

Normalisation de la surveillance et propagation de la manipulation : quelle place pour la liberté d'autodétermination ?

Par Suzanne Vergnolle

Docteure en droit de l'université Paris II Panthéon-Assas

Post-doc à l'Université de Lausanne et à l'Institut Suisse de droit comparé

1. Introduction. La surveillance prend des formes multiples et provient de sources diverses. Naturellement, la première référence qui vient à l'esprit est celle d'un État qui souhaite protéger son territoire contre des attaques extérieures. Pour autant, d'autres formes de surveillance existent et leurs effets sur les personnes ne doivent pas être sous-estimés. Avec le développement de l'informatique et de la mise en réseau des ordinateurs, les moyens pour surveiller les personnes (physiques et morales) se sont démultipliés et ont gagné en précision. En effet, il n'est plus beaucoup de gestes quotidiens, d'achats, de déplacements, de décisions personnelles ou professionnelles qui ne soient pas enregistrés dans une base de données¹. Cet enregistrement systématique contribue à l'élaboration de portraits de plus en plus précis et détaillés des personnes². Comme le remarquait déjà le doyen Hauriou à propos de la personnalité juridique, « plus la civilisation progresse, plus la personnalité juridique se rapproche de la personnalité réelle ; ce qu'il y a d'excessif dans sa continuité artificielle s'atténue »³. Désormais, il semble que plus l'informatique progresse, plus la personnalité numérique se rapproche de la personnalité réelle⁴. L'enregistrement des goûts, hésitations, attirances, déceptions, contribue à atténuer la distinction entre la personne et les données qui la représentent.

2. Nous vivons donc dans une *société de données*, dans laquelle tout mouvement, même trivial ou sans intérêt apparent, est retranscrit et enregistré⁵. Une fois enregistré, des traitements peuvent être effectués sur ces données notamment avec l'objectif de manipuler ou d'influencer les personnes concernées. La publicité ciblée est l'un des versants les plus

¹ D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data*, Seuil, 2015, p. 7.

² À ce titre, les autoportraits de Cindy Sherman dans lesquels l'artiste se met en scène dans des costumes et des attitudes variés, invitent l'observateur à se questionner sur l'identité et ses modes de représentation.

³ M. Hauriou, « De la personnalité comme élément de la réalité sociale », *Revue générale du droit* 1898, p. 20.

⁴ Sur ces différences, v. déjà : P. Mouron, « Internet et identité virtuelle des personnes », *Revue de la recherche juridique - droit prospectif* 2008, n° 124, p. 2409.

⁵ Sur le besoin de prendre appui sur des choses pour établir des mesures, voir l'analyse d'Alain Desrosières de la règle de méthodologie sociologique de Durkheim selon laquelle « il faut traiter les faits sociaux comme des choses », A. Desrosières, *La politique des grands nombres. Histoire de la raison statistique*, La Découverte, 2010, p. 7 s.

connus de cette manipulation⁶. Au mieux, le caractère grossier de la publicité excède le voyageur qui vient d'acheter un billet d'avion et qui se voit proposer une location de voiture au meilleur prix. Au pire, cette publicité façonne insidieusement ses intérêts. La plupart de nos activités sont désormais soumises à ces algorithmes de recommandation⁷. Notre façon de nous informer, nos préférences cinématographiques, nos opinions politiques, nos goûts gastronomiques sont façonnés par ces recommandations⁸. Publicité après publicité, vidéo après vidéo, article après article, la personne est influencée et manipulée. La plupart du temps, ces manipulations servent des intérêts extérieurs, souvent ceux des plateformes numériques sur lesquels ces contenus sont visualisés.

Avec de telles manipulations, opérées à l'insu des utilisateurs, la capacité de développer sa personnalité de manière libre et autonome existe-t-elle encore ? En d'autres termes, le droit positif offre-t-il des garanties suffisantes pour protéger le libre développement individuel ?

3. Plan. Pour savoir si le droit répond efficacement aux dangers pesant sur la protection des personnes, encore faut-il identifier les risques que l'informatique et la mise en réseau des ordinateurs font peser sur les libertés individuelles. Après avoir analysé les atteintes classiques aux personnes résultant des traitements de données à caractère personnel (§ I), il faudra s'intéresser aux nouvelles atteintes (§ II).

§ I. Les atteintes classiques aux personnes résultant des traitements de données à caractère personnel

4. Plan. Ce sont les développements informatiques (A) et les risques qu'ils font peser sur les personnes qui ont encouragé des adaptations juridiques (B).

A. Les développements informatiques

5. Les risques liés à la mémorisation informatique. C'est dans les années 1960, avec la diversification des tâches effectuées par les ordinateurs, que la question de la protection

⁶ V. parmi de nombreux travaux de sociologie sur cette question, H. Le Crosnier, « Usage des traces par la publicité comportementale », in *Traces numériques. De la production à l'interprétation*, dir. B. Galinon-Melenec et S. Zlitni, CNRS, 2013, p. 91 s., spéc. p. 95.

⁷ Le terme algorithme vient de l'arabe, *al-Kharezmi*, surnom d'un savant arabe du IX^e siècle, et signifie « ensemble de règles dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations », v. Dictionnaire Larousse, *Dictionnaire de français*, V^o « Algorithme ».

⁸ P. de Filippi, « Gouvernance algorithmique : vie privée et autonomie individuelle à l'ère des *Big Data* », in *Open data & data protection : nouveaux défis pour la vie privée*, dir. D. Bourcier et P. de Filippi, Mare & Martin, 2016.

des données enregistrées par ces machines a commencé à se poser. Initialement, seules les administrations et les grandes entreprises pouvaient s'offrir ces assistants utiles, notamment pour des raisons de budget et de place⁹. L'apparition des ordinateurs personnels et leur diffusion progressive au grand public à la fin des années 1970 ont modifié en profondeur la manière dont les humains traitent l'information, notamment celle relative aux personnes¹⁰. Les fiches perforées cèdent la place aux bases de données rendant l'accès, le traitement et la conservation des données plus rapides et plus simples. Le développement des réseaux a contribué aux transferts des bases de données entre les pays, et les moteurs de recherche ont facilité les opérations de croisement et de synthèse de fichiers¹¹. Rapidement, l'informatique n'est plus réservée à une élite, elle se répand partout : dans les banques, les entreprises, les foyers... Cette diffusion de l'informatique a banalisé la collecte d'informations nominatives. Pourtant, les risques induits par ces enregistrements et mémorisations sont considérables. Contrairement au cerveau humain, la mémoire d'un ordinateur n'oublie pas : la conservation informatique prolonge donc la durée de traitement et de sauvegarde des informations¹². Par ailleurs, l'informatique permet de traiter les informations bien plus rapidement et efficacement qu'un humain. À ces éléments s'ajoute la possibilité d'interconnecter des fichiers se trouvant à des endroits différents, faisant ainsi peser des risques nouveaux de centralisation des informations. L'ensemble de ces facteurs ont démultiplié les risques d'atteintes aux personnes. Ainsi, c'est parce que les ordinateurs sont capables de manier de très grandes quantités de données, dans des temps inédits, que les dangers liés à leur utilisation ont augmenté.

6. Le développement d'une société de surveillance. Tous ces éléments ont favorisé le développement d'une société de surveillance et de contrôle, se rapprochant dangereusement de celle décrite par Georges Orwell dans son roman emblématique *1984*¹³ ou des mécanismes de surveillance retracés par les philosophes Michel Foucault¹⁴

⁹ Comme le remarquait déjà Monsieur Michel Volle en 1999, « 50 ans séparent le premier ordinateur (50 tonnes, 25 kW, quelques milliers de positions de mémoire, cent instructions par seconde) du microprocesseur Pentium (quelques grammes, 25 watts, 8 à 32 Megaoctets de mémoire, 100 MIPS). L'évolution n'est pas terminée : la loi de Moore (...) se vérifie depuis le début des années 70. Les chercheurs pensent qu'elle jouera jusque vers 2010 », v. M. Volle, *Économie des nouvelles technologies. Internet, télécommunications, informatique, audiovisuel, transport aérien*, Economica, 1999.

¹⁰ V. sur l'évolution du traitement des informations du recensement aux États-Unis, v. Census Bureau, « A monograph on confidentiality and privacy in the U.S. census », 2001.

¹¹ G. Braibant, « Données personnelles et société de l'information. Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46 », La Documentation française, 1998, p. 1.

¹² Sur le droit à l'oubli, v. *infra*, n°s **Error! Reference source not found.** s.

¹³ G. Orwell, *1984*, Gallimard, 1950.

¹⁴ M. Foucault, *Surveiller et punir. Naissance de la prison*, Gallimard, 1975, p. 202 s.

et Gilles Deleuze¹⁵. Ces nouvelles modalités de traitement de l'information font peser des risques inédits sur la vie privée puisqu'elles rendent possible une surveillance diffuse, généralisée et à faible coût. Une telle normalisation de la surveillance n'atténue pas pour autant ses effets qui, selon certains auteurs, seraient comparables à ceux des barreaux d'une prison¹⁶. Ce n'est sans doute pas un hasard si les frères Bentham ont appliqué le concept de Panoptique¹⁷ aux établissements surveillant les personnes, notamment aux prisons. La spécificité de ce bâtiment circulaire était de permettre l'observation à tout moment des faits et gestes des détenus grâce à une vision totale sur l'ensemble des cellules¹⁸. Lorsque Foucault transpose l'analyse de la structure du Panoptique à l'organisation sociale, celle-ci ressort métamorphosée en une société disciplinaire axée sur le contrôle social. Foucault remarque que la sensation de visibilité induite par la structure du Panoptique assure le fonctionnement automatique du pouvoir : la surveillance est permanente dans ses effets, même si elle est discontinuée dans son action¹⁹. Confirmant ces analyses, de nombreuses études effectuées en sciences sociales ont montré que le sentiment d'être sous surveillance a d'importants effets sur la santé, tant physique que morale, et engendre des sentiments de faible estime de soi, de dépression et d'anxiété²⁰. C'est notamment pour encadrer ces risques que les législations relatives aux données à caractère personnel sont apparues.

B. Les développements juridiques

7. L'adoption des législations protégeant les données personnelles. Plusieurs principes du droit des données à caractère personnel permettent de répondre aux dangers liés au développement de cette société de surveillance. Par exemple, le principe de transparence, interdisant la collecte secrète des données ; le principe de pertinence, encadrant les finalités des traitements ; le principe de sécurité, prescrivant l'obligation de protéger les données contre des accès par des tiers ; ou encore les droits des personnes sur leurs données²¹. La loi du 6 janvier 1978 reconnaissait ainsi aux personnes concernées

¹⁵ G. Deleuze, « Post-scriptum sur les sociétés de contrôle », *Pourparlers* 1990.

¹⁶ « A man without privacy is a man without dignity ; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars », Z. Cowen, *The private man*, The Boyer Lectures Australian Broadcasting Commission, 1969, p. 9 s.

¹⁷ Le Panoptique est un type architectural imaginé par les frères Bentham. La structure du bâtiment est simple : une tour centrale est entourée de cellules individuelles percées par de larges fenêtres laissant la lumière traverser la cellule.

¹⁸ J. Bentham, *Panopticon or the inspection house*, vol. 1, Payne, 1791, p. 63.

¹⁹ M. Foucault, *Surveiller et punir. Naissance de la prison*, Gallimard, 1975, p. 234.

²⁰ B. Schneier, *Data and Goliath : The hidden battles to collect your data and control your world*, Norton & Company, 2015, p. 127.

²¹ V. not. United States Department of Health, Education and Welfare, « Records, computers, and the rights of citizens », 1973, p. 40 s. ; OCDE, Lignes directrices du 23 sept. 1980 sur la vie privée et les flux transfrontières de données à caractère personnel.

plusieurs droits pour que celles-ci gardent le contrôle sur leurs informations, notamment le droit d'accès, le droit d'opposition, ou le droit de mettre à jour les données²². La volonté de garantir un droit de contrôle aux personnes concernées est si centrale qu'en 2016, les législateurs européen et français l'ont érigé en principe général de la matière²³. Cette prérogative de contrôle se rapproche du concept allemand d'autodétermination informationnelle.

8. L'autodétermination informationnelle, un principe en rapport avec le pouvoir de contrôle. Le droit à l'autodétermination informationnelle a été consacré par la Cour constitutionnelle fédérale allemande dans un arrêt du 15 décembre 1983²⁴. La juridiction allemande l'avait défini comme « le pouvoir de l'individu de décider lui-même, sur la base du concept d'autodétermination, quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui »²⁵. Pour certains auteurs, ce principe établit une conception renouvelée du rapport de la personne avec ses données, puisque chaque individu bénéficierait d'une véritable autonomie dans leur gestion²⁶. En France, le Conseil d'État a reconnu dans son rapport sur *Le numérique et les droits fondamentaux* l'intérêt de ce concept, tout en rappelant que « la seule affirmation de ce droit ne permet pas de le rendre effectif et les instruments de la protection des données doivent être profondément transformés pour y parvenir »²⁷. Ainsi, le droit français des données personnelles reconnaît, au travers de plusieurs prérogatives, un pouvoir de contrôle à l'égard des données, mais celui-ci n'englobe pas complètement un droit à l'autodétermination informationnelle. Ce pouvoir de contrôle suffit-il à protéger de manière efficace les personnes contre les nouvelles formes d'atteintes aux personnes issues des traitements de données personnelles ?

²² Sur les droits reconnus aux personnes, v. P. Kayser, *La protection de la vie privée*, 2^e éd., Economica, 1990, n^{os} 289 s., p. 367 s.

²³ L'article 54 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique a complété l'article 1^{er} de la loi Informatique et libertés par une phrase prévoyant que « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ». Le législateur européen a, quant à lui, proclamé dans le considérant 7 du règlement UE n° 679/2016 sur la protection des données que « Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant ».

²⁴ BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983, pour une analyse de l'arrêt en français, v. Y. Pouillet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité*, dir. K. Benyekhlef et P. Trudel, Thémis, 2009, p. 157 s. Pour une analyse des précédents arrêts ayant conduit à cette reconnaissance, v. C. Koumpli, *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, th. Paris I, 2019, p. 100 s.

²⁵ BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983.

²⁶ J. Rochfeld, « Données personnelles : quels nouveaux droits ? », *Statistiques et société* 2017, vol. 5, n° 1, p. 47.

²⁷ Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 267.

§ II. Les atteintes nouvelles aux personnes résultant des traitements de données à caractère personnel

9. Plan. Il est courant d'affirmer que les traitements de données à caractère personnel sont intrusifs (A). Pour mieux circonscrire les risques engendrés par ces traitements, il convient de reconnaître une liberté d'autodétermination (B).

A. Des traitements intrusifs

10. L'explosion des quantités de données produites, facilitant un traçage des personnes sans précédent. Le numérique, réservé pendant plusieurs décennies à une communauté d'experts, s'est amplement popularisé. L'avènement du Web 2.0 a acté le passage d'un web statique au web social, dans lequel la dimension de partage et d'échange d'informations est centrale. L'explosion du nombre d'utilisateurs a engendré une surabondance des données produites, et les risques identifiés au début du développement de l'informatique se sont amplifiés.

Progressivement, tout est devenu quantifiable et quantifié, nos moindres actions sont traduites en données pour ensuite être analysées²⁸. Chaque pas, chaque activité physique, chaque site consulté, génère désormais des données. Une fois consignées dans une base de données, ces informations sont ensuite traitées pour produire un nouveau savoir sur la personne : c'est l'arrivée du Web 3.0, centré autour de l'humain et de la personnalisation de contenus²⁹. Les algorithmes de recommandation rythment, plus que jamais, les contenus visionnés, les trajets empruntés, les musiques écoutées ou les restaurants choisis.

11. L'explosion des producteurs de données. Longtemps élément central de la collecte d'informations personnelles, l'ordinateur partage depuis près de deux décennies cette attribution avec les *smartphones*. Le lancement de l'iPhone en 2007 acte définitivement l'entrée de ces micro-ordinateurs dans nos vies quotidiennes. De petite taille et avec de multiples fonctionnalités, ils se déplacent avec leurs détenteurs et permettent une collecte de données en continu. Ils ont ainsi contribué à l'augmentation de données collectées, mais surtout à leur diversité, leur qualité et leur précision. Tels de véritables petits mouchards dans nos poches, les *smartphones* permettent de collecter un

²⁸ D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data*, Seuil, 2015, p. 7.

²⁹ Pour une présentation de l'évolution du Web, v. O. Le Deuff, « Du web 2.0 à l'Arcadie », *URFIST Info* 2007.

nombre considérable de données. La moindre seconde d'attente est désormais occupée par ce petit écran : on lève un pouce pour montrer son approbation, on prend une photo du coucher de soleil pour la publier sur les réseaux sociaux, on utilise son application de navigation connectée pour trouver la route la plus rapide³⁰. Toutes ces actions, en apparence parfaitement anodines, laissent d'invisibles petites traces, permettant ensuite de broser un portrait de l'utilisateur³¹.

Avec la mise en réseau des ordinateurs, puis le développement du *big data*, les responsables du traitement ont préféré centraliser les données sur leurs serveurs pour y effectuer de l'apprentissage automatique³². Cette centralisation des données était nécessaire parce que le développement des modèles exigeait une puissance de calcul plus large que celle disponible sur l'appareil de l'utilisateur. Pour autant, cette centralisation présente d'importants risques, tant en matière de sécurité des données qu'en matière de protection de la vie privée. Au cours de la dernière décennie, l'augmentation de la puissance de calcul disponible sur les *smartphones* a permis de mettre en œuvre des traitements d'apprentissage directement sur l'appareil de l'utilisateur, réduisant ainsi la quantité d'informations transférées aux responsables du traitement, tout en permettant d'améliorer le modèle grâce à l'envoi de statistiques agrégées³³. Pour autant, cette pratique est loin d'être diffuse et la centralisation des données demeure encore le modèle dominant.

En plus des *smartphones*, de nombreux autres objets connectés³⁴ envahissent notre quotidien et collectent toujours plus de données sur nos vies : l'œuf minuteur de la cuisine est remplacé par un assistant vocal « intelligent »³⁵, la poupée en porcelaine laisse place

³⁰ Selon une opinion doctrinale récente, le droit devrait également protéger l'attention, v. C. Zolynski, M. Le Roy et F. Levin, « L'économie de l'attention saisie par le droit », *Daloz IP/IT* 2019, p. 614. Sur la transformation apportée par Internet dans la production de contenus en ligne et le déluge d'informations auquel les personnes sont désormais confrontées, v. E. Pariser, *The filter bubble*, Penguin Press, 2011, p. 32. Pour une étude des frontières entre la productivité et la distraction, v. S. Genner, « ON / OFF. Risks and rewards of the anytime-anywhere Internet », University of Zurich, 2015, p. 57.

³¹ Sur le traçage des personnes, v. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes », in *Mélanges J. Hauser*, Dalloz, 2012, p. 619 s., n° 1, spéc. p. 619 s. Sur le recours au *data mining* aux fins de profilage, v. not. Y. Pouillet, *La vie privée à l'heure de la société numérique*, Larcier, 2019, n° 13, p. 29 s. Sur l'encadrement du profilage par le règlement européen, v. G29, WP 251 rév. 01, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 févr. 2018, p. 5 s.

³² L'apprentissage automatique est une forme d'intelligence artificielle qui permet à un système d'apprendre à partir des données et non pas à l'aide d'une programmation explicite, J. Hurwitz et D. Kirsch, *Machine learning for dummies*, John Wiley & Sons, 2018, p. 4.

³³ La technique d'apprentissage fédéré est utilisée pour améliorer la qualité des dictionnaires d'auto-correction sur les *smartphones*, K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal et K. Seth, « Privacy secure aggregation for privacy-preserving machine learning », *CCS'* oct. 2017, Dallas.

³⁴ L'objet connecté est classiquement défini comme « un dispositif matériel permettant de collecter, stocker, transmettre et traiter des données issues du monde physique », v. E. Daoud et F. Plénacoste, « Cybersécurité et objets connectés », *Daloz IP/IT* 2016, p. 409.

³⁵ Les assistants vocaux, notamment ceux de Google (Echo), Amazon (Alexa) et Apple (Siri), ont fait l'objet de polémiques quant aux enregistrements des interactions, à leur transmission et à leur écoute par des employés de ces entreprises, v. pour un bref résumé N. Six, « Avec des enceintes connectées, des conversations loin d'être privées », *Le Monde* 12 avr. 2019. Sur ce sujet, v. CNIL, « À votre écoute. Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux », Livre Blanc, n° 1, 2020.

à la poupée connectée, et la montre analogique est substituée par une montre connectée enregistrant chaque battement de notre cœur. Ces objets envahissent nos foyers et affinent, grâce aux données qu'ils collectent, les traits de nos vies. Pour le dire simplement, les données sont générées tout le temps et stockées partout.

Le nombre de traces, leur variété et leur précision favorisent ainsi l'émergence d'un modèle de société fondé sur le prédictif et la personnalisation : la société de surveillance est alors couplée à celle de manipulation. C'est effectivement l'un des dangers liés à l'expansion des traitements de données et à la diffusion des traitements de données personnalisés.

12. Une personnalisation des services. La collecte croissante de données entraîne une meilleure connaissance des personnes, laquelle facilite ensuite leur manipulation³⁶. Cette collecte de données n'est que la première étape d'un processus complexe : les données sont ensuite consignées dans de gigantesques bases de données afin de leur appliquer des méthodes de traitement visant à inférer de nouvelles informations sur les personnes³⁷. Dès 1978, le législateur s'était montré très frileux à l'égard des décisions prises sur le fondement des traitements automatisés en consacrant, dans les premiers articles de la loi, des dispositions visant à les encadrer, voire à les interdire³⁸. Cette interdiction se limitait toutefois aux seules décisions de justice et à quelques décisions administratives ou privées³⁹. En effet, le législateur de 1978 ne pouvait pas anticiper l'ampleur des traitements à venir. Plus récemment, la Commission européenne a proposé, dans sa proposition de Règlement sur l'intelligence artificielle d'avril 2021, d'interdire les systèmes d'intelligence artificielle altérant substantiellement le comportement des personnes sans que celles-ci ne s'en aperçoivent et qui causent un préjudice physique ou psychologique⁴⁰. Les législateurs tentent donc de prévenir les effets négatifs que pourraient avoir les traitements de données sur la liberté de la vie privée. Celle-ci est

³⁶ Sur l'évolution des déterminismes sociologiques des comportements et des opinions, v. D. Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data*, Seuil, 2015, p. 47 s. citant P. Bourdieu, *La distinction. critique sociale du jugement*, Minuit, 1979.

³⁷ Le volume de données collectées donne du sens à des informations apparaissant pourtant, à première vue, très anodines ou clairsemées, v. P. Delort, *Le big data*, 2^e éd., PUF, 2018, p. 29 ; Y. Pouillet, *La vie privée à l'heure de la société numérique*, Larcier, 2019, n° 13, p. 29 s.

³⁸ L'article 2 de cette loi interdisait les décisions de justice, administrative ou privée impliquant une appréciation sur un comportement humain fondée sur un traitement automatisé d'informations (notamment lorsqu'il est fondé sur un profil ou une analyse de la personnalité de l'intéressé). L'article 3 garantissait aux personnes le droit de connaître et contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats leur sont opposés. Ces principes avaient été repris dans l'article 10 de la loi n° 78-17 du 6 janvier 1978 telle que modifiée par la loi n° 2004-801 du 6 août 2004.

³⁹ V. *infra*, n° **Error! Reference source not found.**

⁴⁰ Article 5 de la proposition de règlement UE établissant des règles harmonisées concernant l'intelligence artificielle, 21 avr. 2021.

définie comme un ensemble de possibilités d'actions infinies qui « constituent des phénomènes de non-droit (lire tel livre ou tel autre, porter des chaussettes bleues ou vertes, se réveiller tôt ou tard...) ; elles n'entrent dans le domaine juridique que pour déterminer leurs limites et donc leur degré de protection (l'ordre public ou un tiers prétendent m'interdire le port de chaussettes bleues : j'avance alors un droit au respect de la liberté) »⁴¹. Mais, qu'en est-il lorsqu'un tiers ne vient pas m'interdire de porter des chaussettes bleues, mais me manipule pour que je porte des chaussettes vertes ? La question de la mise en œuvre de la liberté de la vie privée trouve un écho particulier lorsque des traitements opérés sur des données personnelles visent à manipuler la personne afin qu'elle adopte un certain comportement. Madame Judith Rochfeld évoquait précisément ces risques en considérant que « dès lors qu'il devient possible [...] de prédire nos comportements, il est également possible de les orienter : de nouveaux modes d'influence se développent dont nous n'avons pas toujours pleinement conscience »⁴². Ce sont notamment les techniques liées au profilage qui rendent possibles de telles manipulations.

13. L'atteinte à la liberté personnelle par le profilage. Le profilage est un traitement consistant à utiliser des données à caractère personnel pour évaluer, par le biais d'analyses ou de prédictions, certains aspects personnels d'une personne physique⁴³. Lorsqu'elle est profilée, la personne est enfermée dans des catégories générales de comportement afin de prédire, à l'avance, ses agissements futurs. Schématisée et objectivée de la sorte, la personne se voit nier l'existence d'un *libre arbitre* et sa faculté d'agir différemment des autres dans une même situation⁴⁴. Le profil instaure donc une forme de déterminisme incompatible avec l'attribut le plus précieux de la liberté : le choix d'un *futur*

⁴¹ J.-C. Saint-Pau, « La distinction des droits de la personnalité et de l'action en responsabilité civile », in *Mélanges H. Groutel*, Litec, 2006, p. 404 s., n° 9, spéc. p. 412 ; P. Kayser, *La protection de la vie privée par le droit*, 3^e éd., Economica, 1995, n^{os} 18 s., p. 45 s.

⁴² J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in *Les biens numériques*, dir. E. Netter et A. Chaigneau, CEPRISCA, 2015, p. 221 s., n° 4, spéc. p. 225.

⁴³ L'article 4 du règlement UE n° 2016/679 définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

⁴⁴ J. Eynard, *Les données personnelles, quelle définition pour un régime de protection efficace ?*, th. Toulouse I, 2013, Michalon, p. 184 ; S. Merabet, *Vers un droit de l'intelligence artificielle*, th. Aix-Marseille, 2018, Dalloz, n^{os} 246 s., p. 238 s.

*autodéterminé*⁴⁵. Avec cette conception de la personne, on nie les qualités qui font d'elle un être humain⁴⁶.

À ce stade de l'analyse, deux observations peuvent être formulées : d'une part, la tendance de l'homme à vouloir quantifier les choses pour éviter l'imprévisibilité, le pousse à recourir à des outils (notamment informatiques et numériques) l'aidant à mieux anticiper et prédire l'avenir, et d'autre part, les algorithmes de profilage présentent le risque de nier la complexité du comportement humain en enfermant la personne dans un carcan trop rigide de choix prédéfinis⁴⁷. Ces outils sont souvent loin d'être neutres pour les personnes, puisqu'ils peuvent avoir d'importantes implications sur l'autonomie individuelle (en considérant que la personne va agir de la même façon qu'une autre personne placée dans la même situation), et qu'ils tendent à reproduire les biais et renforcer les discriminations⁴⁸.

Ces techniques sont largement utilisées par le secteur privé qui a recours, notamment au sein des compagnies d'assurance et des établissements bancaires, à des systèmes de *scoring*⁴⁹. D'autres branches du secteur privé, notamment les entreprises présentes sur Internet, utilisent également le profilage pour influencer leurs utilisateurs. Les risques liés à la manipulation sont, avec les traitements automatisés de données, accrus.

⁴⁵ F. Rigaux, *La protection de la vie privée et les autres biens de la personnalité*, Bruylant, 1990, n° 537, p. 597 s.

⁴⁶ D'ailleurs, pour Emmanuel Mounier, « la personne est ce qui ne peut être répété deux fois », E. Mounier, *Le personnalisme*, PUF, 2010, p. 49. Monsieur Guillaume Lécuyer affirmait également qu'au-delà de son appartenance à l'humanité, l'individu est un être unique c'est-à-dire différent de son prochain, v. G. Lécuyer, *Liberté d'expression et responsabilité. Étude de droit privé*, th. Paris I, 2006, n° 4, p. 5.

⁴⁷ V. not. J. Rochfeld, « La vie tracée ou le code civil doit-il protéger la présence numérique des personnes », in *Mélanges J. Hauser*, Dalloz, 2012, p. 619 s., n° 10, spéc. p. 630. Dans cet article, Madame Judith Rochfeld rappelle l'importance des algorithmes derrière les traces laissées par les personnes sur Internet. Madame Antoinette Rouvroy critique aussi ces catégorisations automatiques en rappelant que les « opérations de *datamining* et de profilage n'apparaissent objectives et égalitaires que dans la mesure où l'on ignore qu'elles sont aveugles et sourdes à tout ce qui, du monde – les idiosyncrasies individuelles, les raisons des actions – ne se laisse pas traduire sous une forme numérique », v. A. Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », in Conseil d'État, « Le numérique et les droits fondamentaux », *Rapport Public 2014*, La Documentation française, 2014, p. 416.

⁴⁸ White House, « Big data : a report on algorithmic systems, opportunity and civil rights », *Executive office of the President* mai 2016 ; v. aussi, J. Angwin, J. Larson, S. Mattu et L. Kirchner, « Machine bias. There's software used across the country to predict future criminals. And it's biased against blacks », *ProPublica* 23 mai 2016. Plus récemment aux États-Unis, 27 organisations ont signé une lettre ouverte à destination de la FTC pour l'inviter à prendre en compte les effets des pratiques de politiques de personnalisation de données sur les biais et discriminations, v. Working group, « Letter to FTC : data, biais, and disparate impact », 18 sept. 2020. Le Conseil de l'Europe s'est également intéressé à ces questions, v. not. F. Zuiderveen Borgesius, « Discrimination, artificial intelligence and algorithmic decision-making », Conseil de l'Europe 2018. Pour des travaux sur le droit français, v. not., J. Charpenet et C. Lequesne Roth, « Discrimination et biais générés. Les lacunes juridiques de l'audit algorithmique », *D.* 2019, p. 1852.

⁴⁹ La CNIL avait d'ailleurs adopté une autorisation unique pour les traitements mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit, CNIL, délibération n° 2006-019 du 2 février 2006 portant autorisation unique de certains traitements de données à caractère personnel mis en œuvre par les établissements de crédit pour aider à l'évaluation et à la sélection des risques en matière d'octroi de crédit (décision d'autorisation unique n° AU-005).

14. Des traitements effectués à des fins de manipulation. Une part croissante de la doctrine anglo-saxonne s'intéresse aux interactions entre le droit et la manipulation. Cette dernière est définie comme l'action par laquelle on cherche à influencer l'opinion, les décisions, la conduite d'une ou plusieurs personnes, à des fins non avouées et par des moyens détournés⁵⁰. Déjà en 1999, Messieurs Jon Hanson et Douglas Kysar expliquaient que le format de l'information et le pouvoir de présentation des choix ont un rôle conséquent dans la prise de décision⁵¹. Ceux qui réussissent à influencer les biais cognitifs⁵² ont le pouvoir de manipuler les personnes dans leurs décisions et sont donc investis d'un *pouvoir d'influence*. Si la manipulation est un trait fondamental des interactions humaines⁵³, les pratiques numériques ont modifié en profondeur ses méthodes, formes et effets⁵⁴. La capacité de personnaliser les contenus, de les adapter en fonction des expériences précédentes, ainsi que les outils d'analyse de données permettent des formes de persuasion révolutionnaires⁵⁵. Le numérique rend cette manipulation invisible pour la plupart des utilisateurs. Plusieurs exemples illustrent ces influences et les risques qu'elles engendrent pour la protection des personnes.

15. Des traitements effectués à des fins de manipulation, illustrations. En 2014, Facebook a reconnu avoir manipulé les informations visibles par certains de ses utilisateurs pour étudier le phénomène de « contagion émotionnelle ». Deux ans plus tôt, Facebook avait autorisé des chercheurs à afficher dans le fil d'actualité de certains utilisateurs des publications tantôt positives tantôt négatives en vue d'analyser le résultat produit sur leurs émotions⁵⁶. Une telle étude illustre bien les effets des traitements de

⁵⁰ *Dictionnaire de l'Académie française*, 9^e éd., V^o « Manipulation », sens 4.

⁵¹ J. Hanson et D. Kysar, « Taking behavioralism seriously : the problem of market manipulation », *New York University Law Review* 1999, vol. 74, p. 630 s. [74 N.Y.U L. REV. 630], spéc. p. 635.

⁵² La nature des biais cognitifs est le plus souvent définie comme des tendances à produire des croyances ou des jugements erronés en vertu du fait qu'ils violent certaines règles de raisonnement, M. van Loon, « Biais cognitifs », in *L'Eycyclopédie philosophique*, dir. M. Kristanek. D'ailleurs des études se sont intéressées à l'influence du design des bandeaux de cookies sur l'obtention du consentement, v. not. C. Utz, M. Degeling, S. Fahl, F. Schaub et T. Holz, « (Un)informed consent : studying GDPR consent notices in the field », *CCS'* nov. 2019, Londres ; M. Nouwens, I. Liccardi, M. Veale, D. Karger et L. Kagal, « Dark patterns after the GDPR : scraping consent pop-ups and demonstrating their influence », *CHI'* avr. 20, Honolulu.

⁵³ Sur les pouvoirs de manipulation, v. R.-V. Joule et J.-L. Beauvois, *Petit traité de manipulation à l'usage des honnêtes gens*, PUG, 1987, réimpr. 2014.

⁵⁴ C. Sunstein, « Fifty shades of manipulation », *Journal of Marketing Behavior* 2016, vol. 1, p. 213 s. [1 J. MARKETING BEHAV. 213] spéc. p. 244.

⁵⁵ T. Zarsky, « Privacy and manipulation in the digital age », *Theoretical Inquiries in Law* 2019, vol. 20, p. 158 s. [20 THEOR. INQ. LAW 158], spéc. p. 169.

⁵⁶ A. Kramer, J. Guillory et J. Hancock, « Experimental evidence on massive-scale emotional contagion through social networks », *Proceedings of the National Academy of Sciences of the United States of America* 2014, vol. 111, p. 8788 s. [111 PROC. NATL. ACAD. SCI. USA 8788].

données et leur impact sur les personnes : notre humeur devient un objet malléable au gré de la curiosité des responsables du traitement⁵⁷.

Dans un autre domaine, l'algorithme de recommandations de vidéos de YouTube illustre également les effets négatifs de certains traitements de données à caractère personnel. L'un des principaux objectifs de l'algorithme de YouTube⁵⁸ est de retenir le plus longtemps possible l'utilisateur sur le site, afin de lui montrer de la publicité et d'augmenter les revenus publicitaires de la plateforme⁵⁹. Pour réaliser cet objectif, l'algorithme fait évoluer graduellement l'intensité des vidéos qu'il recommande⁶⁰. L'utilisateur se voit ainsi proposer des vidéos confirmant son opinion ou du contenu sensationnel ou radical⁶¹. Selon le *New York Times*, 70 % du temps de visionnage sur YouTube serait choisi par l'algorithme de recommandation⁶².

Ces deux exemples illustrent les défis modernes auxquels le droit des données à caractère personnel doit répondre pour garantir une protection effective des personnes.

B. La reconnaissance de la liberté d'autodétermination

16. La liberté d'autodétermination. Pendant plusieurs décennies, le droit à l'autonomie personnelle permettait d'ériger la vie privée comme une valeur sociale protégeant la personne contre la société de surveillance⁶³. Bien que ce droit soit défini largement par la CEDH qui l'entend comme « le droit de mener sa vie comme on l'entend avec un minimum d'ingérence »⁶⁴, il a désormais besoin d'évoluer afin de protéger les personnes contre une société de manipulation. L'augmentation considérable du nombre de traitements, la banalisation du profilage et de la personnalisation des services

⁵⁷ R. Schroeder, « Big data and the brave new world of social media research », *Big Data and Society* 2014.

⁵⁸ Pour une analyse de l'algorithme fournie par trois employés de l'entreprise Google, v. P. Covington, J. Adams et E. Sargin, « Deep neural networks for YouTube recommendations », *RecSys* sept. 2016. V. déjà en 2010 plusieurs employés de Google avaient également publié un article sur le système de recommandation de YouTube, v. J. Davidson, B. Liebald, J. Liu, P. Nandy et T. Van Vleet, « The YouTube video recommendation system », *RecSys* sept. 2010.

⁵⁹ Selon Monsieur Guillaume Chaslot, ancien employé de Google, YouTube gagnerait environ 1 centime d'euro par heure de visionnage pour chaque utilisateur. Sur ce sujet, v. les travaux de la plateforme AlgoTransparency.

⁶⁰ M. Ledwich et A. Zaitsev, « Algorithmic extremism : examining YouTube's rabbit hole of radicalization », *Frist Monday* 25 févr. 2020.

⁶¹ V. not. P. Lewis, « 'Fiction is outperforming reality' : how YouTube's algorithm distorts truth », *The Guardian* 2 févr. 2018 ; M. Fisher et A. Taub, « How YouTube radicalized Brazil », *The New York Times* 11 août 2019. Une récente étude montre que l'algorithme de YouTube a tendance à diriger l'utilisateur vers du contenu de plus en plus radical, v. M. Ledwich et A. Zaitsev, « Algorithmic extremism : examining YouTube's rabbit hole of radicalization », *Frist Monday* 25 févr. 2020, § 5.

⁶² M. Fisher et A. Taub, « How YouTube radicalized Brazil », *The New York Times* 11 août 2019.

⁶³ P. Malaurie et L. Aynès, *Droit des personnes. La protection des mineurs et des majeurs*, 8^e éd., LGDJ, 2015, n° 312, p. 151 s.

⁶⁴ V. not. CEDH, 29 avr. 2002, *Pretty c. Royaume-Uni*, n° 2346/02, § 62 ; CEDH, 17 févr. 2005, *K.A. et A.D. c. Belgique*, n° 42758/98 et n° 45558/99, § 83. Pour une analyse de ces jurisprudences, v. F. Sudre (dir.), *Droit européen et international des droits de l'homme*, 14^e éd., PUF, 2019, n°s 490 s., p. 741 s. Sur le domaine de l'autonomie personnelle, v. M. Fabre-Magnan, « Le domaine de l'autonomie personnelle. Indisponibilité du corps humain et justice sociale », *D.* 2008, p. 31.

contribuent à dessiner une représentation très précise des personnes, permettant ensuite de mieux les influencer. Ce n'est pas seulement l'autonomie individuelle qui est atteinte par ces traitements, puisqu'en apparence, les personnes peuvent toujours agir comme bon leur semble ; *c'est l'essence même de leur capacité d'agir librement qui est touchée*. Épiée, profilée et influencée, la personne peut-elle encore former librement ses désirs et sa volonté ?

17. La liberté d'autodétermination en philosophie. Les théories philosophiques autour du concept de libre arbitre et de liberté sont éclairantes. Par exemple, Monsieur Robert Kane, philosophe analytique contemporain, a conceptualisé cinq types de liberté, parmi lesquelles figure la liberté d'autodétermination⁶⁵. Celle-ci serait « le pouvoir ou la capacité à agir de sa propre volonté libre, au sens d'une volonté (caractères, motifs et buts) créée par soi-même ; une volonté que l'on est soi-même, jusqu'à un certain degré, ultimement responsable d'avoir formée »⁶⁶. Selon cette conception, une personne ne peut être libre que si elle a contribué à forger elle-même son propre caractère et donc, sa propre volonté⁶⁷. Le concept de liberté d'autodétermination est donc *nécessaire* à la réalisation de celui d'autonomie personnelle : sans liberté dans la formation de la volonté, celle-ci ne peut s'exprimer librement. En effet, c'est seulement parce que la personne est libre au stade de la formation de sa volonté et de ses choix qu'elle est libre au moment de leur réalisation.

18. La liberté d'autodétermination en droit. La transposition de la conception philosophique de la liberté d'autodétermination en droit permettrait de protéger la formation de la volonté des personnes. Cette liberté d'autodétermination est donc une sorte de prérequis à l'effectivité de l'autonomie individuelle. En effet, elle permet à la personne de former librement sa volonté, sans être soumise à des influences extérieures prolongées, afin de mener sa vie selon sa propre volonté. Bien sûr, il n'est pas question de remettre en cause le besoin de toute personne d'entretenir avec les autres des relations sociales qui peuvent avoir une influence sur ses choix personnels. Il s'agit plutôt d'encadrer les traitements de données qui, sur le long terme, nous influencent. La liberté

⁶⁵ K. Appourchaux, « Neurosciences et techniques de redirection de l'attention : redéfinir le libre arbitre en termes d'apprentissage de la maîtrise de nos capacités attentionnelles », *Psychiatrie, Sciences humaines, Neurosciences* 2013, vol. 11, p. 43, spéc. p. 45.

⁶⁶ R. Kane, *A contemporary introduction to free will*, Oxford University Press, 2005, p. 172.

⁶⁷ K. Appourchaux, « Neurosciences et techniques de redirection de l'attention : redéfinir le libre arbitre en termes d'apprentissage de la maîtrise de nos capacités attentionnelles », *Psychiatrie, Sciences humaines, Neurosciences* 2013, vol. 11, p. 43, spéc. p. 46.

d'autodétermination est donc centrale, indispensable même, à la substance de l'autonomie personnelle. Sans liberté d'autodétermination, la personne ne peut mener sa vie comme elle l'entend, puisque sa volonté est orientée par des intérêts extérieurs dont elle n'a pas toujours conscience. L'influence ou la manipulation au stade de la formation de la volonté aboutit nécessairement à son entrave au stade de son expression et au rétrécissement de l'autonomie personnelle. D'ailleurs, il n'est pas surprenant que le droit des contrats protège non seulement l'expression de volonté, mais aussi la réflexion qui a permis d'arriver à cette volonté⁶⁸. Si une personne a été trompée par les manœuvres de son cocontractant, il n'y a point de consentement valable et le contrat est déclaré nul⁶⁹.

Le concept de liberté d'autodétermination, entendu comme le pouvoir d'une personne de former sa volonté de manière autonome, participe donc à l'autonomie personnelle.

19. Le droit des données personnelles et la liberté d'autodétermination. Le droit des données personnelles apporte quelques garanties pour encadrer les risques que les technologies font courir à la liberté d'autodétermination⁷⁰. Par exemple, l'obligation d'information sur les finalités pour lesquelles les données sont traitées⁷¹ ou les obligations de transparence sur les traitements effectués⁷² contribuent indéniablement à une meilleure connaissance des traitements de données et, en théorie, à une meilleure compréhension de leurs effets. La personne concernée peut plus facilement identifier les influences auxquelles elle pourrait être soumise. Pour autant, comme souvent en droit des données à caractère personnel, la mise en œuvre effective de ces principes reste, le plus souvent, lacunaire. Pour rendre effective la liberté d'autodétermination ainsi que le pouvoir de contrôle des personnes sur leurs informations, certains principes du droit des données devront être renforcés et leur mise en œuvre substantiellement améliorée.

20. Conclusion. Depuis ses origines, le droit des données à caractère personnel n'a cessé d'être modifié pour répondre au besoin de protection des personnes face aux évolutions technologiques. Désormais, cette matière doit évoluer de nouveau pour

⁶⁸ F. Terré, P. Simler, Y. Lequette et F. Chénéde, *Droit civil. Les obligations*, 12^e éd., Dalloz, 2018, n° 147, p. 183.

⁶⁹ Le parallèle avec le droit des contrats trouve sa limite dans plusieurs encadrements des vices du consentement, notamment le « bon dol » ou l'erreur non déterminante.

⁷⁰ Pour certains auteurs, cela serait même la raison des régimes de protection des données, v. Y. Pouillet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », in *État de droit et virtualité*, dir. K. Benyekhlef et P. Trudel, *Thémis*, 2009, p. 157 s., spéc. p. 207.

⁷¹ Art. 13 § 1 c) et 14 § 1 c) du règlement UE n° 2016/679.

⁷² L'article 12 du règlement UE n° 2016/679 pose le principe de transparence des informations.

protéger les personnes contre de nouvelles formes d'atteinte permises par certains traitements de données. Ces traitements ne visent plus seulement à surveiller nos faits et gestes mais tentent également de nous manipuler. Ainsi, les risques liés à la société de surveillance sont couplés à ceux liés à la société de manipulation. Pour que les personnes puissent continuer de développer librement leur personnalité, il convient de reconnaître une nouvelle liberté : celle d'autodétermination. Cette liberté est définie comme le pouvoir d'une personne de former sa volonté de manière autonome. Le droit des données à caractère personnel devra encore évoluer pour contribuer à la protection de cette liberté nouvelle.