ ; Julia Lane, Helen Nissenbaum, Victoria Stodden, Stefan Bender (éd.), *Privacy, Big Data, and the Public Good,* Cambridge University Press, (2016) ; Julie E. Cohen, T*urning Privacy Inside Out* (April 12, 2018). etc.

45 Si un bien public pur (définis par Samuelson en 1954) est un bien non rival et non exclusif, le coût de son financement est tel qu'aucun intérêt privé n'accepterait de le financer n'ayant pas de certitude quant à la rentabilité de l'investissement.

46 Edward J. Janger, Paul M. Schwartz, « The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules », (2002), *86 Minnesota Law Review 1219*, pp. 1253–54.

47 Schwartz, *op. cit. ;* Fairfield, Engel, *op. cit.*

48 Edward J. Janger et Paul M. Schwartz, *op. cit.*, note 46.

49 Les propriétés de rivalité et de non exclusion définissent *les biens en commun*. On considère qu'ils ont des externalités positives et pour cette qualité, il faut les protéger via la puissance publique. Voir François Lévêque, *Les théories de la réglementation*, Ed. La découverte, Collection Repères, (2005).

50 Priscillia M. Regan, *op. cit.*, note 9.

51 Mark MacCarthy, *op. cit.*, note 13.

privé, ni à un acteur public, et qui sont partagées et gérées par une communauté qui en définit les droits d'usage (accès, partage, circulation) »[52].

[8] Les *communs* existent sous une diversité de formes et d'arrangements institutionnels, comme l'ont démontré l'ensemble des travaux d'Elinor Ostrom, Prix Nobel d'économie, et d'autres chercheurs qui ont étudié l'action collective et la gestion des biens communs. Menés durant plusieurs décennies, les travaux d'Ostrom démontrent que l'action collective peut être un moyen efficace de gérer des ressources de manière équitable et pérenne, tout en renforçant les liens sociaux qui tissent des communautés résilientes et durables[53]. Envisager les données, et à fortiori les données de santé, sous le prisme de biens collectifs permettrait de reconnaitre leur valeur publique tout en prenant en compte les enjeux collectifs de la vie privée préalablement identifiés.

[8] Ces approches divergentes montrent que le point de friction demeure la sempiternelle évolution du rapport entre l'individuel et le collectif, entre l'autonomie accrue de chacun et la protection que nécessite l'utilisation généralisée des technologies de traitement de données de masse. Les progrès de l'une inspire le renforcement de la seconde. Leur concordance ne va pas sans heurts et suscite de vives tensions car intérêt individuel et collectif ne coïncident pas nécessairement. Conceptions individuelle, collective ou relationnelle peuvent contribuer à la recherche d'un point d'équilibre à constamment assortir aux progrès technologiques et à l'évolution des modes de vie.

52 Concrètement, un commun peut prendre la forme d'une ressource naturelle (forêt, pâturage), matérielle (voiture, musée) ou immatérielle (logiciel libre, article scientifique). Le plus célèbre d'entre tous, c'est bien sûr l'encyclopédie en ligne Wikipédia, avec ses milliers d'administrateurs et ses millions d'usagers.

53 David Bollier, « Elinor Ostrom Remembered (1933-2012) », *blog personnel,* (12 juin 2012).