HAL open science

Regards sur le nouveau droit des données personnelles

Emmanuel Netter, Valère Ndior, Jean-Ferdinand Puyraimond, Suzanne Vergnolle

To cite this version:

Emmanuel Netter, Valère Ndior, Jean-Ferdinand Puyraimond, Suzanne Vergnolle (Dir.). Regards sur le nouveau droit des données personnelles. Centre de droit privé et de sciences criminelles d'Amiens. , 2019, Morgane Daury, 979-10-97323-05-9. hal-02357967

HAL Id: hal-02357967

https://hal.science/hal-02357967v1

Submitted on 11 Nov 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CEPRISCA
Collection colloques

Regards sur le nouveau droit des données personnelles

Sous la direction de :
Emmanuel Netter,
Maître de conférences HDR en droit privé

Comité scientifique :
Valère Ndior
Professeur de droit public à l'Université de Bretagne occidentale
Jean-Ferdinand Puyraimond,
Avocat au barreau de Bruxelles
Suzanne Vergnolle
Doctorante à l'Université Paris II Panthéon Assas

LISTE DES CONTRIBUTIONS

La gouvernance des données personnelles dans la banque
par Aurélie Banck, juriste. Responsable pédagogique du DU Data Protection Officer. Université Paris Nanterre. Co-auteur du Vade-mecum de la protection des données personnelles pour le secteur bancaire et financier, Essentiel de la banque et de la Finance, 2018.

La protection des données personnelles et la mort
par Céline Béguin-Faynel, maître de conférences en droit privé à l'Université du Mans (THÉMIS-Um ; EA-4333). Responsable du Certificat Informatique et Internet, niveau 2, spécialité Métiers du Droit (C2I2®)

Le règlement 2016/679/eu à la lumière du droit américain : à la recherche d'un fonds commun entre l'union européenne et les états-unis
par Céline Castets-Renard, membre de l'Institut Universitaire de France (IUF). Professeur, Université Toulouse 1 Capitole. Directrice du Master Droit du numérique. Directrice adjointe de l'IRDEIC - Centre d'Excellence Jean Monnet

La protection des données personnelles en assurance : dialogue du juriste avec l'actuaire
par Arthur Charpentier, professeur de mathématiques à l'Université de Rennes / Delphine Cocteau-Senn, maître de conférences en droit privé à l'Université de Picardie - Jules Verne / Rodolphe Bigot, maître de conférences en droit privé à l'Université de Picardie - Jules Verne

Tous responsables de traitement de données personnelles ?
par Mélanie Clément-Fontaine, maître de conférences HDR, DANTE, UVSQ. Université de Paris-Saclay

Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence
par Jean-Marc Deltorn, doctorant au laboratoire E.A. 4375. Centre d'études internationales de la propriété intellectuelle. Université de Strasbourg

Recherche en santé et protection des données personnelles à l'heure du RGPD
par Frédérique Lesaulnier, docteur en Droit. Déléguée à la protection des données de l'INSERM

Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls
par Emmanuel Netter, maître de conférences HDR en droit privé. Université d'Avignon, Laboratoire Biens, normes, contrats (EA 3788). Membre associé du Centre de droit privé et de sciences criminelles d'Amiens (EA 3911)

Données personnelles et transparence de la vie publique
par Charles-Édouard Sénac, professeur à l'Université de Bordeaux CERCCLE (EA 7436), CURAPP ESS (UMR 7319)

le règlement général sur la protection des données à caractère personnel appliqué aux états tiers : une appréciation de son caractère extraterritorial
par Élodie Weil, doctorante en droit public à l'Université de Cergy-Pontoise. Déléguée à la protection des données au Centre interdépartementale de gestion de la Grande Couronne d'Ile-de-France

LE MODÈLE EUROPÉEN DE PROTECTION DES DONNÉES PERSONNELLES À L'HEURE DE LA GLOIRE ET DES PÉRILS[1]

Emmanuel Netter, maître de conférences HDR en droit privé
Université d'Avignon, Laboratoire Biens, normes, contrats (EA 3788)
Membre associé du Centre de droit privé
et de sciences criminelles d'Amiens (EA 3911)

« La *civilisation de l'informatique ne va-t-elle pas devenir celle de l'indiscrétion et de l'implacabilité, celle qui n'oublie, ni ne pardonne, qui enfonce le mur de l'intimité, enfreint la règle du secret de la vie privée, déshabille les individus ?* » ?
Jean Foyer, rapporteur de la loi informatique et libertés,
JO du 4 octobre 1977, p. 5782

« *Nous abordons un terrain qui est encore en friche et presque inconnu. Il serait déraisonnable de prétendre organiser en détail un domaine aussi nouveau. L'informatique est promise à un développement très rapide qui, dans une assez large mesure, est imprévisible, comme l'est la recherche scientifique elle-même. Par conséquent, la loi que nous vous proposons a un caractère expérimental. Nous ne prétendons pas légiférer pour l'éternité* ».
Alain Peyrefitte, ministre de la Justice,
JO du 4 octobre 1977, p. 5789

Il y a quarante ans, les fondations du droit français des données personnelles étaient posées[2]. Les travaux parlementaires, dont ces deux citations sont extraites, révèlent la conscience qu'on avait alors d'adopter un texte d'ores et déjà fondamental, mais dont l'importance, surtout, ne ferait que croître avec la montée en puissance de l'informatique. La direction exacte que ces progrès devaient emprunter était certes inconnue. Il était difficile, à l'orée des années 80, d'imaginer que les plus puissantes menaces planant sur l'intimité des citoyens seraient à rechercher dans les bases des entreprises privées, et non plus seulement dans le recoupement

1 - Le titre est emprunté à R. Merle, *La Gloire et les Périls*, éd. De Fallois, 1999.

2 - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

des fichiers administratifs. On ne pouvait entrevoir les téléphones perpétuellement géolocalisés, on ne pouvait anticiper la publicité ciblée, on ne pouvait imaginer l'internet des objets ou les réseaux sociaux. Mais si l'on ne connaissait ni la nature ni l'origine exactes des dangers à venir, on avait bien prévu, il y a quatre décennies déjà, leur exceptionnelle intensité.

Pourtant, ces solennelles mises en garde n'ont longtemps suscité qu'un désintérêt poli, que ce soit de la part de la petite communauté des juristes, de celle, autrement plus importante, des entreprises privées et des administrations, ou même du grand public.

S'agissant de la communauté des juristes, remarquons qu'une maîtrise élémentaire de la loi « informatique et libertés » n'était pas attendue, il y a peu, d'un généraliste du droit public ni du droit privé. Il y a dix ans encore, il était commun de suivre un cursus juridique complet sans rien avoir appris de substantiel de ce texte ni de la législation européenne ultérieure en matière de données personnelles. La connaissance de ces règles semblait réservée au petit nombre des spécialistes de droit de l'informatique. Depuis peu, la tendance évolue nettement, et bien des enseignants décident de réserver quelques dizaines de minutes, voire quelques heures à ces questions. En droit privé, ce sera à l'occasion d'un cours de droit des personnes ; en droit public, dans le cadre d'un enseignement de libertés fondamentales. La question, il est vrai, est de celles qui transcendent cette *summa divisio* française. Quant aux formations consacrées plus ou moins directement au « droit du numérique », et qui ne peuvent faire l'économie de modules substantiels consacrés au droit des données, elles se multiplient sur tout le territoire. Le niveau général de connaissance des juristes dans ce domaine a donc fortement augmenté en peu de temps.

Au-delà du milieu des juristes, ce sont les responsables de traitement privés et publics qui semblent avoir redécouvert tardivement l'existence du droit des données personnelles. Autrement dit, pratiquement toutes les administrations et entreprises privées, car chacun est aujourd'hui un « responsable de traitement »[3]. Dès le

3 - V. dans cet ouvrage M. Clément-Fontaine, « Tous responsables de traitement de données personnelles ? ».

texte du Règlement général sur la protection des données (RGPD) divulgué, jusqu'à son entrée en vigueur – et sans doute bien au-delà… – une véritable « course à la mise en conformité » s'est engagée. Son carburant est connu : le net rehaussement des sanctions encourues en cas de violation de certaines dispositions du règlement[4]. «Vingt millions d'euros », répétaient les petits entrepreneurs saisis par l'angoisse. « Quatre pour cent du chiffre d'affaires mondial », scandaient les géants de l'économie, incrédules. Quelles nouvelles obligations issues du RGPD peinaient-ils à mettre en œuvre pour s'effrayer ainsi ? Le droit à la portabilité des données ? Le nouveau régime de la sous-traitance ? Le droit à l'effacement spécifiquement reconnu par le texte aux mineurs ? Non : les obligations qui font l'objet des sanctions les plus lourdes sont celles qui, pour l'essentiel, existent depuis… 1978[5]. Les responsables de traitement et sous-traitants qui tremblaient tout à coup mettaient parfois en œuvre depuis longtemps des traitements dont la finalité n'était pas identifiée, ou à tout le moins pas communiquée aux personnes concernées ; ils ne pouvaient pas toujours justifier d'un fondement de licéité précis, ou se reposaient sur un consentement grossièrement extorqué aux personnes dont les données étaient traitées, ou encore faisaient un usage abusif du fondement particulier qu'est l' « intérêt légitime » ; ils faisaient fi du principe de minimisation, ou se montraient totalement laxistes sur le terrain de la sécurité des informations[6]. Pourquoi ces exigences avaient-elles mis quarante ans à pénétrer les consciences ? La réponse est simple : une mise en conformité sérieuse est coûteuse en temps ainsi qu'en compétences. Les plus cyniques ajouteront qu'elle peut constituer un désavantage concurrentiel si une entreprise vertueuse fait face à des adversaires moins scrupuleux, voire même qu'elle peut disqualifier certains modèles d'affaires radicalement incompatibles avec le respect des données personnelles. Ainsi, le bilan coûts contre

4 - Art. 83 du 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 95/46/CE.

5 - L'art. 83, 5) punit en effet de l'amende la plus lourde, notamment, la violation des « principes de base d'un traitement » (a) et des « droits dont bénéficient les personnes concernées » (b), ce qui renvoie bien à une majorité de règles déjà en vigueur depuis la première version de la loi informatique et libertés.

6 - Il s'agit de contraventions aux « principes relatifs au traitement des données à caractère personnel », que le règlement énonce en son article 5 avant de les développer plus loin.

avantages était bien souvent défavorable lorsque, avant l'entrée en vigueur du règlement, les amendes françaises les plus élevées étaient plafonnées à 150 000 euros[7]. Il est nettement plus incitatif à présent. Le secret de l'effectivité du droit serait-il aussi simple et aussi décevant ? Il semblerait que oui. La loi, dans ce domaine au moins, n'est pas obéie parce qu'elle est l'expression de la volonté générale, parce qu'elle est bonne et juste ou parce qu'elle a été votée par les autorités habilitées dans les formes constitutionnellement requises, mais parce qu'elle frappe, durement, au portefeuille. En marge d'un colloque, un ancien de la CNIL rappelait malicieusement cette maxime, qui fleure bon l'Amérique de la Prohibition : « on peut obtenir beaucoup plus avec un mot gentil et un revolver qu'avec un mot gentil tout seul ».

L'intérêt pour le droit des données personnelles a, enfin, largement progressé au sein du grand public. Il serait certes excessif de dire que, dans les années 70, la question n'intéressait pas du tout l'opinion. On sait que la loi informatique et libertés est l'enfant du scandale : celui provoqué par un article du journal Le Monde révélant l'existence du « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus » (SAFARI)[8]. Le ministre de l'Intérieur, un certain Jacques Chirac, se frottait semble-t-il les mains à l'idée que l'INSEE procède à cette interconnexion massive des bases de données des administrations autour d'un identifiant unique pour chaque citoyen, le numéro de sécurité sociale[9]. Il fallut encore plusieurs années avant que la question n'arrive devant le Parlement, et que ne naisse la CNIL. L'émotion suscitée à l'époque dans l'opinion a-t-elle été suivie d'effets durables ? On peut en douter. Les citoyens se pensaient protégés passivement, par les formalités préalables et les obligations diverses pesant sur les responsables de traitements et sous-traitants. Mais bien peu étaient acteurs de la protection de leurs données, même si les droits « informatiques et libertés » qu'il leur

7 - 300 000 euros en cas de récidive.

8 - P. Boucher, « Une division de l'informatique est créé à la chancellerie. «SAFARI» ou la chasse aux français », article *Le Monde* du 21 mars 1974.

9 - Face aux dénégations du ministère de l'intérieur à la suite de son précédent article, le journaliste P. Boucher rétorquait : « Il n'a jamais été écrit que la place Beauvau assurait le leadership du projet SAFARI, mais qu'elle s'y intéressait de très près... Les convoitises dont il est l'objet ne sont un secret pour personne, non plus que les pressions exercées sur M. Jean Ripert, directeur de l'INSEE » : P. Boucher, « Le ministère de l'intérieur affirme qu'il n'est pas question de porter atteinte aux libertés individuelles », article *Le Monde* du 22 mars 1974.

était loisible d'invoquer s'étalaient régulièrement sous leurs yeux, sous forme de mentions obligatoires, à l'occasion de l'ouverture d'un compte bancaire ou de la participation à un jeu-concours, îlots perdus dans l'océan des contrats jamais lus. Mais ici encore, un vent nouveau paraît souffler depuis quelques années. Pour exister sur la scène médiatique et marquer les esprits, il manquait à la cause des données personnelles deux choses dont elle dispose à présent : une actualité perpétuelle et des incarnations marquantes.

D'abord, il existe aujourd'hui dans cette matière une actualité perpétuellement renouvelée. La société Facebook pourrait quasiment l'assurer à elle seule. Elle a particulièrement marqué les esprits à l'occasion de l'affaire dite « Cambridge Analytica »[10]. Un questionnaire d'apparence anodine était autorisé par des utilisateurs du réseau social à accéder à leur profil. Il y aspirait ensuite toutes les données possibles – qui peuvent comprendre, outre les centres d'intérêts des informations sur les convictions politiques ou religieuses, l'orientation sexuelle ou la profession exercée – non seulement sur l'internaute ayant accordé l'autorisation, mais aussi et surtout sur ses centaines d'amis. Il est probable que l'utilisateur du questionnaire n'avait pas véritablement saisi ce à quoi il s'exposait ; il est en toute hypothèse certain que ses amis n'avaient consenti à rien. Ces données, qui concernaient une majorité de citoyens américains – mais aussi des Européens, dont des Français – ont notamment été exploitées aux fins de démarchage politique ciblé dans le cadre de la campagne électorale qui a vu Donald Trump remporter la présidence des États-Unis. Facebook a présenté ses excuses, a modifié sa gestion des applications tierces autorisées à exploiter les profils de ses utilisateurs. Entendu successivement par le Congrès américain et par le Parlement européen, le dirigeant Marc Zuckerberg a impressionné par sa capacité à éviter toute réponse précise et substantielle aux questions qui lui étaient posées[11]. Mais l'affaire Cambridge Analytica, pour fondamentale qu'elle soit, ne doit

10 - Sur laquelle V. par ex. G. Pépin, « Facebook a laissé fuiter les données de 50 millions d'internautes, UE et USA vont enquêter », article *nextinpact.com* du 19 mars 2017.

11 - V. par ex. l'inventaire des questions auxquelles M. Zuckerberg a soit répondu qu'il se concerterait avec son équipe et répondrait ultérieurement, soit qu'il ne connaissait pas la réponse : « Facebook : comment Mark Zuckerberg a évité de répondre à certaines questions », article *lemonde.fr* du 11 avril 2018.

pas occulter les incidents intervenus avant et depuis lors. Avant cette affaire, Facebook s'était déjà distingué lors de son rachat de la célèbre messagerie WhatsApp, en promettant de ne pas croiser les deux bases de données d'utilisateurs, puis en agissant à l'inverse, s'attirant une sanction de la Commission européenne en matière de droit des concentrations, mais sans que la question de la conformité de ces pratiques au RGPD ne soit encore véritablement éclaircie à cette heure[12]. Depuis Cambridge Analytica, l'actualité est restée riche. À la rentrée 2018, on apprenait que la sécurité de millions de comptes, dont certains appartenant à des internautes européens, avait été compromise par des attaques sophistiquées[13]. Il ne faut pas être trop prompt, cette fois-ci, à blâmer la société, car un réseau social d'une telle ampleur et d'une telle complexité ne sera jamais invulnérable du point de vue de la sécurité informatique. Les spécialistes diront si la firme avait fait preuve d'une légèreté blâmable, ou si les diligences accomplies avaient été à la hauteur des moyens disponibles. En revanche, quasiment au même moment, une étude menée par des chercheurs américains démontrait que Facebook avait détourné des numéros de téléphone, qui lui avaient été fournis par ses utilisateurs dans le but exclusif d'améliorer la sécurité de leur compte : la société les a pourtant exploités afin de se livrer à de la publicité ciblée[14]. Depuis, la liste des révélations s'est encore largement allongée[15]. Bien d'autres responsables de traitement encourent des reproches

12 - Commission européenne, « Concentrations: la Commission inflige des amendes de 110 millions EUR à Facebook pour avoir fourni des renseignements dénaturés concernant l'acquisition de WhatsApp », communiqué de presse du 18 mai 2017.

13 - V. par ex. L. Ronfaut, « Piratage de Facebook : 5 millions de comptes concernés en Europe », article *lefigaro.fr* du 2 octobre 2018.

14 - G. Gebhart, « You gace Facebook your number for security. The used if for ads », article *eff.org* du 27 septembre 2018 ; G. Venkatadri, E. Lucherini, P. Sapierynski et A. Mislove, « Investigating sources of PII used in Facebook's targeted advertising », : http://mislove.org/publications/PII-PETS.pdf.

15 - Actualisant cet article avant la parution de l'ouvrage, nous pouvons mentionner les accès octroyées par Facebook à Netflix ou à Spotify à la messagerie privée de certains utilisateurs, révélée en décembre 2018 (V. par ex. Le Poiny du 19 décembre 2018, « Facebook a octroyé aux géants du Net un large accès aux données personnelles) ; la possibilité pour des milliers d'employés de Facebook d'accéder aux mots de passe des utilisateurs stockés dans une base non chiffrée, révélée en mars 2019, (V. par ex. L. Ronfaut, « Des employés de Facebook ont pu consulter des millions de mots de passe d'utilisateurs) ; ou encore un nouveau scandale lié à l'accès à des données par des applications tierces, dans la lignée de l'affaire Cambridge Analytica, les informations étant stockées en clair sur des serveurs non protégés, révélé en avril 2019 (V. par ex. l'article du Monde du 4 avril 2019, « Des données de 540 millions d'utilisateurs de Facebook librement accessibles).

sur le plan du droit des données personnelles, mais Facebook, avec 2,2 milliards d'utilisateurs actifs mensuels, occupe une place particulière dans les préoccupations des citoyens[16]. Son seul exemple suffit donc à démontrer que l'opinion publique n'a pas manqué, ces derniers mois, d'occasions de s'interroger sur le sort réservé à ses informations intimes.

Pour aiguillonner encore davantage les consciences et cristalliser l'attention médiatique, la thématique des données personnelles avait besoin d'incarnations marquantes, autrement dit de héros ou d'antihéros. La première de ces figures a surgi en 2013, et il est à peine besoin d'y revenir : c'est celle d'Edward Snowden, qui a interpellé le monde entier en révélant la toute-puissance des services de renseignement américains[17]. Les révélations sur les programmes de surveillance ont attiré indirectement l'attention sur leur carburant : les données de géolocalisation, de navigation, les métadonnées de télécommunication, les publications sur les réseaux sociaux... À ce moment-là, dans l'esprit du grand public, le concept de données personnelles passait brutalement du statut d'abstraction lointaine et inoffensive à celui de réalité quotidienne et menaçante. Or, ces mêmes informations qui font parfois l'objet d'une surveillance publique à des fins de sécurité nationale sont par ailleurs la matière première d'une industrie privée qui les exploite à des fins lucratives. On peut ajouter un deuxième personnage à la galerie de portraits, déjà évoqué du reste : le fondateur et dirigeant de Facebook, Mark Zuckerberg. Tout oppose Snowden et Zuckerberg, et l'on rencontre souvent sur les réseaux sociaux cette présentation en raccourci : le premier est devenu un traître et un fugitif pour avoir dénoncé la surveillance des masses ; le second est devenu l'un des hommes les plus riches du monde pour l'avoir organisée[18]. La réalité est évidemment plus subtile, mais ce qui est intéressant est que l'on assiste ici à la naissance de grandes figures populaires susceptibles l'une et l'autre, selon le locuteur, d'être admirées ou honnies.

16 - Chiffres 2018 issus du *Blog du modérateur* : https://www.blogdumoderateur.com/chiffres-facebook/.

17 - V. not. le documentaire de L. Poitras, *Citizenfour*, 2015.

18 - Réagissant à l'audition de Mark Zuckerberg devant le Congrès suite à l'affaire Cambridge Analytica, Edward Snowden n'a d'ailleurs pas pu s'empêcher d'écrire sur Twitter : « And they call me a criminal » : https://twitter.com/snowden/status/983801604519407616.

Nos peurs et nos fantasmes à l'égard des nouvelles technologies cherchent ainsi à s'accrocher à des visages. Ce besoin, le dénommé Chris Dancy l'a identifié très tôt, et transformé en un fonds de commerce fort lucratif. Se présentant à travers la presse mondiale comme « l'homme le plus connecté du monde », il se vante de mesurer un maximum de paramètres de son existence, à grand renfort « d'internet des objets » : son rythme cardiaque, la fréquence de ses passages aux toilettes, la température et l'hygrométrie de son logement, la qualité de son sommeil, la musique qu'il écoute... Il fait ensuite varier certains de ces paramètres, et observe l'effet produit sur les autres[19]. Il prétend ensuite, à l'intention des naïfs, avoir appliqué la même démarche expérimentale à l'analyse des comportements humains, accédant à une compréhension de leurs mécanismes sous-jacents qui lui procurerait un pouvoir « terrifiant » de manipulation d'autrui [20]. Peu seront dupes, mais suffisamment tout de même pour assurer à ce conférencier professionnel un train de vie confortable. Comment est-ce possible ? Sans doute parce que le personnage de « *mindful cyborg* » construit par M. Dancy n'est qu'une spectaculaire hyperbole, une caricature débridée d'attentes que certains nourrissent véritablement à l'égard du progrès technique. Il prétend qu'en agrégeant assez de données personnelles et en les confiant à des algorithmes suffisamment sagaces, le sens caché de notre environnement, de nos comportements et de nos vies apparaîtra tout à coup[21]. C'est en définitive un pacte faustien qu'il propose à ses adeptes : faire don de son essence à une figure puissante et dangereuse, et recevoir en contrepartie d'extraordinaires pouvoirs. Les grandes entreprises du numérique revêtent, dans ce récit, des atours méphistophéliques, et offrent l'accès à une nouvelle transcendance. Ainsi, plus encore peut-être que Mark Zuckerberg, Faust-Dancy s'offre comme l'exact opposé du martyr Snowden dans l'imaginaire collectif.

19 - C. Richard, « L'homme le plus connecté du monde s'est fait dévorer par ses données », article *nouvelobs.com* du 9 septembre 2016 : Je prenais ces petites unités de comportement et je les changeais de place pour voir ce qui se produisait : une même conversation avec un ami prend-elle un tour différent s'il fait chaud ou s'il fait froid, si on marche ou si on est assis ? ».

20 - *Ibid.* : « c'était trop facile de pousser les gens à faire ce que je voulais ».

21 - Pour un aperçu : chrisdancy.com.

Des scandales d'ampleur survenant à intervalles réguliers, une galerie de personnages marquants, et la couverture médiatique de l'entrée en vigueur du RGPD ont ainsi, à n'en pas douter, éveillé l'intérêt du public. Cela a-t-il produit des effets concrets ? Au premier abord, il semble que oui. La CNIL, en livrant son premier bilan après 4 mois d'application du règlement, faisait état d'une augmentation de 64 % des plaintes par rapport à la même période en 2017, qui constituait déjà elle-même une année record. Et l'autorité de commenter : « Ceci est sans doute consécutif à un coup de projecteur médiatique important récemment sur la protection des données : RGPD, Cambridge Analytica, etc. »[22]. Deux mois plus tard, la CNIL révélait les résultats d'un sondage IFOP dont elle était commanditaire : 66 % des Français se disaient « plus sensibles que ces dernières années à la protection de leurs données personnelles », et 65 % d'entre eux avaient entendu parler du règlement européen[23].

À l'heure des 40 ans de la loi informatique et libertés, le bilan prend ainsi des allures de triomphe. Le droit des données personnelles n'a jamais été mieux considéré, mieux connu, plus puissant en Europe. Toutefois, derrière ces apparences flatteuses se cachent de nombreux motifs d'inquiétude, qui ne doivent pas être occultés. Sans rien remettre en cause des formidables acquis du droit français et, surtout, du droit de l'Union, il nous faut identifier ces difficultés. Si elles n'étaient pas résolues, le RGPD pourrait n'être qu'un feu de paille, dont l'éclat s'épuiserait en quelques années seulement. Ces faiblesses se nichent à la fois au sein du droit européen (I) et en dehors de lui (II).

§1 : Le droit européen des données menacé en dedans

Deux défauts majeurs affectent cette législation. Dans son état actuel, elle est très difficilement intelligible pour les citoyens, et même pour les milieux professionnels non spécialisés (A). Surtout, si son effectivité semble en nette hausse, à la faveur notamment d'une augmentation drastique des sanctions, elle risque pourtant d'atteindre rapidement un plateau avant de décliner (B).

22 - CNIL, « RGPD : quel premier bilan 4 mois après son entrée en application » ?, article *cnil.fr* du 25 septembre 2018.

23 - CNIL, « RGPD : quel bilan 6 mois après son entrée en application ? », article *cnil.fr* du 23 novembre 2018.

A. Le manque de lisibilité

Si la CNIL se réjouissait des résultats du sondage qu'elle avait commandé s'agissant de la proportion de Français ayant entendu parler du RGPD, elle reconnaissait sa déception quant au chiffre de ceux qui estimaient comprendre l'intérêt du texte : 54 % seulement[24]. Mais il serait déjà extraordinaire qu'une majorité de la population, fût-elle courte, ait accédé à une maîtrise élémentaire de ces règles. Il est permis d'en douter, non par manque de confiance dans les capacités d'apprentissage de nos concitoyens, mais parce que tout a été fait pour leur compliquer la tâche.

Cela a d'abord commencé avant même l'adoption du texte européen. La loi dite « République numérique » du 7 octobre 2016 aborde des thématiques nombreuses[25]. Le droit des données personnelles en fait partie. Au moment où le projet de loi est présenté, et pendant une large part du processus parlementaire, le RGPD est en cours de négociation. Pourquoi adopter une approche purement française de questions qui s'apprêtent à faire l'objet d'une harmonisation européenne complète, dont la teneur n'est pas encore entièrement connue ? Le calendrier politique a ses raisons que la raison ignore. Cette stratégie du cavalier seul n'aura pas nui s'agissant de points sur lesquels le règlement ne s'est finalement pas prononcé, comme le sort qu'il convient de réserver aux données personnelles après la mort[26]. Sur d'autres questions, comme le droit à la portabilité des données, la France a mis au point sa propre qualification juridique et son propre régime, qui sont immédiatement entrés en conflit avec les arbitrages retenus dans le cadre du RGPD. Pour mettre fin à cette situation confuse, les textes français ont récemment été supprimés[27]. Quel citoyen, même s'il avait fait preuve d'une curiosité raisonnable pour l'actualité législative, aurait pu retenir quoi que ce soit d'exact d'un tel processus ?

---

24 - *Ibid.*

25 - Loi ° 2016-1321 du 7 octobre 2016 pour une République numérique.

26 - Art. 40-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, issu de la loi précitée pour une République numérique. Sur cette question, V. dans le présent ouvrage C. Béguin-Faynel, « La protection des données personnelles et la mort ».

27 - Les articles L. 224-42-1 et s. du Code de la consommation ont été supprimés par l'article 33 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

C'est ensuite au niveau européen qu'ont surgi des obstacles à la bonne intelligibilité des textes. Il était attendu du règlement qu'il réalise une harmonisation complète du droit des données personnelles, à la fois au bénéfice des citoyens de l'Union, dotés partout des mêmes droits, mais aussi au bénéfice des responsables de traitement, placés en vertu d'une logique bien connue face à un « marché unique » permettant une « libre circulation » des données. L'échec est patent, puisqu'il est renvoyé aux droits nationaux sur une cinquantaine de points[28]. Était-il véritablement impossible de s'accorder, par exemple, sur l'âge à partir duquel un enfant peut consentir seul à un traitement de données le concernant[29] ? Aujourd'hui, un juriste auquel un parent demanderait si son enfant peut ouvrir un compte Facebook sans son concours ne pourrait répondre sans avoir vérifié quel droit national est applicable, puis sans avoir recherché les textes locaux pertinents, à supposer qu'il maîtrise la langue européenne concernée. Mais ce n'est pas tout. Imaginons un citoyen européen si courageux qu'il aurait entrepris la lecture des 173 considérants et des 99 articles du règlement, tout en acceptant d'être renvoyé 50 fois à son droit national. Pourrait-il se vanter de connaître le droit européen des données personnelles ? Malheureusement pas, car l'Union a de surcroît ajouté à sa législation générale des textes sectoriels qu'il convient de maîtriser également. S'agissant des traitements de données relatifs à des infractions ou sanctions pénales, au moins doit-on se féliciter que la directive sectorielle ait été adoptée en même temps que le RGPD[30]. Il suffit donc de consulter ce supplément de législation… ainsi que l'instrument de droit national l'ayant transposé – ce qui, s'agissant d'une directive, n'est cette fois-ci pas une surprise. Mais considérons à présent la protection de la vie privée dans le secteur des communications

28 - Le décompte est celui de la CNIL dans sa délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978, p. 3.

29 - L'article 8 du règlement 2016/679 fixe un minimum de treize ans et un maximum de seize ans. En France, l'âge de quinze ans a été retenu à l'article 7-1 de la loi précitée du 6 janvier 1978 dans sa rédaction issue de la loi du 20 juin 2018.

30 - Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

électroniques : elle est principalement régie par une directive quelque peu dépassée par les évolutions techniques[31]. Cela concerne des questions auxquelles nous sommes confrontés tous les jours, comme le dépôt et la gestion des cookies par des sites internet dans les navigateurs internet de ceux qui les consultent, ou encore les campagnes publicitaires de masse par courrier électronique. Un nouveau règlement dit « *e-privacy* » devait être adopté, en principe avant l'entrée en vigueur du RGPD[32]. Cela aurait notamment permis aux services en ligne de travailler de manière globale à leur mise en conformité. Ce texte a pris du retard, et sera adopté, au mieux, au cours de l'année 2019.

Revenons à présent à l'échelon français, mais en nous situant cette fois-ci après l'adoption du règlement. Il fallait prendre position pour chacune de la cinquantaine de « marges de manoeuvre» que le texte offrait aux États membres. Le chef du bureau du droit public à la direction des affaires civiles et du sceau avait surpris l'auditoire, lors d'un colloque, en évoquant la nécessité de « transposer » le règlement alors, que ce terme technique, on le sait, est en principe réservé aux directives[33]. Il avait immédiatement précisé qu'il s'agissait d'une facilité de langage, mais qui révélait l'importance du travail à accomplir. On le conçoit bien, mais tout de même : le règlement avait été adopté le 14 avril 2016 et n'entrait en application que le 25 mai 2018[34]. Le délai semblait suffisant, et il était même souhaitable que les textes nationaux soient adoptés début 2018, afin que les responsables de traitement et sous-traitants aient le

31 - Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, modifiée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

32 - Pour l'heure V. la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM/2017/010 final - 2017/03 (COD).

33 - Intervention de M. Cyril Noël lors du colloque *Règlement général sur la protection des données : nouveaux principes, nouvelles règles et application sectorielle*, Université Paris V, le 18 mai 2016.

34 - Aux termes de son article 99, le Règlement est « entré en vigueur » le vingtième jour suivant celui de sa publication au JOUE, mais n'est « devenu applicable » qu'à partir du 25 mai 2018.

temps de se mettre en conformité avec un arsenal législatif complet, entrant en vigueur d'un bloc. Malheureusement, le Gouvernement a lancé le processus parlementaire tardivement, et n'a pas demandé le bénéfice de la procédure accélérée. Le texte n'a été adopté en lecture définitive par l'Assemblée nationale que le 14 mai 2018. Il ne restait que dix jours avant l'entrée en application du RGPD, et il fallait encore compter avec la saisine du Conseil constitutionnel. Là encore, le Gouvernement n'a pas usé de la faculté dont il dispose de demander un examen en urgence, de sorte que la décision (de non-conformité partielle) a été rendue le 12 juin, et la loi promulguée le 20 juin[35]. Le règlement était en vigueur depuis plus d'un mois. Il pouvait certes être appliqué, pour l'essentiel, avant l'adoption des dispositions nationales, mais il en résultait au minimum un effet d'image plutôt déplaisant. Passons rapidement sur le fait que la loi elle-même appelle un certain nombre de décrets d'application et d'instruments normatifs que la CNIL produira dans l'avenir, car il est vrai que Rome ne s'est pas faite en un jour.

Mais les pouvoirs publics français ne se sont pas contentés d'être en retard : ils ont pêché dans la forme, et même sur le fond. La forme, d'abord, était critiquable : alors qu'il aurait été bien plus simple de faire table rase du passé, la France a absolument tenu à conserver la loi informatique et libertés, déjà modifiée à plusieurs reprises depuis 1978, et à lui faire subir les lourds remaniements nécessaires à son alignement avec le nouveau règlement. Le résultat est d'une lecture pour le moins pénible. Pire encore : en son article 32, la loi faisait d'elle-même l'aveu que le parti ainsi pris était mauvais, puisqu'elle habilitait le Gouvernement à réécrire l'ensemble du droit français des données personnelles par ordonnance. Le texte est arrivé en décembre 2018[36]. Pourquoi n'avoir pas commencé par là ?

Le fond, ensuite, fait jaillir de nouvelles critiques. Par exemple, le RGPD encadre rigoureusement les décisions produisant des

35 - Décision n° 2018-765 DC du 12 juin 2018. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

36 - Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

effets juridiques sur le fondement de traitements automatisés. Ces décisions peuvent consister par exemple en l'octroi d'un crédit bancaire, dans le fait de sélectionner ou d'écarter une candidature pour un entretien d'embauche, ou dans une décision administrative. Sur cette question d'une grande importance pratique, l'encadrement français a pu sembler moins exigeant que celui décidé par le règlement[37].

Le bilan est donc celui-ci : le droit européen des données personnelles est constitué d'un empilement d'une législation générale et de législations sectorielles, chaque texte étant par lui-même d'une grande complexité ; les droits nationaux transposent ensuite les directives et exploitent les « marges de manœuvre » du règlement en ordre dispersé ; la France, pour ce qui la concerne, a produit en retard un texte de son propre aveu inintelligible, et peut-être déloyal à l'égard des solutions européennes sur certains points.

À ce manque de lisibilité, qui suscite déjà l'inquiétude, il faut ajouter le risque d'un manque d'effectivité, qui en découle pour partie.

B. Le manque d'effectivité

L'effectivité du droit européen des données personnelles peut être évaluée d'un double point de vue : celui des personnes concernées, et celui des responsables de traitement.

37 - N. Martial-Braz, « L'abus de textes peut-il nuire à l'efficacité du droit ? », *Dalloz IP/IT*, 2018, 459 : « L'article 22 du RGPD prévoit un droit (subjectif ?) de tout individu «à 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». La reconnaissance d'un tel droit confère donc un caractère automatique à cette prérogative de la personne concernée et va évidemment au-delà d'une simple faculté d'opposition ou du renforcement des conditions de licéité des traitements automatisés reposant sur un tel profilage permettant une prise de décision ayant des effets juridiques ou affectant la personne concernée de manière similaire ». En revanche, poursuit l'auteur, « (...) l'alinéa 2 de l'article 10 de la LIL (...) prévoit désormais que «Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception : [...]». Une telle rédaction n'a pas le même sens que celle précité prévue dans le règlement. Le fait qu'aucune décision «ne peut être prise sauf exception», n'a pas la même force que la reconnaissance d'un droit subjectif à ne pas faire l'objet de décision prise sur le fondement d'un profilage ».

1) Du point de vue des personnes concernées

En dépit des quelques améliorations récentes, il faut constater la faible mobilisation de leurs droits par les personnes dont les données sont manipulées. L'entrée en application du RGPD a suscité l'attention médiatique, ce qui a certes contribué, on l'a vu, à sensibiliser la population à l'importance de ces questions. Mais l'optimisme, en cette matière, doit rester mesuré. Il est facile de faire état d'une forte croissance du nombre de plaintes en un an lorsque l'on part de loin. Moins de 3800 signalements entre la fin mai et la fin septembre 2018 : le chiffre est loin d'être spectaculaire, rapporté à la population du pays, dans un contexte où les entreprises privées comme les administrations en parfaite conformité avec le règlement sont encore bien rares[38]. Il est probable que la capacité à défendre son intimité numérique soit fort mal distribuée dans la population. Le recours à la CNIL est le fait d'une petite élite bien renseignée, capable de comprendre ses droits et d'en demander le respect au régulateur : c'est elle seule qui a été aiguillonnée par les récentes actualités. Ses effectifs ont bel et bien augmenté, mais ils restent faibles. La grande complexité des textes applicables risque de dissuader le plus grand nombre, en dépit des efforts remarquables de vulgarisation de la CNIL - qui prennent la forme de synthèses rédigées dans un langage clair et de fiches pratiques.

Non seulement la motivation des individus s'effrite rapidement lorsqu'ils cherchent à comprendre la nature de leurs droits, mais leur patience est également mise à rude épreuve par les trop nombreuses demandes de consentement au traitement de leurs données qu'ils reçoivent. Le « bandeau cookies » qui s'affiche sur chaque site internet visité pour la première fois constitue l'illustration la mieux connue de ce phénomène[39]. Cette formalité vise en théorie un double objectif : rendre visibles les collectes de données en ligne pour en

38 - CNIL, « RGPD : quel premier bilan 4 mois après son entrée en application » ?, art. préc.

39 - Ce bandeau vise à délivrer l'information exigée par l'art. 5, 3) de la directive 2002/58 précitée : « Les États membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données [...] ».

avertir l'individu et, surtout, permettre à la personne concernée de refuser son consentement, si elle le souhaite et que le traceur n'est pas absolument indispensable à l'exécution du service. Chacun sait qu'en pratique, il n'en est rien : ces bandeaux sont considérés par la plupart des internautes comme de simples obstacles placés sur le chemin de la lecture d'un article ou de l'accès à un service, et ils ne cherchent qu'à s'en débarrasser le plus vite possible. Lorsque l'on propose à un individu de choisir entre une récompense immédiate et tangible, même minuscule, et un danger lointain et impalpable, même redoutable, la fiction de l'agent rationnel a tôt fait de disparaître[40]. Certaines extensions de navigateur ont même été créées aux fins d'assurer la fermeture automatique et invisible de ces bandeaux. Certes, les rédacteurs du projet de règlement *e-privacy* sont conscients de cette difficulté, que l'on va tenter de contourner en invitant l'internaute à s'exprimer une fois pour toutes dans les réglages de son navigateur[41]. Mais si un tel système entre véritablement en action demain, rares seront les personnes qui choisiront, si elles ont la possibilité de s'exprimer une et une seule fois, d'être suivies au travers de leur navigation par des régies publicitaires centralisées, et de s'exposer à des annonces personnalisées. On touche ici à un non-dit de cette réglementation : s'il était véritablement aussi facile de dire oui que de dire non à ces formes de collecte de données, des centaines d'entreprises feraient faillite en quelques semaines. Un secteur économique entier s'est bâti sur le relâchement total, par sa clientèle, de son contrôle sur ses données.

Laissons de côté le cas particulier des cookies, et laissons même derrière nous le droit des données personnelles : le consentement machinal, rituel purement mécanique sans signification intellectuelle, affaiblit depuis longtemps le droit des contrats de masse. On signe sans les lire ses contrats bancaires, d'assurance et de

40 - En ce sens : Alessandro Acquisti et al., « Les comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate », *Réseaux,* 2011/3 (n° 167), p. 105-130.

41 - « Le fait de centraliser le consentement dans des logiciels comme les navigateurs Internet, d'inviter les utilisateurs à choisir leurs paramètres de confidentialité et d'étendre les exceptions à la règle du consentement pour les cookies donnerait à une grande partie des entreprises la possibilité de se débarrasser des bandeaux et avis en la matière et conduirait donc à des économies de coûts et une simplification potentiellement importantes » (extrait de l'analyse d'impact accompagnant la proposition de règlement 2017/003 précitée).

téléphonie mobile. En ligne, on clique pour cocher une case « j'accepte les conditions générales » d'iTune*s*, ou de Google, ou de Facebook. S'il y a une deuxième case pour la politique de confidentialité, parce que le RGPD exige que le sort des données personnelles ne soit pas mêlé au reste du contrat, on cliquera simplement une deuxième fois[42]. Et si le traitement concerne des données sensibles au sens de l'article 9 – les convictions politiques, l'orientation sexuelle, des données génétiques – il y aura peut-être une troisième case à cocher, puisque le consentement doit alors être « explicite »[43]. Mais cela changera-t-il quelque chose, au fond ? Le Comité européen de la protection des données fait de son mieux, au travers de ses lignes directrices, pour donner de l'épaisseur, de la substance, de la réalité au consentement[44]. Mais la bataille est perdue d'avance et la réalité est celle-ci : le consentement est une machine à faire sauter la protection des personnes. Placées dans un contexte propice et face à un design suffisamment habile, elles disent oui à tout[45].

Postulons donc que la quasi-totalité de la population n'invoquera jamais les droits qu'elle tire du RGPD, et qu'on cherchera à lui extorquer des consentements vides de toute signification. Cette situation pourra s'améliorer (très) lentement si la CNIL est rejointe par l'Éducation nationale dans ses efforts de pédagogie et que l'on change ainsi d'échelle. En attendant, si la connaissance et le maniement habile du règlement sont le fait d'une petite élite spécialisée, alors pourquoi ne pas se reposer en partie sur elle ? C'est le sens des actions de groupe en matière de violation du droit des données personnelles. Le droit français s'est montré volontariste en la matière, puisque ces actions permettent aujourd'hui non seulement de faire cesser les violations de la réglementation, mais aussi d'obtenir la réparation des préjudices matériels et moraux

42 - Art. 7, 2) du règlement 2016/679 précité.

43 - Art. 9, 2), a) du règlement 2016/679 précité.

44 - G29 (qui était la dénomination du Comité européen de la protection des données avant le RGPD), *Lignes directrices sur le consentement*, 28 novembre 2017, révisées le 10 avril 2018.

45 - Sur ce point, la délibération SAN-2019-001 du 21 janvier 2019, par laquelle la CNIL inflige à Google une sanction de 50 millions d'euros, constituera sans doute un tournant historique. En exigeant un véritable « opt-in » clair et précis des utilisateurs pour que de la publicité ciblée puisse leur être adressée, la CNIL va contraire les modèles d'affaires à évoluer profondément.

subis par les personnes ayant rejoint l'action[46]. Toutefois, il faut ici encore regretter que la question n'ait fait l'objet d'aucune harmonisation européenne au sein du règlement, alors même que certaines des violations les plus graves du texte seront le fait d'acteurs internationaux et concerneront de nombreux pays de l'Union[47]. Les différences entre les législations nationales rendront difficiles, parfois même impossibles les regroupements de personnes concernées dépassant les frontières des États. Mais même ainsi entravées, ces actions de groupe constituent des outils puissants pour pousser les plus grands acteurs à se mettre en conformité avec la loi. Devant la CNIL, trois plaintes collectives ont été déposées par « la Quadrature du Net (plaintes concernant Google, Amazon, Facebook, LinkedIn et Apple, pour un total de 45 000 personnes concernées), l'association NOYB (Google) et l'ONG anglaise Privacy International (plaintes concernant 7 entreprises procédant à de la collecte à grande échelle de données en ligne) »[48].

Que des foyers de compétence de la société civile s'attribuent ainsi le rôle de vigies est une bonne chose. Mais les moyens qui sont les leurs les obligent à choisir leurs combats et à s'attaquer à quelques géants dont il n'est pas douteux qu'ils auraient fait l'objet de contrôles spontanés de la part de la CNIL assez rapidement. Si ces actions revêtent une importance symbolique indéniable, et à supposer qu'elles soient fondées et qu'elles aboutissent, elles ne feront que retirer quelques – grosses – gouttes d'eau à l'océan de la non-conformité. Il reste en effet à s'occuper des quelques centaines de milliers de responsables de traitement restants : considérons à présent l'effectivité du règlement de ce point de vue.

46 - Art. 43 ter de la loi n° 78-17 du 6 janvier 1978 dans sa rédaction issue de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Dans sa rédaction antérieure issue de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, l'action ne pouvait viser qu'à faire cesser le manquement.

47 - L'article 80 du RGPD laisse aux États membres une très large marge d'initiative en la matière.

48 - CNIL, « RGPD : quel bilan 6 mois après... », art. préc. *Adde* La Quadrature du Net, « Dépôt des plaintes collectives contre les GAFAM », article *laquadrature.net* du 28 mai 2018. En France, ces plaintes ont d'ores et déjà donné lieu à la délibération précitée SAN-2019-001 du 21 janvier 2019.

2 – Du point de vue des responsables de traitement et sous-traitants

À supposer que l'écrasante majorité des individus se désintéresse du sort de ses données personnelles, subsisterait malgré tout l'essentiel du règlement, constitué d'obligations qui pèsent sur les responsables de traitement et sous-traitants sans qu'il soit besoin de ne rien leur demander. Si cette protection plancher, ce statut d'ordre public développe réellement ses effets, l'essentiel est sauf, et l'incurie des personnes concernées sans conséquence grave. Respecter le RGPD, c'est, entre autres : fixer une finalité de traitement claire et précise ; collecter le minimum de données nécessaire à l'accomplissement de cette finalité, et pas une de plus ; les conserver le temps strictement nécessaire, et pas une minute en trop ; si une inexactitude est constatée, la rectifier de son propre chef ; empêcher leur destruction et leur altération par l'effet d'un accident ou d'une attaque ; s'abstenir de faire circuler les données auprès de sous-traitants non fiables ou les envoyer dans des pays où elles sont en danger[49].

La difficulté vient, on l'a dit, de ce que ces exigences existent depuis quarante ans, mais ne sont bien souvent respectées que depuis quelques mois, ou ne sont qu'en voie de l'être. La grande masse des responsables de traitement n'est pas mue par la poursuite de valeurs, par une saine conscience de son propre pouvoir ou des risques liés au développement frénétique de la société de l'information, car sans cela leur adhésion aurait été ancienne : elle a peur du gendarme. Ce ressort est puissant, mais il ne fonctionne durablement que si perdure l'impression qu'une chance sérieuse existe d'être pris et de subir effectivement les foudres de la loi.

Imaginons que la peine encourue pour un important excès de vitesse automobile passe d'un coup à plusieurs dizaines de milliers d'euros. Il s'ensuivrait probablement une stupeur des automobilistes, les poussant à surveiller leur compteur de très près. Mais si après quelques semaines le bruit commençait à courir qu'il n'existe que deux radars sur l'ensemble des routes de France, fussent-ils mobiles, il est probable que monterait doucement un sentiment d'impunité, une certitude qu'on ne sera pas, soi, frappé par un coup du sort aussi improbable. Cette situation, c'est celle dans laquelle se trouveront

49 - Art. 5 du règlement 2016/679 précité.

rapidement les entreprises privées de tailles petite et moyenne, de même que des collectivités territoriales de moindre importance. Car c'est un fait : les effectifs et le budget de la CNIL ne sont pas à la hauteur des missions confiées à cette autorité. Le rapport d'activité 2017 fait état d'environ 340 contrôles, dont une cinquantaine étaient spécifiquement dédiés à la vidéoprotection[50]. C'est beaucoup si l'on considère que la CNIL n'emploie que 198 personnes. C'est peu, très peu si l'on a égard au nombre des traitements de données déployés dans notre pays. Quant au budget de l'Autorité, il était en 2017 d'environ 17 millions d'euros. À titre de comparaison, le budget du Conseil supérieur de l'audiovisuel était de 38 millions d'euros[51].

En révisant tardivement la loi informatique et libertés, pour un résultat peu lisible, et en dotant la CNIL de moyens insuffisants, le gouvernement affiche une regrettable nonchalance à l'égard de la question des données personnelles. Pourtant, le modèle européen de protection des données aura besoin d'une promotion déterminée et d'un soutien sans faille de la part de l'ensemble des pays de l'Union, s'il veut s'imposer sur la scène mondiale. Car c'est bien de cela qu'il s'agit : d'une lutte pour imposer l'un des modèles possibles face à ses concurrents.

§2 : Le droit européen des données menacé au-dehors

Beaucoup de grandes entreprises souhaitent faire circuler les données personnelles des citoyens européens hors de l'Union, en particulier vers les États-Unis d'Amérique. Or, la sécurisation juridique d'un tel transfert se révèle particulièrement délicate, à supposer même qu'elle soit possible (A). Mais il n'y a là qu'une manifestation d'un mal plus profond : il est difficile d'envisager la coexistence de long terme, à l'échelle mondiale, de modèles de protection des données trop divergents (B).

50 - CNIL, 38ème rapport d'activité, présenté le 10 avril 2019, consultable sur cnil.fr.

51 - Source pour la CNIL : https://www.data.gouv.fr/fr/datasets/budget-de-la-cnil-1/. Pour le CSA : http://www.cbnews.fr/medias/plus-de-38-meur-de-budget-pour-le-csa-en-2017-a1031400.

A. Le difficile dialogue des modèles : le transfert des données hors de l'Union

Il est fréquent que les données personnelles circulent : d'un point de vue organisationnel, entre plusieurs co-responsables de traitement, entre un responsable de traitement et un sous-traitant, entre plusieurs sous-traitants successifs ; d'un point de vue géographique, entre pays de l'Union, mais aussi en direction de pays tiers. Or, une chaîne n'est aussi solide que le plus faible de ses maillons. Il ne servirait à rien d'instaurer un degré élevé de protection dans l'Union si des données pouvaient, en quelques millisecondes, se trouver collectées, hébergées, ou exploitées dans un pays n'y voyant qu'une matière première ordinaire. Dans la plupart des cas, il est ainsi difficile d'exporter des données hors de l'Europe dans un parfait respect du règlement.

La solution théoriquement la plus simple est celle-ci : « Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique »[52].

Mais un étudiant en droit déterminé du nom de Maximillian Schrems a balayé toute certitude en la matière. Membre, s'il en est, de cette élite étroite durablement marquée par les révélations d'Edward Snowden, il a remis en question devant la CJUE la décision de la Commission européenne de reconnaître les États-Unis d'Amérique comme un pays offrant une protection adéquate, dans le cadre du mécanisme appelé *Safe Harbor*. La Cour jugea notamment, à la lumière des révélations sur les programmes de la NSA, que « [...] une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée » [53]. Bien sûr, le RGPD a tiré les conséquences de cet arrêt en livrant à la Commission des instructions précises

52 - Article 45, 1) du règlement précité.

53 - CJUE, 6 octobre 2015, C-362/14, *Maximillian Schrems c/ Data Protection Commissioner*, §94.

dans l'examen des demandes d'adéquation présentées par les pays tiers[54]. Mais la Commission peut néanmoins encore se tromper, et ses décisions être encore invalidées par la Cour, avec effet immédiat au jour du prononcé de l'arrêt. Il n'est pas impossible que ce soit le destin du *Privacy Shield*, successeur du *Safe Harbor*[55].

Que faire, alors, si l'on ne peut faire confiance à une décision d'adéquation ? L'article 46 ouvre dans ce cas la porte à des « transferts moyennant des garanties appropriées »[56]. Deux de ces garanties sont actuellement pratiquées à une large échelle : les « règles d'entreprise contraignantes » et les « clauses types de protection des données adoptées par la Commission »[57]. Commençons par le second type, car il est le plus simple à mettre en œuvre : il suffit d'intégrer – certains diront de « copier-coller » – les clauses conçues par la Commission européenne dans un contrat conclu entre l'exportateur et l'importateur de données. Ce RGPD en miniature va alors contraindre l'importateur signataire, en théorie, à une rigoureuse discipline.

La solution semble simple. Trop peut-être, car il ne faut que quelques heures pour mettre en place le contrat, alors qu'il faudrait des mois d'efforts pour en tirer les conséquences techniques et organisationnelles, et certains risquent de s'en tenir à la première partie. Surtout, M. Schrems a trouvé là un nouveau champ de bataille : il estime que la décision par laquelle la Commission européenne a validé les clauses types peut être remise en cause de la même façon que ses décisions d'adéquation, si ces clauses sont insuffisamment protectrices. L'autorité irlandaise de protection des données a trouvé ses arguments convaincants et posé une question préjudicielle à la CJUE : pour ceux qui espéraient avoir trouvé là un fondement solide aux transferts internationaux de données, un nouveau naufrage est donc à redouter[58].

54 - Art. 45, 2) du règlement précité.

55 - En ce sens, V. not. C. Castets-Renard, « Adoption du Privacy Shield : des raisons de douter de la solidité de cet accord », *Dalloz IP/IT*, 2016.444.

56 - Pour une présentation plus détaillée de ces mécanismes : F. Naftalski, « L'impact du nouveau règlement sur les stratégies de transferts internationaux de données personnelles », *Dalloz IP/IT*, 2016.340.

57 - Art. 46, 2, b) et d).

58 - Hight court commercial, 3 octobre 2017, n° 4809 P, spéc. n° 338 : https://www.dataprotection.ie/docimages/documents/Judgement3Oct17.pdf.

La dernière solution envisageable, les « règles contraignantes d'entreprise » (en anglais *BCR*, pour *Binding corporate rules*), concerne les grands groupes de sociétés. Il s'agit de rédiger un document conçu sur mesure, contraignant et très détaillé sur la politique applicable aux données personnelles au sein de la multinationale considérée[59]. Il n'entrera pas en vigueur avant d'avoir été approuvé par les autorités de contrôle : contrairement aux « clauses types » de la Commission, il garantit donc véritablement un degré élevé de protection avant que la moindre information ne commence à circuler. Mais cette solution s'adresse exclusivement aux très grandes entreprises, qui seules auront les moyens et les compétences nécessaires à la rédaction de ces « règles contraignantes ».

Plus fondamentalement, si l'on reprend le cas d'export le plus courant, celui vers les USA, on comprend que ni les clauses-types, ni les *BCR* ne pourront résoudre l'intégralité des problèmes dénoncés par M. Schrems et les autres défenseurs de la vie privée[60]. Ces mécanismes essaient de faire surgir, sur une base contractuelle et non plus légale, des obligations à la charge des responsables de traitement et des sous-traitants, telles que celles de respecter une finalité de traitement, de minimiser les manipulations de données ou de les sécuriser. Mais la signature d'un simple contrat ne suffira pas à couper l'importateur de données de l'environnement législatif national dans lequel il évolue. Si l'on débarrasse la discussion sur les transferts internationaux de données de ses oripeaux techniques, la question qui surgit est d'une nature fondamentalement politique : si le reste du monde ne veut pas se hisser aux standards européens de protection des données, cela constituera un problème qu'aucun outil exclusivement juridique ne pourra résoudre. Dans un monde où les informations ne demandent qu'à circuler, les modèles de protection des données fondamentalement divergents ne pourront pas toujours coexister de manière simple et pacifique. Régulièrement, ils entreront en collision.

59 - https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr-binding-corporate-rules.

60 - En ce sens : B. Haftel, « Transferts transatlantiques de données personnelles : la Cour de justice invalide le Safe Harbour et consacre un principe de défiance mutuelle », *D.*, 2016.111.

B. L'affrontement des modèles : un choc des souverainetés

Puisqu'il semble aujourd'hui très difficile d'assurer à un export de données hors de l'Union européenne une sécurité juridique satisfaisante à long terme, quelles conséquences faut-il en tirer ? Ces flux doivent-ils tout simplement cesser ? Les grandes multinationales doivent-elles mettre en place deux circuits de traitement de données totalement hermétiques l'un à l'autre : un pour l'Europe, un pour le reste du monde ? On peine à l'imaginer. Certains sites américains, notamment les versions en ligne de grands quotidiens régionaux, ont pourtant choisi de faire sécession d'avec l'Internet européen. Le *Los Angeles Times*, par exemple, indique à ses visiteurs du vieux continent : « *Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism* »[61]. Le symbole constitué par ces blocages de sites est fort, et l'on peut comprendre qu'il ait marqué les esprits[62]. Un « rideau de fer numérique » s'abattrait-il autour de l'Union ? La stratégie autarcique du *Los Angeles Times* est cependant réservée à des acteurs qui tiraient des revenus négligeables, voire nuls, des visites des internautes européens. Tous ceux pour qui l'Europe constitue un marché important, fût-il secondaire, ou qui souhaitent tout simplement véhiculer une image de plus grande ouverture internationale, seront poussés à trouver des solutions pour agir conformément au règlement. Le quotidien national *USA Today* propose ainsi une version de son site internet « spéciale Europe » sans aucun traceur ni publicité ciblée[63].

61 - Il s'agit de la page http://www.tribpub.com/gdpr/latimes.com/ telle qu'elle s'affichait encore à la date du 10 décembre 2018.

62 - Par ex. T. Noisette, « RGPD : des sites américains claquent la porte au nez des internautes européens », article n*ouvelobs.com* du 28 mai 2018.

63 - https://eu.usatoday.com/EU-learn-more/ : « This site does not collect personally identifiable information or persistent identifiers from, deliver a personalized experience to, or otherwise track or monitor persons reasonably identified as visiting our Site from the European Union. We do identify EU internet protocol (IP) addresses for the purpose of determining whether to direct you to USA TODAY NETWORK's EU Experience ».

À présent, que va-t-il se passer ? Entre les modèles européen et américain, la tension continue à monter. La question de la portée territoriale du droit au déréférencement en constitue l'une des plus frappantes manifestations. Dans un arrêt très remarqué de 2014, la Cour de justice de l'Union européenne avait décidé qu'une personne est en droit de demander à un moteur de recherche généraliste, tel que celui de Google, de retirer certains résultats associés à une recherche portant sur ses seuls nom et prénom[64]. Peuvent ainsi être supprimés des liens qui mènent vers des pages pourtant parfaitement licites au regard des règles régissant la liberté d'expression. La solution peut choquer celui qui la découvre pour la première fois. Elle s'explique pourtant : un moteur de recherche peut avoir pour effet d'attacher une information gênante à un individu durant des décennies, alors qu'elle serait sans cela rapidement retournée dans l'ombre. Voici qui rappelle une autre formule visionnaire de Jean Foyer, en 1977 : « [...] l'ordinateur a une mémoire qui, à la différence de la mémoire des hommes, n'a pas la faculté d'oublier. Il n'oublie que ce qu'on efface en lui ». La jurisprudence *Google Spain* constitue un remède à cette hypermnésie informatique, raison pour laquelle elle est parfois désignée sous l'appellation, techniquement trop vague, de « droit à l'oubli ». L'aspect qui nous intéresse ici tient à la manière dont cette décision a été appliquée, s'agissant d'un point sur lequel elle n'avait pas pris position explicitement : sa portée territoriale. Lorsqu'elle devait retirer des résultats de recherche relatifs, par exemple, à un internaute français, la société Google avait commencé par le faire seulement sur l'adresse www.google.fr. La CNIL ne s'en est pas satisfaite, car alors un Espagnol pouvait toujours consulter une version non expurgée du moteur sur www.google.es. Pire, un

64 - CJUE, 13 mai 2014, *Google Spain SL, Google Inc. c./ Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12 : *RLDI*, août 2014, n° 107, p. 32, note O. Pignatari ; *RJPF*, juill. 2014, n° 7, p. 19, note S. Mauclair ; *JCP G,* juin 204, n° 26, p. 1300, note L. Marino. *Adde* not. J.-M. Bruguière, « Droit à l'oubli numérique des internautes ou... responsabilité civile des moteurs de recherche du fait du référencement ? », *CCE,* mai 2015, n° 5, p. 15 ; R. Perray et P. Salen, « La Cour de justice, les moteurs de recherche et le droit "à l'oubli numérique" : une fausse innovation, de vraies questions », *RLDI,* nov. 2014, n° 109, p. 35 ; V.-L. Bénabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », *D.*, 2014, p. 1476 ; N. Martial-Braz et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : le droit à l'oubli numérique, l'éléphant et la vie privée », *D.,* 2014, p. 1481 ; L. Marino, « Comment mettre en œuvre le "droit à l'oubli" numérique ? », *D.,* 2014, p. 1680.

internaute français pouvait en réalité accéder lui aussi aux résultats sans censure s'il forçait la connexion à s'instaurer avec google.com ou .es plutôt que .fr. L'Autorité demandait alors qu'un résultat retiré le soit sur toutes les versions mondiales du moteur, ce qui aurait eu pour effet d'altérer même des résultats affichés par un internaute américain sur le sol des USA. Google a alors formulé une nouvelle proposition : détecter, en utilisant l'adresse IP, que la requête était formulée par un internaute situé sur le territoire national du demandeur, et expurger alors les résultats pour toutes les extensions utilisées dans l'adresse du moteur. La CNIL a considéré une nouvelle fois cette proposition comme insuffisante, notamment car « il existe des solutions techniques qui permettent de contourner la mesure de filtrage proposée par la société en permettant à l'internaute de choisir l'origine géographique de son adresse IP (utilisation d'un VPN par exemple) [...]. Seule une mesure s'appliquant à l'intégralité du traitement lié au moteur de recherche, sans distinction entre les extensions interrogées et l'origine géographique de l'internaute effectuant une recherche est juridiquement à même de répondre à l'exigence de protection telle que consacrée par la CJUE »[65]. Saisi d'un recours contre cette décision, le Conseil d'État a posé une question préjudicielle à la CJUE, à laquelle il n'a pas encore été apporté de réponse[66]. L'affaire a suscité une vive émotion outre-Atlantique, où l'on accepte mal qu'une autorité administrative française entende altérer l'information accessible aux Américains sur leur propre sol[67]. L'Europe pourrait rétorquer que de telles altérations ne se produisent que lorsque des données personnelles de citoyens de l'Union sont en cause, et que le lieu où les informations sont consultées n'est pas la considération fondamentale.

Par-delà les argumentations juridiques, on aperçoit donc à nouveau la question politique et, surtout, le choc frontal des souverainetés. Des visions différentes du monde entrent en collision et cherchent à s'imposer. Disons-le d'emblée : il est vain d'espérer que le modèle européen essaime dans son intégralité. La jurisprudence sur le déréférencement en constitue un excellent exemple : certains points

65 - Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société X.

66 - CE, 19 juillet 2017, *GOOGLE INC.*, N° 399922.

67 - V. dans le présent ouvrage E. Weil, « Le règlement général sur la protection des données à caractère personnel appliqué aux états tiers : une appréciation de son caractère extraterritorial », spéc. les références citées notes 97 et s.

du régime européen sont le fruit d'un arbitrage si difficile entre des valeurs toutes cardinales – ici, la vie privée contre la liberté d'expression – qu'un large consensus à travers le temps et l'espace apparaît improbable. Tout le monde ne sera pas convaincu. Mais si l'on revient au cœur de ce qui constitue le RGPD, il s'agit d'accepter quelques idées simples : les données personnelles ne constituent pas une matière première comme une autre pour les entreprises ; elles doivent être manipulées d'une main tremblante, rassemblées avec sobriété, pour des objectifs précis, et faire l'objet de protections sérieuses contre les erreurs et les agressions. À partir de là, proposons un parallèle, quelque peu forcé, mais à caractère pédagogique, avec la lutte contre le réchauffement climatique. Si de nombreux pays sont convaincus que les objectifs poursuivis par l'Europe sont louables et servent le bien commun, ils peuvent les rallier et former une zone relativement homogène, au sein de laquelle le jeu économique se déploie ensuite, dans le respect de règles comparables. Mais si certains géants comme les USA considèrent que tout ceci n'est qu'obstacles à l'efficacité de leurs modèles d'affaires, ils peuvent envoyer au monde une contre-proposition, qui risque d'avoir des adeptes, au sein de laquelle les entreprises évoluent sans ces contraintes, ce qui suppose des coûts moindres et des bénéfices plus élevés. Pour représenter cette lutte d'influence, l'image de deux blocs statiques entre lesquels un rideau de fer serait tombé n'est décidément pas la bonne. La tectonique des plaques constitue une meilleure représentation : des deux modèles qui se pressent actuellement l'un contre l'autre, l'un finira par passer au-dessus. L'issue de cet affrontement est en partie dans les mains de l'opinion publique américaine, comme l'a montré l'adoption récente par la Californie, pourtant berceau des GAFA, d'un *Consumer Privacy act* améliorant singulièrement la protection des données personnelles de ses citoyens[68]. L'affaire *Cambridge Analytica* avait donné naissance à une pétition signée plus de 600 000 fois, enjoignant le législateur californien d'agir[69]. À l'heure où le volontarisme de nos décideurs politiques en matière de protection des données manque de constance, il est fort possible que le meilleur ambassadeur du modèle européen se nomme Mark Zuckerberg.

68 - V. not. caprivacy.org, « AB 375 Signed - Californians for Consumer Privacy Applauds Successful Passage of Groundbreaking Legislation », article du 28 juin 2018.

69 - A. Schwartz, L. Tien et C. McSherry, « How to improve the California Consumer Privacy Act of 2018 », article *eff.org* du 8 août 2018.

PREMIÈRE PARTIE :

APPROCHE TRANSVERSALE

LA PROTECTION DES DONNÉES PERSONNELLES ET LA MORT

Céline Béguin-Faynel[1]
Maître de conférences en droit privé à l'Université du Mans (THÉMIS-Um ; EA-4333)
Responsable du Certificat Informatique et Internet, niveau 2, spécialité Métiers du Droit (C2I2®)

« Il n'est probablement pas loin le jour où, en accompagnement de l'urne funéraire qui recèle les cendres du dé funt, sera proposé aux familles l'ensemble des données numériques accumulées au cours de sa vie, comme l'historique indigeste de son existence contenant son dossier médical, ses émotions, ses habitudes de consommation, ses préférences sexuelles et intellectuelles ».
M. Dugain, C. Labbé, L'homme nu, la dictature invisible du numérique, Robert Lafon, Plon, 2016, p. 12.

Au tournant du XXIe siècle, développer la société de l'information fut un fer de lance de la politique européenne[2]. La mutation du flux informationnel a pris corps dans le quotidien des pays industrialisés. Très récemment, on a pu relever que le monde s'organise vers une potentielle « *datacratie* ». Émerge une forme innovante de régulation « par la data », tandis que Bruxelles prône l'innovation pilotée par les données, *data-driven innovation*, comme clé de la croissance et de l'emploi[3]. Dans la dernière décennie, la production de données s'est en

1 - Mes sincères remerciements vont à Emmanuel Netter pour m'avoir associée à ce projet et avoir accepté une remise différée de cette recherche. Elle prolonge la réflexion engagée dans le *Traité des nouveaux droits de la Mort*, L'Épitoge Lextenso éd., 2014, auquel Magali Bouteille-Brigant m'avait proposé de contribuer. Qu'elle soit remerciée de m'avoir introduit à ce champ d'étude, m'ayant conduit à explorer le sort des données personnelles après la mort.

2 - Conseil européen de Lisbonne, concl. de la Présidence, 23-4 mars 2000, <http://www.europarl.europa.eu/summits /lis1_fr.htm> [Les liens vers les sites Internet de l'article ont été vérifiés au 21 février 2019].

3 - Dossier *Datacratie*, *Pouvoirs* 2018/1, n° 164 ; J. Van Dijck, « Datafication, dataism and dataveillance », *Surveillance & Society* 2014, 12/2, p. 197 ; C. Berthet, C. Zolynski, « L'empouvoirement" des citoyens de la République numérique regards sur une réforme en construction », *RLDI* 2018/1, n° 144, p. 60, spéc. n° 14 ; « *Guidance on private sector data sharing* », 25 avr. 2018, <https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing>.

effet développée de manière exponentielle[4]. Il en est résulté une mise en données du monde, qui a conquis de nouvelles terres immatérielles[5]. Les évolutions technologiques des outils informatiques, mais aussi l'amélioration constante de leurs capacités de captation, reproduction et d'analyse de données, ont permis l'avènement d'une ère numérique. De cette révolution scientifique découlent diverses évolutions sociales, qui influencent largement les modes de vie. Les relations humaines et économiques au sein de la société en ressortent redéfinies. La mémoire des hommes et de leurs archivistes s'adapte[6]. Pour autant, l'innovation numérique ne saurait être réduite à « une nouvelle forme qui succéderait à toutes celles – livres, enregistrements audiovisuels analogiques, spectacles, récits – sous lesquelles les mémoires ont circulé et circulent encore »[7]. Plus profondément, elle façonne les relations entre mémoire et Internet en tant que phénomène socio-culturel, technique, économique.

L'attitude des « *consom-acteurs* » numériques évolue. Dès 2009, alors que se développait en France l'usage des réseaux sociaux numériques, on soulignait l'apparition d'un *homo numericus*, et la difficulté à vivre une vie déconnectée[8]. Ces réseaux ont modifié notre appréhension du monde et ce qui est ressenti comme relevant de la vie privée

4 - G. Siméon, « Données, le vertige », 3 déc. 2012, <http://www.liberation.fr/futurs/2012/12/03/donnees-le-vertige_8645 85> notant qu'en 2010 tous les deux jours étaient générées autant de données qu'entre l'aube de l'humanité et 2003.

5 - S. Abiteboul, V. Peugeot, *Terra data*, Le Pommier Universcience, Paris 2017, p. 11-31 ; P. Gargov, M. Baldassi, C. Rotrou, *Mise en données du monde : imaginaires en équation gouverner par la donnée : entre transparence et résistance, quelle prospective ?*, avr. 2017, p. 5-8 ; CSA Lab, *Les mutations de la mise à disposition de contenus audiovisuels à l'ère du numérique : conséquences et enjeux, Rapport 1 Le rôle des données et des algorithmes dans l'accès aux contenus*, jan. 2017, spéc. p. 6-8 ; A. Basdevant, J.-P. Mignard, *L'Empire des données - Essai sur la société, les algorithmes et la loi*, Don Quichotte éd. 2018, p. 10-2.

6 - *Id.*, p. 317-32 ; M. Serres, *Petite poucette*, Le Pommier Manifestes, Paris, 2012, p. 12-4 sur la transformation cognitive induite par l'Internet pour les générations envoyant avec les pouces des messages écrits par téléphone ; M. Lasterre, « L'archiviste est-il soluble dans le numérique ? », *La Gazette des archives,* 2015/4, n°240, p. 339.

7 - R. Besson, C. Scopsi, « La médiation des mémoires en ligne », *Les Cahiers du numérique* 2016/3, vol. 12, p. 9, spéc. p. 9-14 sur la médiation numérique mettant en relation avec une information via un support dématérialisé.

8 - Dossier *Homo numericus*, *Esprit* 2009/3, spéc. M.-O. Padis, « L'internet et les nouveaux outils numériques », p. 68 ; J.-C. Heudin, *Immortalité numérique*, Science ebook, 2016, p. 95-101 chap. « *Homo numericus* ». *Adde*, J. de Rosnay, *La révolte du pronétariat, des mass média aux média de masses*, Fayard, 2015, p. 9 et 12 décelant une démocratie de la communication issue des pronétaires usagers des technologies de l'information générant de gros flux de visiteurs.

d'une personne[9]. Se révèle désormais une « *tech-sistence* », une vie appareillée, prothétique et dépendante de la technologie, axée sur la nécessité d'enregistrer et de « partager » sur les réseaux sociaux chaque geste et action[10], renforcée par l'usage de téléphones mobiles toujours plus performants[11]. Mais l'évolution des usages impose une prise de conscience face à « l'hypermnésie du web »[12] conservant de manière inaltérable et universelle les informations qui y ont été intégrées...

Les progrès numériques dans la conservation des données tendent à être exploités dans la quête d'une forme d'immortalité : recherches vers le post-humain, le transhumanisme ou encore une immortalité immanente assise sur la technologie numérique et les biotechnologies[13]. Même sans chercher à différer la mort physique du corps, Internet conduit au contournement de la « mort sociale », par la survivance de l'identité numérique pour dépasser, voire vaincre, la mort[14]. Analyser le devenir des éléments identitaires laissés sur Internet après le décès nécessite une approche pluridisciplinaire. Du point de vue sociologique et philosophique, « les pratiques techno-spirituelles et communicationnelles relatives à la mort » apparaissent comme la traduction d'une quête de personnalisation pour accomplir des rituels de commémoration

9 - D. Piotet, « Comment les réseaux sociaux changent notre vie », *Esprit* 2011/7, p. 82 citant l'analyse de la vie privée de l'ethnologue D. Boyd, <http://www.danah.org/papers/talks/2010/SXSW2010.html> ; L. Merzeau, *Identity commons* : du marquage au partage, *Identités numériques*, L'Harmattan, 2014, p. 35 sur la régulation de l'image.

10 - B. Naivin, « Le numérique a-t-il déjà modifié notre être ? », *Nectart*, 2017/1, vol. 4, p. 129 ; *Id.*, *Selfie, un nouveau regard photographique*, L'Harmattan, 2016 recension *in* <https://www.huffingtonpost.fr/bertrand-naivin/selfie-symbole-dune-techsistence_b_10233860.html>.

11 - Le trafic de données est dopé par l'usage de téléphones mobiles, v. R. Gueugneau, « Mobile : le trafic data a été multiplié par 18 en cinq ans », 9 févr. 2017, <https://www.lesechos.fr/09/02/2017/lesechos.fr/0211788047116_mobile---le-trafic-data-a-ete-multiplie-par-18-en-cinq-ans.htm#PPsIfHP2Hqbv3v8E.99>.

12 - J. Giusti, A. Ndiaye, « L'identité numérique, monnaie d'aujourd'hui et rente de demain », *RLDI* 2017/8, p. 56, spéc. IIB renvoyant au droit à l'oubli liberté d'extraire de la sphère publique une information issue du passé.

13 - J.-C. Heudin, *op. cit.*, p. 25-75 sur la quête religieuse, scientifique et numérique d'immortalité ; J.-M. Besnier, *Demain les posthumains : Le futur a-t-il encore besoin de nous ?*, Fayard Pluriel, 2012 ; F. Gamba, « Rituels postmodernes d'immortalité : les cimetières virtuels comme technologie de la mémoire vivante », *Sociétés* 2007/3, n° 97, p. 109, spéc. p. 111-2 voyant les rituels funèbres comme stratégies d'immortalité ; *Id.*, « *Body enhancement* ou écologie corporelle ? Le défi de l'immortalité contemporaine », *Corps* 2017/1, n° 15, p. 233, spéc. p. 233-5.

14 - H. Bourdeloie, « Usages des dispositifs socionumériques et communication avec les morts », *Questions de Communication* 2015/28, p. 101, spéc. p. 114.

numérique[15]. Ces pratiques de deuil se développent sur les réseaux sociaux numériques et des sites Internet mémoriaux, qui permettent le maintien des relations avec le défunt et de croire à une « existence numérique *post-mortem* éternelle », qui donnerait lieu à une nouvelle forme de religion en ligne[16]. À la différence de la vie matérielle, dans les espaces numériques, la mort n'est plus circonscrite dans un temps et un lieu précis, elle oblige les survivants à gérer une présence continue du défunt en ligne et à adopter une nouvelle distance[17]. En effet, la présence de la personne décédée demeure sur les réseaux sociaux numériques si le compte n'a pas été désactivé ou est devenu un mémorial. Variés, les usages mémoriaux sur Internet posent la question des « éternités numériques » et de la construction des identités numériques *post-mortem*[18] ; il peut s'agir de sites mémoriaux, réseaux sociaux numériques, mais aussi des sites spécialisés, *cybercimetières*, du marquage par *QR codes* des stèles et leur géolocalisation[19]. Les nouvelles pratiques funéraires en ligne semblent participer du mouvement de déni et de mise à distance de la mort formulé par Philippe Ariès en 1975[20].

15 - F. Gamba, *Mémoire et immortalité aux temps du numérique*, Paris, L'Harmattan, 2016, spéc. IIIe partie ; *Id.*, La personnalisation numérique de nouveaux rituels funéraires, *in La fabrication des rites*, D. Jeffrey, A. Cardita (Dir.), Presses de l'Université Laval, 2015, p. 195.

16 - H. Bourdeloie, *op. cit.*, p. 103 et 120-1 ; F. Gamba, « Rituels postmodernes (...) », *op. cit.*, p. 116 estimant que ces rituels plus personnels montrent une « resacralisation de la mort », que l'on accepte de partager avec d'autres bien qu'elle signifie une « reliance avec les morts » ; Dossier Vie éternelle, « Comment le transhumanisme concurrence les religions », *Usbek & Rica*, jan. févr. mars 2018, n° 21, p. 34-49 ; S. Guillemot, A. Gourmelen, « Quand les entreprises s'emparent de la mort numérique, qui sont les consommateurs potentiels ? », *Revue française de gestion* 2017/1, vol. 262, p. 123, spéc. p. 126 renvoyant au sacré, à la vie éternelle digitale.

17 - Dossier *Les jeunes et la mort*, Frontières, 2017/1, n° 29, spéc. les articles de J. Lachance, M. Julier-Costes, « Le deuil dans un monde connecté », <https://www.erudit.org/fr/revues/fr/2017-v29-n1-fr03382/1042980ar/resume/> ; et F. Quinche, « aire mémoire sur Internet. Les réseaux sociaux et sites de commémoration induisent-ils de nouveaux rapports à la mort ? », <http://id.erudit.org/iderudit/1042981ar>.

18 - F. Georges, *Éternités numériques. Les identités numériques* post mortem *et les usages mémoriaux innovants du web au prisme du genre. Programme financé par l'ANR Sociétés innovantes édition 2013*, <hal-01575171>.

19 - *Id.* ; F. Gamba, *Mémoire et immortalité* (...), *op. cit.*, p. 53-69 sur les cimetières et 79-100 sur Twitter et Youtube.

20 - *Id.*, « Le spiritisme en ligne. La communication numérique avec l'au-delà », *Les Cahiers du numérique*, 2013/3, vol. 9, p. 211 exposant le déni de la mort au XXe siècle et l'émergence d'une « représentation agissante » des défunts dans les réseaux socionumériques, niant leur trépas. Comp. T. Châtel, « Le besoin de ritualisation devant la mort », 29 sept. 2013, < https://www.millenaire3.com/Interview/2013/le-besoin-de-ritualisation-devant-la-mort> relativisant ce déni.

En parallèle du phénomène de deuil digital, la transmission involontaire d'informations nous paraît le volume le plus important du trafic *via* les outils numériques. Des travaux sémiologiques sur la communication ont pu dégager un concept d'hypostase du mort « ensemble des traces numériques (données personnelles, fichiers non partagés sur le disque dur de l'usager) qui manifestent une qualité de la présence passée du défunt (le « ça a été ») »[21]. Des hypostases sont laissées par le mort « données personnelles numériques, qu'elles soient issues du numérique (document partagé), numérisées par le sujet (selfies, date, heure) », elles sont « l'équivalent numérique des objets ayant appartenu au défunt ou de ses portraits photographiques utilisés dans les autels domestiques laïques et spirituels. Elles partagent avec ces objets et effets personnels, une trace de la vie et du vivant défunt ». Une approche anthropologique a également mis en avant « *l'afterlife numérique* », en tant que phénomène d'organisation par les usagers de toutes leurs données personnelles après leur mort par des dispositions concernant leur stockage, destruction ou utilisation posthume[22]. Il conviendra de protéger ces contenus numériques créant une identité *post-mortem* spécifique par des mesures juridiques et des intervenants appropriés. En ce sens, Michel Serres relevait qu'un capital des données se forme et nécessiterait des « dataires », ou notaires des données, qui seraient dépositaires, comme pour les secrets des personnes, leurs testaments, contrats de mariage[23].

Le raz de marée généré par l'afflux de données bouleverse également l'organisation des rapports juridiques. Les évolutions techniques et sociales commandent de s'interroger sur les aspects juridiques relatifs à leur traitement, leur archivage et encore leurs conditions d'accès et de rectification dans le respect des droits des personnes qui les émettent. Le « droit de la mort » était ignoré de l'ancien

21 - *Id.*, *De l'identité numérique aux éternités numériques : la mort extime. L'usage des grandes bases de données personnelles après le décès des usagers*, 2018, <halshs-01683260>, spéc. p. 21-2.

22 - F. Gamba, *Mémoire et immortalité* (...), *op. cit.*, p. 203-13 ; E. Carroll, J. Romano, *Your Digital Afterlife : When Facebook, Flickr and Twitter are your estate, What's Your Legacy ?* New Rider's Press, 2010, Berkeley.

23 - B. Ferran, L. Ronfaut, M. Serres, « La question est de savoir qui sera le dépositaire de nos données », 13 mars 2015, <http://www.lefigaro.fr/secteur/high-tech/2015/03/13/32001-20150313ARTFIG00159-michel-serres-la-question-est-de-savoir-qui-sera-le-depositaire-de-nos-donnees.php>.

droit, empreint d'une vision religieuse de la destinée humaine. Apparaissant comme un concept récent, il a notamment permis d'organiser une transmission ordonnée du patrimoine par le droit civil[24]. Encore plus jeune, le droit des données personnelles, né il y a juste quarante ans[25], se devait de construire une législation *post-mortem*. Le droit des données personnelles est un droit des vivants. L'associer, voire l'étendre, à des personnes décédées peut surprendre. Néanmoins, cette étude tend à dépasser ce clivage, opposant personne vivante et défunt privé de personnalité, pour résoudre les questions liées au devenir des informations sur la personne, qui ne disparaissent pas avec sa mort, car, s'en étant dissociées, elles lui survivent. Les données à caractère personnel sont les informations identifiantes, dont la définition s'est enrichie au-delà des données objectives sur l'individu (âge, sexe, profession...) aux goûts, opinions, relations, déplacements, signaux biologiques ou corporels[26]. Elles s'élargissent encore des traces laissées par l'internaute ainsi que des caractéristiques spécifiques figurant dans ses comptes d'accès sur Internet, ses profils d'adhérent ou abonné à un réseau social, à un site de jeu en ligne, un site commerçant ou d'une administration publique, y compris ses identifiants et code d'accès[27].

Quid des données personnelles *post mortem* ? Faut-il enterrer les données avec le mort en scellant ses comptes en ligne tels des cénotaphes numériques ou les supprimer dans un oubli généralisé ?

24 - J. Moreau-David, « Approche historique du droit de la mort », D. 2000. 266, spéc. introduction et II.

25 - Loi n° 78-17 du 6 janv. 1978 *relative à l'informatique, aux fichiers et aux libertés*, JO 7 janv. 1978, p. 227.

26 - Conseil d'État, *Le numérique et les droits fondamentaux*, Rapport public 2014, Doc. fr., spéc. p. 16 ; Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avr. *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 95/46/CE* (Règlement général sur la protection des données), *JOUE* L 119/1, 4 mai 2016, p. 1, art. 4, incluant dans la définition des données personnelles, celles permettant l'identification (in)directe par « un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale », ainsi que les données de localisation, un identifiant en ligne.

27 - V.-L. Benabou, « L'extension du domaine de la donnée », *Legicom* 2017/2, vol. 59, p. 3, spéc. p. 4-6 ; C. Béguin-Faynel, « Héritage numérique & cadavre(s). Pour un testament des dernières volontés numériques », *in Traité des nouveaux droits de la Mort*, *Tome II : La mort, incarnation(s) cadavérique(s)*, Chapitre V. section 3, M. Touzeil-Divina, M. Bouteille-Brigant, J.-F. Boudet (Dir.), L'Épitoge Lextenso éd., 2014, p. 67, spéc. p. 70-3. *Adde*, J. Giusti, A. Ndiaye, « L'identité numérique, monnaie » (...), *op. cit.*, spéc. I distinguant identité « vitrine » en ligne et administrative.

Comment organiser l'ultime volet de l'*e-réputation* et prévenir les responsables de traitement de données du décès et leur indiquer que faire de ces informations ? Les héritiers et les proches peuvent-ils intervenir *post-mortem* ? Ces difficultés ont été abordées par la presse et sur Internet dès 2005 aux États-Unis, d'abord sous l'angle de l'accès aux comptes de réseaux sociaux de membres décédés à la demande de leurs proches, puis celui des directives données aux tiers en cas de décès. Corrélée au développement des réseaux sociaux plus tardif en France, la question du « vivre et mourir » sur Internet est plus récente dans l'Hexagone. Peut-être est-ce la conséquence du refus de la société de l'information de penser l'oubli, convaincue à tort qu'il n'est pas nécessaire de choisir entre effacer et conserver, comme si le stockage machinique pouvait suffire à constituer une mémoire[28]. En 2007, le Groupe de travail de l'article 29 avait rappelé que la directive de 1995 sur la protection des données personnelles ne s'appliquait pas aux informations du mort, car lorsqu'une personne décède ses données ne sont plus à caractère personnel, en ce sens que la personne n'existe plus[29]. Son avis relevait cependant que certains législateurs nationaux pouvaient décider de leur étendre la protection transposée en droit interne. Et d'ajouter qu'en dehors de la législation sur les données personnelles subsistait la *personalitas praeterita* permettant la protection des informations relatives aux personnes décédées par des dispositions spécifiques sur le respect de l'image, de l'honneur afin de protéger sa mémoire, tandis que perdure au-delà du décès l'obligation de confidentialité du personnel médical. Dans cette logique protectrice des personnes, le droit français prévoyait déjà, avant la loi du 7 octobre 2016, des règles préservant ponctuellement les données *post-mortem* en droit civil et de la santé.

Dans son rapport 2013, la Commission nationale de l'informatique et des libertés a ouvert le débat sur « comment concilier le droit à l'oubli numérique et les possibilités d'atteindre l'éternité numérique offertes par la vie en ligne ? » et désamorcer les conflits potentiels

28 - L. Merzeau, « Les données *post mortem* », *Hermès, La Revue* 2009/1, vol. 53, p. 30, spéc. p. 30-1.

29 - Avis 4/2007 sur le concept de données à caractère personnel, spéc. p. 25 citant *Procès-verbal du Conseil de l'Union européenne, 8.2.1995, n° 4730/95*, art. 2a. Organe consultatif indépendant de l'Union Européenne sur la protection des données et la vie privée, ce groupe titre son nom de l'article 29 de la directive 95/46/CE.

au décès entre les héritiers et les professionnels de l'Internet[30]. Jusqu'en 2016, en l'absence de norme, seule la volonté individuelle permettait en effet d'organiser la transmission aux proches et héritiers des identifiants nécessaires pour administrer le sort des données avec les opérateurs contractuels du défunt, refusant de faire suite aux demandes des ayants droit après son trépas ; que l'on envisage un testament[31] ou un mandat *post-mortem* sur les données personnelles collectées[32]. La survivance d'une certaine protection est assurée par l'article 40-1 venu amender la loi Informatique et libertés. Issu de la loi du 7 octobre 2016, il affirme le principe d'extinction au décès de la personne des droits relatifs à ses données personnelles, qu'il tempère immédiatement par une importante exception en étendant expressément les prérogatives que la loi du 6 janvier 1978 confère à la personne concernée par un traitement de données personnelles après sa mort[33]. Il permet à la personne de transférer « temporairement » vers autrui certains droits sur les données protégées par des directives générales ou spéciales expressément adoptées. Après quatre moutures assez disparates[34], le texte confère un rôle déterminant à la volonté du défunt dans le sort de ses données *post-mortem*. On attend toujours la publication de son décret d'application pour organiser notamment le répertoire des directives, qui était annoncé pour mars 2017[35]. Il était nécessaire de légiférer pour éviter que les opérateurs économiques du secteur numérique ne continuent de bloquer tout accès aux proches ou décident de régir exclusivement la situation par leurs conditions générales de vente ou d'utilisation du service,

30 - CNIL, *34ème Rapport annuel 2013*, mai 2014, p. 73-4 et *Fiche pratique, Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ?*, 29 oct. 2014.

31 - A. Favreau, « Mort numérique, quel sort juridique pour nos informations personnelles ? », *RLDC* 2015/4, p. 66 ; A. Mâzouz, « Être ou ne plus être, les volontés à l'origine de la mort numérique », *in Droit et réseaux sociaux,* V. Ndior (Dir.), coll. Lejep Univ. Cergy-Pontoise, Lextenso éd. 2015, p. 183 ; C. Béguin-Faynel, *op. cit.*, spéc. II.

32 - *Id.*, Mort numérique : précisions sur la nature et le régime du contrôle post mortem des données à caractère personnel collectées, RLDI 2016/12, p. 36, spéc. IB.

33 - Loi n° 2016-1321 du 7 oct. 2016 *pour une République numérique*, JO 8 oct. 2016, Texte n°1, art. 63.

34 - A. Favreau, « L'accès des proches aux données personnelles du défunt », *in Numérique – Nouveaux droits, nouveaux usages*, S. Chatry, Th. Gobert (Dir.), Éd. Mare & Martin, 2017, p. 65, spéc. p. 68.

35 - Calendrier d'adoption des décrets d'application de la loi, <https://www.economie.gouv.fr/republique-numerique>.

qui pourraient prévoir la suppression pure et simple des comptes en cas de décès de l'utilisateur[36]. De plus, un régime légal supplétif, à défaut de directives, confère une marge d'action aux héritiers du mort inspiré des solutions déjà dégagées. Notons que l'ordonnance du 12 décembre 2018 a transféré aux articles 84 et 85 de la loi de 1978 le contenu de l'article 40-1, complété par un article 86[37]. Ce dispositif est désormais valorisé dans un chapitre V dédié, consacré aux « Dispositions régissant les traitements de données à caractère personnel relatives aux personnes décédées ». Ces textes s'avèrent la seule législation spéciale applicable, car les données à caractère personnel des personnes décédées n'entrent pas dans le champ d'application du nouveau règlement européen, laissant toute latitude aux États membres pour y pourvoir[38]. Cette frilosité, qui lui a été reprochée[39], tient à l'absence de consensus européen.

La mort est un état définitif, qui s'appréhende dans le temps. Point d'orgue de l'existence, elle articule un avant : une vie, dont la durée est limitée, et un après sans limite temporelle. Anticiper les conséquences de ce changement d'état est possible de son vivant[40], tandis qu'après la mort il incombera aux proches d'agir selon leurs droits respectifs. Trois points s'avèrent fondamentaux : quand intervenir, quelles mesures prendre et par quel acteur. Les directives adoptées *ante-mortem* par le défunt missionnent un tiers pour mettre en œuvre la protection de ses données après son décès. En outre, si le mort est resté passif, laissant la loi investir ses proches de différentes facultés, encore faudra-t-il déterminer comment celles-ci s'articulent avec les droits des vivants chargés de les appliquer. Par suite, examinons les mesures prises de son vivant par la personne

36 - Étude d'impact, Projet de loi pour une République numérique, 9 déc. 2015, p. 96 et 109 ; Rép. Min. n°13422, JO Sénat Q, 1er déc. 2016, p. 5198 ; Rép. Min. n°94520, JOAN Q, 29 nov. 2016, p. 9844.

37 - Ordonnance n° 2018-1125 du 12 déc. 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JO 13 déc. 2018, texte n° 5 remaniant l'organisation interne de la loi de 1978 renumérota ce texte, ventilé en deux articles sans en modifier le contenu.

38 - Règlement général sur la protection des données, consid. 27, 158, 160.

39 - N. Martial-Braz, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017 p. 253, spéc. I *in fine*.

40 - M. Magnusson, *La vie en ordre*, Flammarion, 2018 exposant le concept suédois de *döstädning*, rangement pré-mortem pour ne laisser que le meilleur de soi à ceux qui restent (tri des vêtements, objets, souvenirs ou secrets).

pour régir le sort de ses données personnelles après décès (sect. 1) puis la mise en œuvre d'une protection *post-mortem* de ses données par ses héritiers, qu'ils soient investis ou non par ses directives (sect. 2).

Section I – Les mesures *ante mortem* organisées par la personne

La loi *pour une République numérique* inaugure un dispositif inédit prévoyant comment se transmettent des directives sur la préservation des données personnelles à la mort d'une personne, inséré dans un nouvel article 40-1 de la loi Informatique et libertés du 6 janvier 1978. Son contenu, déplacé aux articles 84 et 85, laisse planer diverses incertitudes sur la nature des mesures prises et leur portée. La loi prolonge les droits de la personne, dont les données personnelles font l'objet d'un traitement, ce qui implique un questionnement sur la portée du nouveau dispositif au regard du droit de la protection des données personnelles (§1). Des interrogations se font parallèlement jour sur la mise en pratique d'une administration *post-mortem* de l'identité numérique forgée du vivant de la personne (§2).

§1 : Proroger les droits des personnes sur leurs données *après la mort*

En 2016, la loi *pour une République numérique* avait innové en intégrant un facteur temporel dans le droit des données à caractère personnel en régissant dans la loi du 6 janvier 1978 la période *post-mortem*. Un double principe en ressort. Bien que ces droits soient viagers, comme s'éteignant « au décès de leur titulaire », leur survie provisoire est prévue par le nouveau cadre légal, qui autorise en effet toute personne à prendre des directives destinées à la « conservation, à l'effacement et à la communication de ses données à caractère personnel » et prévoit un régime supplétif en l'absence de directives expresses. Or, il existait déjà quelques mesures éparses d'opposition spécifiques au traitement de données de santé après le décès (A), qu'il convient de rappeler avant d'examiner les directives susceptibles d'être prises au titre du nouveau mécanisme législatif faisant perdurer les droits issus de la loi du 6 janvier 1978 (B). Plus profondément, organiser le traitement des données *post mortem* n'est pas sans implication sur le principe de la protection des données personnelles et l'idéologie qui la justifie (C).

A. Mesures préexistantes relatives aux données de santé *post-mortem*

De manière assez inattendue, dès avant la loi *pour une République numérique*, il existait en faveur des personnes physiques une protection résiduelle instituant une défense spécifique des données du mort. Le rapprochement des textes des codes civil, de la santé publique et de la loi de 1978 met en lumière des cas ponctuels dans lesquels une protection sur des données personnelles survit au décès de la personne protégée. Une illustration intéressante est offerte par le régime spécial du traitement des données de santé à des fins de recherche. De façon assez insoupçonnée, une protection des droits de la personne défunte se dégage en effet d'une exception à une exception posée à l'article 57 ancien de la loi de 1978 concernant les données de santé (1). Ainsi apparaissent les prémisses d'une préservation légale des données personnelles du mort, complétées par un second dispositif assurant le respect du cadavre et la préservation de la paix des morts (2).

1) Limitation du traitement à fins de recherche des données de santé *post-mortem*

À peine est-il besoin de souligner la spécificité des données de santé[41], composante de la vie privée de la personne[42], qui constituent des données sensibles au sens de l'article 6 de la loi du 6 janvier de 1978. Examiner leur sort *post-mortem* impose une analyse de leur régime juridique *ante-mortem*. En principe interdit, le traitement de données sensibles peut être admis dans le secteur de la santé avec un

41 - V. Règlement européen définissant les données personnelles à partir de l'identification (in)directe par « un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (art. 4, point 1), et plus précisément les « données concernant la santé » (art. 4, point 14), comme celles « relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

42 - CEDH, 27 août 1997, *M. S. c/ Suède*, n° 74/1996/693/885, § 41 relevant que « la protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention ».

encadrement strict[43]. De longue date, des formalités préalables sont prévues, lorsqu'est poursuivi un but d'intérêt général, la Commission nationale de l'informatique et des libertés pouvait autoriser le traitement des données de santé à des fins de recherche scientifique, d'étude ou d'évaluation[44], conformément à l'ancien chapitre IX de la loi Informatique et liberté, composé des articles 53 à 65[45]. Un rééquilibrage était opéré en permettant au patient de s'opposer à la levée du secret professionnel sur ses données, sans avoir à exposer de motifs[46], en vertu de l'article 57 al. 1 ancien de la loi du 6 janvier 1978 et en l'en informant avant le début du traitement de données. À la mort de la personne, la qualité de sujet de droit est perdue et la protection des données personnelles tombe. L'article 57 alinéa 2 ancien de la loi du 6 janvier 1978 affirmait d'ailleurs la licéité du traitement des « informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès ». Mais, l'assortissant d'une exception, il le tempère. Il innovait en ravivant les droits de la personne qui auraient dû s'éteindre à sa mort, puisqu'il est permis à « l'intéressé [de s'opposer au traitement de ses données personnelles à son décès lorsqu'il] a, de son vivant, exprimé son refus par écrit ». De manière originale, l'article 57 alinéa 2 ancien de la loi du 6 janvier 1978 se révélait donc le siège de la protection

43 - Renvoi par l'art. 6 II de la loi de 1978 aux exceptions prévues par le Règlement européen (art. 9). Voir spéc. points i, j, h autorisant les dérogations à des fins de médecine préventive ou du travail, au titre des services de soins et de protection sociale, pour des motifs d'intérêt public : de protection de la santé publique, des fins de recherche scientifique, historique, statistiques, archivistiques.

44 - CNIL, Délib. n°2015-173, 11 juin 2015, *Comm. com. électr.* 2015, comm. 73, obs. A. Debet refusant d'autoriser une recherche sur la fin de vie du fait de l'insuffisance d'information des personnes y participant.

45 - Dispositif protecteur refondu aux art. 64 à 71 de la loi de 1978 par l'ordonnance du 12 décembre 2018. Rappr. art. 74 de la loi de 1978 prévoyant un droit de s'opposer à la levée du secret professionnel en matière de santé. La loi de 1994 avait levé l'obstacle des règles relatives au secret professionnel en cas de transmission des données de santé détenues par les membres des professions de santé, afin d'éviter sa violation, ainsi que favoriser la recherche scientifique et faire cesser les transmissions de données en violation de la vie privée de la personne dont l'état de santé était divulgué. V. J. Frayssinet, Ph. Pedrot, La loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé, *JCP* 1994, doctr. 3810, spéc. n°13.

46 - Légalement prévu, le refus de la personne n'a pas à être motivé, laissant apparaître un droit discrétionnaire de la personne, qui déroge au droit général d'opposition au traitement de données (Art. 38 al. 1er de la loi de 1978), qui est conditionnel comme imposant d'exciper d'un motif légitime. V. M. Bénéjat, *Droits de la personnalité*, J.-C. Saint-Pau (Dir.), LexisNexis Traité 2013, p. 592, n° 962.

des données de santé du mort, dont il restaurait la protection. Les commentateurs de la loi du 1er juillet 1994 insérant ce dispositif novateur avaient noté « Après avoir soulevé le problème, le Parlement s'est bien gardé de trancher comment et auprès de qui le refus serait enregistré ; dans la pratique, le droit au refus risque bien de déboucher sur une clause de style dépourvue de toute application. Comme quoi, on peut apparaître soucieux de protéger l'individu en lui attribuant un droit de refus essentiellement virtuel »[47]. Cette exception est désormais reprise à l'article 86 de la loi de 1978 remaniée en 2018[48] au chapitre V consacré aux traitements de données des personnes décédées. Il en ressort que par une opposition écrite, la personne prend une mesure de protection efficace la réinvestissant de ses droits sur ses données et la prémunissant contre leur réutilisation posthume, quand bien même il s'agirait de poursuivre un but de recherche scientifique, d'étude ou d'évaluation dans le secteur de la santé. La loi ne protégeant ici que la personne prévoyant ses propres mesures anticipatrices, mieux vaudrait formuler opposition dans un testament conservé par un notaire ou parmi les directives *post-mortem* nouvellement mise en avant par la loi de 2016. En outre, une protection complémentaire des données de santé de la personne survit encore à son décès, grâce à la protection du corps mort qui s'étend aux empreintes génétiques du défunt.

2) Limitation des expertises génétiques *post-mortem*

Les caractéristiques génétiques d'une personne révèlent ses données personnelles de santé. Le règlement européen de 2016 le reconnaît explicitement en prenant soin de les définir tandis que la loi du 20 juin 2018 les intègre dans les données sensibles[49].

47 - J. Frayssinet, Ph. Pedrot, *op. cit.*, n° 20.

48 - Le nouvel article. 86 de la loi de 1978 pose que « Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit ».

49 - Art. 6, loi de 1978, transposant le Règlement de 2016, issu de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JO 21 juin 2018, texte n° 1, incluant dans la définition des données personnelles (art. 4, point 13) « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ».

L'examen des empreintes génétiques d'un individu n'est donc admis qu'à titre dérogatoire. Les articles 16-10 et 16-11 du code civil ne l'autorisent que dans des hypothèses limitativement énumérées : à des fins médicales ou de recherche scientifique, ainsi que pour établir l'identité inconnue d'un défunt, ou encore pour identifier une personne par ses empreintes génétiques dans le cadre de mesures d'enquête ou d'instruction diligentées lors d'une procédure judiciaire. De surcroît, ils exigent le consentement exprès de la personne à l'examen de ses caractéristiques génétiques, après information sur la nature et la finalité de celui-ci[50]. Le rapport 2018 de l'Agence de la biomédecine a proposé d'étendre ces hypothèses en suggérant que soient admis, sans consentement préalable de la personne, des examens génétiques sur une personne décédée à des fins diagnostiques, dont pourrait tirer bénéfice sa famille en prenant des mesures préventives si était décelée une maladie génétique[51].

Aujourd'hui, dans les procédures judiciaires, l'article 16-11 du code civil limite le recours aux expertises génétiques aux contentieux civils en contestation d'un lien de filiation ou à fins de subsides dirigées par un enfant à l'encontre de son père supposé. À cet égard, il faut souligner le pouvoir de la volonté de la personne sur les traitements affectant ses données de santé postérieurement à sa mort. Si celle-ci n'avait pas donné expressément son accord de son vivant, aucune expertise génétique ne pourra être réalisée *post-mortem* pour établir l'existence d'un lien de filiation biologique à son égard. Ce principe introduit en 2004 traduit les interrogations s'étant fait jour quand une expertise génétique d'un cadavre est demandée pour établir un lien de filiation. Le juge ne pourra passer outre le refus ou le silence de la personne, dont la parenté est discutée en justice, comme il l'avait fait précédemment en ordonnant l'exhumation du corps d'Yves Montand, pour faire pratiquer une

50 - Art. 75, loi de 1978 exigeant un consentement à une recherche nécessitant un examen génétique.

51 - Agence de la biomédecine, *Rapport sur l'application de la loi de bioéthique*, janv. 2018, p. 46 <https://www.agence-biomedecine.fr/IMG/pdf/rapport_complet_lbe_2017_vde_f_12-01-2018.pdf>. Il est précisé que ces examens pourraient être autorisés dans le cadre d'une autopsie, pour la compréhension des causes du décès, ou ultérieurement, si un prélèvement de la personne décédée est conservé en banque.

analyse génétique, à laquelle l'artiste s'était opposé sa vie durant[52]. Il ne faut pas se méprendre sur la portée de la protection de la vie privée, conçue pour contrer les ingérences extérieures atteignant la sphère intime. Il a été souligné que ce principe ne saurait conférer au droit de rapporter librement la preuve de sa filiation une portée telle qu'il prévaudrait sur le choix du législateur d'assurer le respect dû aux morts en s'opposant aux exhumations[53]. En ce sens, le Conseil constitutionnel a considéré que l'article 16-11 du code civil est conforme à la constitution et ne porte pas atteinte au respect de la vie privée en ce sens que les personnes décédées sont présumées ne pas avoir consenti à une identification par empreintes génétiques et que le respect dû au corps humain mis en avant par le législateur doit être pris en compte, sans que le Conseil constitutionnel ne lui substitue sa propre appréciation[54]. Pour autant, le juge judiciaire pourrait avoir à prendre en compte la protection étendue du droit au respect de la vie privée émanant de la Cour européenne des droits de l'homme qui y intègre « le droit à l'identité dont relève le droit de connaître son ascendance »[55] et qui souligne « l'intérêt vital, défendu par la Convention, à obtenir les informations qui leur sont

52 - L'expertise avait exclu sa paternité à l'égard de la requérante avec une très forte probabilité. Paris, 6 nov. 1997, D. 1998. 122, note Ph. Malaurie ; *RTDciv.* 1998, p. 87, obs. J. Hauser ; *JCP G* 1998, I. 101, n° 3, obs. J. Rubellin-Devichi ; *Defrénois* 1998, art. 36753, n° 8, p. 314, obs. J. Massip ; *Gaz. Pal.* 1997, 2, p. 703, note Th. Garé. *Adde* P. Catala, La jeune fille et le mort, *Dr. famille* 1997, étude 12 ; J.-R. Binet, « La loi relative à la bioéthique – Commentaire de la loi du 6 août 2004 : 1re partie », *Dr. famille* 2004, étude 22, spéc. n°19-25 ; M. Mignot, « L'accès à la preuve scientifique dans le droit de la filiation », *RRJ* 2003-2, p. 667-700, spéc. p. 684 ; F. Bellivier, L. Brunet, C. Labrusse-Riou, « La filiation, la génétique et le juge : où est passée la loi ? », *RTDciv.* 1999, p. 529.

53 - J.-F. de Montgolfier, « La QPC et le droit de la famille au Conseil constitutionnel », *AJ Famille* 2012, p. 578 relevant du juge de conférer une portée extensive au droit au respect de la vie privée comme au droit de mener une vie familiale ; F. Chénedé, P. Deumier, « L'œuvre du Parlement, la part du Conseil constitutionnel en droit des personnes et de la famille », *Les nouveaux Cahiers du Conseil constitutionnel* 1er avr. 2013, n°39, p. 7, spéc. IV.

54 - Cons. const., déc. n° 2011-173 QPC du 30 sept. 2011, *RTDciv.* 2011, p. 745, obs. J. Hauser ; note J. Buisson, « Expertises génétiques post mortem : le Conseil constitutionnel refuse de donner le coup de grâce à l'article16-11, alinéa 2, du Code civil », *Dr. famille,* nov. 2011, n° 11, p. 3.

55 - CEDH, 13 juil. 2006, *Jäggi c/ Suisse*, n° 58757/00, § 25 statuant sur la requête arguant d'une atteinte à la vie privée pour ne pas avoir pu diligenter une analyse ADN sur un défunt pour établir s'il était son père biologique ; CEDH, 16 juin 2011, *Pascaud c/ France*, n° 19535/08, § 48. Rappr. moins nets CEDH, gde ch.,13 févr. 2003, *Odièvre c/ France,* no 42326/98, § 29 notant que « l'article 8 protège un droit à l'identité et à l'épanouissement personnel » ; CEDH, 7 févr. 2002, *Mikulić c/ Croatie*, n° 53176/99, § 53 jugeant « la vie privée inclut l'intégrité physique et psychologique d'une personne et englobe quelquefois des aspects de l'identité physique et sociale d'un individu ».

indispensables pour découvrir la vérité sur un aspect important de leur identité personnelle »[56], « dont l'identité des géniteurs fait partie »[57]. La Cour européenne a cependant considéré qu'il convenait de mettre en balance le droit des « personnes essayant d'établir leur ascendance [qui] ont un intérêt vital à obtenir les informations qui leur sont indispensables pour découvrir la vérité » avec « le droit des tiers à l'intangibilité du corps du défunt, le droit au respect des morts ainsi que l'intérêt public à la protection de la sécurité juridique » dans une affaire où était discutée une mesure d'expertise génétique *post mortem*[58]. Elle estimait néanmoins le prélèvement d'ADN comme une « ingérence relativement peu intrusive » et considérait que le « droit de reposer en paix ne bénéficie donc que d'une protection temporaire », du fait de l'expiration de la concession funéraire en l'espèce[59]. La Cour de cassation n'a pas eu encore à trancher sur le fond. Toutefois, d'un point de vue procédural, elle a décidé, en 2014, que « la recevabilité d'une action tendant à la reconnaissance d'une ascendance génétique par voie d'expertise, lorsque celle-ci nécessite une exhumation, est subordonnée à la mise en cause des ayants droit du défunt »[60]. Il conviendrait donc de les assigner dans la cause, sans toutefois que leur consentement au prélèvement ne soit requis. On peut y déceler l'incursion des méthodes du juge de Strasbourg qui dépasse les textes normatifs pour raisonner en

56 - CEDH, *Mikuli*, préc., « § 64. Selon la Cour, les personnes qui se trouvent dans la situation de la requérante ont un intérêt vital, défendu par la Convention, à obtenir les informations qui leur sont indispensables pour découvrir la vérité sur un aspect important de leur identité personnelle. [Nuançant ensuite, car] D'un autre côté, il faut garder à l'esprit que la nécessité de protéger les tiers peut exclure la possibilité de les contraindre à se soumettre à quelque analyse médicale que ce soit, notamment à des tests ADN ».

57 - CEDH, *Jäggi*, *préc.*, § 25.

58 - *Ibid.*, § 38-9.

59 - *Ibid.*, § 41. V. CEDH, 15 mai 2006, *Succession Kresten Filtenborg Mortensen c/ Danemark*, n°1338/03, p. 11-2 décision d'irrecevabilité distinguant les saisines de la succession au nom d'un défunt et les affaires antérieures sur la vie privée, concluant qu'elle n'était pas atteinte du fait du prélèvement post-mortem ordonné pour établir une filiation.

60 - Sur le pourvoi formé contre un arrêt rejetant une requête en exhumation aux fins d'expertise, cass. 1ère civ., 13 nov. 2014, n° 13-21.018 ; Bull. n° 188 ; *Dr. famille* 2015, comm. 9, obs. C. Neirinck ; *D.* 2015. 649, obs. M. Douchy-Oudot ; *D.* 2015. 702, obs. F. Granet-Lambrechts ; *D.* 2015. 755, obs. H. Gaumont-Prat ; *AJ fam.* 2015. 54, obs. F. Chénedé ; *RTDciv.* 2015. 103, obs. J. Hauser ; *RJPF* 1/20, obs. T. Garé. V. S. Canas, « L'influence de la fondamentalisation du droit au respect de la vie privée sur la mise en œuvre de l'article 9 du code civil », *Nouveaux Cahiers du Conseil constitutionnel*, 1er juin 2015, n° 48, p. 47, spéc. IB.

termes de proportionnalité des atteintes à un principe. Il pourrait en résulter en droit interne la consécration prétorienne d'une sorte d'action *sui generis* en connaissance des origines ou du droit à la reconnaissance de son ascendance génétique[61]. En ce sens s'ouvrirait une action posthume en justice en arguant de l'intérêt vital à établir un lien d'ascendance avec le mort, en assignant ses héritiers. Ces derniers pourraient contester l'intérêt uniquement patrimonial du demandeur, qui ne sera pas forcément aisé à établir vu l'importance reconnue récemment à la quête identitaire ; ce moyen empêcherait en effet de retenir une ingérence dans l'exercice du droit au respect de sa vie privée et familiale garanti à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales[62]. À l'avenir, il n'est donc pas certain que l'expertise *post-mortem* soit totalement exclue en France[63]. Notons qu'elle est admise en Espagne. L'exhumation du corps du peintre Salvador Dali a pu être obtenue en justice, en juin 2017, par une personne se revendiquant sa fille[64]. En France, il devrait s'imposer de recueillir le consentement exprès de la personne *ante-mortem* pour être autorisé après son décès à pratiquer une mesure d'expertise génétique au soutien d'une action alimentaire en justice à fins de subsides ou en établissement de filiation. En matière de santé, il existe donc en faveur de la protection de la personne plusieurs moyens de faire survivre les effets du refus

61 - F. Chénedé, *op. cit.* ; M. Douchy-Oudot, *op. cit.* ; H. Fulchiron, « Les actions du préteur : la Cour de cassation, l'article 8 de la Convention EDH et le droit à la reconnaissance de son ascendance génétique », *D.* 2015. 1070, II.

62 - Cass. 1ère civ., 6 juil. 2016, n° 15-19853 ; obs. M. Bruggeman, « L'article 333 du Code civil et la protection du droit au respect de la vie privée des héritiers : vers de nouveaux arbitrages ? », *Gaz. Pal.* 18 avr. 2017, n° 15, p. 70 retenant que la cour d'appel a relevé que les « descendants ne soutenaient pas avoir subi, personnellement, une atteinte à leur vie privée du fait de l'impossibilité d'établir, au travers de celle de leur père, leur ascendance (...) elle en a déduit que l'action engagée par les consorts X ne poursuivait qu'un intérêt patrimonial (...) elle a pu décider que l'article 333 du code civil [prescription quinquennale pour l'action en contestation de paternité] ne portait pas au droit au respect de leur vie privée une atteinte excessive au regard du but légitime poursuivi, justifiant que ces règles fussent écartées et que l'action fût déclarée recevable ».

63 - C. Neirinck, obs. sous cass. 1ère civ., 13 nov. 2014, *préc.* soulignait que « La découverte de l'ADN a mis fin au repos éternel. Pour ceux qui souhaitent reposer en paix, il ne reste que l'incinération ».

64 - Tribunal de Madrid, 13 oct. 2017, les tests de comparaison de leurs ADN n'ayant pas été concluants, elle fût condamnée à payer les importants frais de procédure, V. « Demande en paternité de Dali : la plaignante condamnée à rembourser les frais, 16 oct. 2017 », <http://www.europe1.fr/international /demande-en-paternite-de-dali-la-plaignante-condamnee-a-rembourser-les-frais-3466142>.

de traitement et d'utilisation de ses données personnelles au-delà de son décès.

B.Mesures conventionnelles de protection des données personnelles *post-mortem*

L'innovation phare du nouveau dispositif légal est de permettre de prendre des directives destinées à la « conservation, à l'effacement et à la communication de ses données à caractère personnel » applicables postérieurement au décès de la personne selon le nouvel article 85 I de la loi du 6 janvier 1978. Elles « définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés » au chapitre II précisant les droits de la personne concernée. Il s'en déduit une prorogation des droits de la personne concernée par le traitement de données, dont la mise en œuvre sera désormais admise *post-mortem*. L'attention doit se porter sur deux points, la dualité de directives prévues par la loi (1) et leur nature, qui n'y est pas précisée (2).

1) Coexistence entre directives générales et particulières

L'exercice *post-mortem* de droits sur les données personnelles du défunt, déjà envisagé dans le passé, reçoit consécration légale au nouvel article 85 I de la loi du 6 janvier 1978. Le pouvoir de la volonté est privilégié en laissant à chaque personne une grande liberté pour organiser ses modalités de mise en œuvre. Pourront être adoptées, soit des directives particulières notifiées à chaque responsable de traitement concerné, soit des directives générales à enregistrer auprès d'un tiers de confiance certifié. En rédigeant ses directives, la personne peut choisir de donner mission à une autre d'en assurer l'exécution. Sorte de curateur aux données numériques[65], celui qui est investi de cette qualité pourra, au décès de la personne concernée, solliciter communication des directives qu'elle avait formulées (Loi de 1978, art. 85 I al. 8). La loi complète cette faculté d'accès en octroyant à la personne désignée par le défunt le pouvoir de solliciter après sa mort directement auprès des responsables de traitement des données de la personne protégée l'application des

65 - C. Béguin-Faynel, « Pour un testament des dernières volontés numériques « (...), *op. cit.*, p. 81.

mesures contenues dans ses directives (Art. 85 I al. 8). Afin de laisser toute latitude à la personne organisant des directives relativement au sort de ses données après sa mort, elle peut toujours les modifier de son vivant ou purement et simplement les révoquer (Art. 85 I al. 7). Présentons les mesures, puis leur mise en œuvre.

Bien que la loi distingue directives générales et particulières, elle leur confère la même fonction, à savoir définir « la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés » au chapitre II du titre II de la loi de 1978 (Art. 85 I al. 5). Ainsi survivront le droit d'opposition au traitement des données personnelles et les droits d'accès et de rectification, régis par les articles 49, 50, 51, 56 et 105, 106 et 110 de la loi Informatique et liberté.

Sont considérées comme particulières, par le nouvel article 85 I al. 4 de la loi de 1978, les mesures relatives à l'exercice des prérogatives sur les données personnelles directement enregistrées auprès de chaque responsable de traitement[66]. On songe tout spécialement aux opérateurs de télécommunications, de commerce électronique et aux fournisseurs de services de réseaux sociaux numériques et de messagerie électronique ou instantanée. La loi est muette sur le contenu des mesures susceptibles d'être retenues, laissant à la personne liberté d'exprimer ses dernières volontés numériques. À l'évidence, les directives dites particulières pourront investir une ou plusieurs personnes déterminées pour agir auprès du responsable de traitement auxquelles elles auront été exprimées. Tous les droits légaux sur les données personnelles sus-évoqués ne seront pas obligatoirement conférés. La personne concernée peut indiquer au responsable de traitement quels droits elle entend confier à telle personne. Les droits d'accès et de rectification pourront être transmis de manière plus ou moins large en donnant pouvoir de sauvegarder l'intégrité du compte, voire d'en récupérer le contenu (texte, illustrations, photographies, vidéos...), ou de permettre de le modifier. Enfin, le droit d'opposition pourra se concrétiser en mission de clôturer le compte.

66 - La transmission de directives particulières a pu s'appliquer sans attendre de décret d'application.

Sont générales les directives organisant dans un même document le sort à réserver aux données traitées par différents opérateurs, suivant l'article 85 I al. 2 et 3 de la loi de 1978. Étonnamment, la loi dit qu'elles « peuvent être enregistrées » auprès d'un tiers de confiance certifié par la Commission nationale de l'informatique et des libertés. Mais, est-ce une simple faculté d'enregistrement ? Ensuite, le texte semble tenir pour obligatoire que les « références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées so[ie]nt inscrites dans un registre unique » (Art. 85 I al. 2 et 3). Les dispositions décrétales tardant à être prises[67], il n'y a pas encore de système de certification et d'enregistrement sur un registre unique opérationnel. Toutefois, l'acte contenant les directives générales, bien que ne pouvant être enregistré, pourrait valoir comme testament olographe comme cela était préconisé avant la loi[68] ; à le supposer écrit en entier la main de la personne défunte, daté et signé, comme l'exige l'article 970 du code civil, ses dispositions (extra)patrimoniales trouveraient application[69].

Dans l'attente du décret, l'incertitude plane sur l'identification du « tiers de confiance numérique » prévu par la loi. On peut supposer qu'il s'agit de la mise en œuvre de la proposition du Conseil d'État tendant à faire garantir que seules les données dont la personne a autorisé la divulgation sont diffusées par des prestataires « tiers de confiance »[70]. La fonction d'enregistrement des directives est mise en avant et non celle d'expression de la volonté de la personne, caractérisant la « personne de confiance » chargée de rendre compte de la volonté de la personne pour les démarches et décisions médicales ou le « tiers

67 - Un décret d'application de la loi *pour une République numérique*, pris en Conseil d'État, après avis motivé et publié de la Commission nationale de l'informatique et des libertés est toujours attendu ; Rép. Min. n°25622, JO Sénat Q, 30 mars 2017, p. 1245 question écrite restée sans réponse demandant quel était l'état de préparation du décret.

68 - A. Mâzouz, « Être ou ne plus être, les volontés à l'origine de la mort numérique », *op. cit.*, p. 183 ; C. Béguin-Faynel, « Pour un testament (…) », *op. cit.*, p. 67 ; CNIL, *34ème Rapport annuel* 2013, publié en sept. 2014, p. 73-4.

69 - *A minima*, la protection des données du mort pourrait être assurée si la personne retranscrit les informations et identifiants nécessaires à l'administration *post-mortem* de ses données dans un document écrit ou dans un stockage dématérialisé, *cloud*, afin d'organiser l'accès direct des proches à ses comptes. V. C. Zorn, « Contrats de *Cloud computing* et données personnelles : éléments de rénovation des techniques contractuelles », *D. IP/IT* 2016, p. 453.

70 - Conseil d'État, *Étude annuelle 2014 - Le numérique et les droits fondamentaux*, *op. cit.*, proposition n° 4.

de confiance » fiscal[71]. La comparaison avec ces institutions semble toutefois fortement à nuancer, le rapprochement avec les services de confiance de l'économie numérique semblant plus cohérent[72]. Le notaire remplit les conditions prévues par ce règlement et semble un interlocuteur parfait non seulement pour l'enregistrement des directives générales, mais aussi pour aider à leur rédaction[73].

Pour tirer profit du nouveau dispositif, la personne concernée devrait anticiper les conséquences de son décès en vérifiant, par un audit simple, auprès de chacun des responsables de traitement les règles prévues à cette date. Au fur et à mesure des consultations des différents comptes et de leur paramétrage, elle évaluerait les mesures envisageables et les configurerait directement, par des directives particulières, ou adopterait des directives générales pour administrer l'ensemble des données personnelles. Rançon de la liberté laissée au défunt, sans indication de sa part, il n'existe aucun moyen d'identifier quels sont les responsables de traitement à joindre. Dresser un inventaire des mesures directement prises auprès des responsables de traitement et des références pour contacter les opérateurs concernés est une mesure indispensable pour les porter à la connaissance des proches, qui pourront vérifier qu'elles sont respectées. On regrette qu'une centralisation de l'information ne soit pas prévue dans le registre imaginé par le nouveau texte, sur le modèle éprouvé du fichier central des dispositions de dernières volontés[74]. Beaucoup de points restent donc à éclaircir, il en va de même de la nature juridique des directives.

---

71 - CSP, art. L. 1111-6 évoquant la mission d'un parent, un proche ou du médecin traitant ; CGI, art. 170 ter réservant la mission de tiers de confiance aux avocats, notaires et experts-comptables. V. A. Favreau, « Loi n° 2016-1321 du 7 octobre 2016, pour une République numérique : un cadre légal pour le devenir des données à caractère personnel des personnes décédées », *Revue droit et santé*, Les Etudes hospitalières, 2016, p.839, spéc. p. 847-8.

72 - Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juil. 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*, JOUE L 257/73, 28 août 2014, p. 1, art. 1 visant en particulier les transactions électroniques.

73 - *#Familles, #solidarité, #numérique*, 113e Congrès des notaires de France, 2017, p. 892.

74 - Le notariat l'avait proposé in Contribution du Conseil supérieur du notariat, observations sur la mort numérique (art. 20), 15 oct. 2015, <https://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/contribution-du-conseil-superieur-du-notariat-observations-sur-la-mort-numerique-art-20>.

2) Nature contractuelle des directives du défunt

Le législateur prévoit que les « directives » écrites d'une personne chargent un tiers d'exercer des droits pour le compte d'autrui. Bien que la loi conserve silence sur la nature des droits créés, le dispositif renvoie à la technique du mandat, que l'on retrouve notamment dans la sphère familiale et en droit des personnes[75]. Le mandat ou la procuration confèrent en effet à autrui « le pouvoir de faire quelque chose pour le mandant et en son nom » ; si le code civil ajoute qu'il cesse en principe lorsque décède le mandant, il permet toutefois qu'il perdure jusqu'à la fin de la mission[76]. De longue date, la jurisprudence admet des tempéraments conventionnels, en validant des mandats *post-mortem* stipulés pour s'exécuter après la mort du défunt[77] ; elle effectue néanmoins un contrôle, en exigeant que la mission ne contrevienne pas à l'ordre public successoral[78]. Le mandat s'exerçant de manière posthume est donc licite s'il ne vient pas contrarier la règlementation des droits successoraux des héritiers[79]. La personne dont les données sont l'objet d'un traitement missionne le mandataire qu'elle choisit, par des directives générales ou particulières, pour veiller au respect des droits garantis par la loi de 1978. Il s'agit d'un « mandat légal »[80] organisé par son article 85 I afin de mettre en œuvre les droits d'accès, d'opposition et de rectification sur les données du défunt, dont les modalités et le contenu sont prévus par le mandant lui-même.

75 - N. Peterka, « Le pouvoir, prérogative privilégiée d'administration du bien d'autrui (mandat, représentation, pouvoir) », *Dr. & patr.* mensuel 2005, n° 252, p. 36, spéc. IB ; P. Malaurie, « Le mandat en droit des personnes », *in Le mandat, un contrat en crise ?*, N. Dissaux (Dir.), Economica coll. Études juridiques, 2011, p. 115.

76 - C. civ., art. 1984, 1991, 2003, 2008, 2009.

77 - Cass. req., 22 mai 1860, S. 1860, p. 724 ; G. Wicker, « Successions – mandats successoraux – le mandat à effet posthume », JCl. Civil Code, Art. 812 à 812-7, fasc. unique, 2014, spéc. n° 133-8 ; M. Mekki, « Mandat – extinction du mandat », JCl. Civil Code, Art. 2003 à 2010, fasc. unique, 2012, spéc. n° 30 ; N. Laurent-Bonne, « Aux origines du mandat à effet posthume », *RDC* 2013, p. 827, spéc. II.

78 - Cass. 1ère civ., 28 juin 1988, n° 86-13639 ; Bull. n° 209 ; *RTDciv.* 1989, p. 116, note J. Patarin.

79 - La validité du mandat *post-mortem* n'a pas été remise en cause par la création du mandat à effet posthume par la loi n° 2006-728 du 23 juin 2006. Plus restrictif, ce mandat doit être authentique et protéger un intérêt légitime. Temporaire, il édicte, pour un à cinq ans, un mandat forcé sans représentation en faveur des héritiers avec mission d'administrer ou liquider tout ou partie de sa succession à son ouverture. V. G. Wicker, *op. cit.*, n° 133 et 137.

80 - Rappr. *mutatis mutandis* du mandat légal d'agir entre époux prévu pour les dettes ménagères (C. civ., art. 220).

Une autre série d'indices tenant au vocabulaire employé dans la loi porte à rattacher les directives particulières à la qualification de contrat et à une modification contractuelle. Tout d'abord, le nouvel article 85 I al. 4 de la loi de 1978 exige qu'elles soient l'œuvre du défunt, qui doit avoir explicitement manifesté sa volonté. Il impose le « consentement spécifique de la personne concernée » et exclut explicitement que celui-ci puisse « résulter de la seule approbation par cette dernière des conditions générales d'utilisation ». Ce faisant, il renvoie à la définition du contrat comme accord de volonté, et aux conditions générales, qui en précisent les modalités de mise en œuvre, au sens des articles 1101 et 1119 du code civil. Or, on sait qu'elles sont rédigées unilatéralement par l'opérateur numérique et parfois à son avantage exclusif, manifestant un déséquilibre significatif sanctionné en réputant les clauses abusives non écrites[81]. La personne concernée, utilisatrice du service, devra donc exprimer un choix spécifique expressément formulé, sans que l'opérateur numérique ne puisse se substituer à elle par des dispositions noyées dans les conditions générales. Les clauses transférant à des tiers – conjoint, héritiers – des droits sur les données personnelles du défunt seraient néanmoins valables si le titulaire du compte y consentait spécifiquement. L'approbation viendrait du renseignement du nom de la personne, des modalités d'exercice de ses droits, en cochant des cases ou en remplissant des espaces laissés libres, suivant les préceptes de la protection des données dès la conception de l'architecture numérique, *data protection by design*[82]. Enfin, la qualification de mandat *post-mortem*[83] semble préférable pour les directives, plutôt que les relier à une transmission successorale légale ou testamentaire, reposant sur une analyse patrimoniale des données, cadrant mal avec l'approche personnaliste de la loi de 1978[84]. Le dispositif légal voté en 2016 ranime le débat sur la nature de la protection des données.

81 - Comm. cl. abusives, recomm. n° 2014-02, 7 nov. 2014, relative aux contrats proposés par les fournisseurs de réseaux sociaux formulant 46 propositions de suppression de certaines clauses relatives aux contrats proposés par les fournisseurs de services de réseaux sociaux. V. A. Debet, *RDC* 2015, p. 496.

82 - Règlement général sur la protection des données, *préc.*, art. 24 et 25.

83 - A. Favreau, « Mort numérique : précisions (...) », *op. cit.*, p. 36 ; *Id.*, « L'accès des proches (...) », *op. cit.*, p. 74-6.

84 - C. Pérès, « Les données à caractère personnel et la mort : observations relatives au projet de loi pour une République numérique », *D.* 2016. 90, spéc. n°11 et s..

C. Rénovation de l'analyse du droit sur les données après la mort

La durée de la protection légale des données personnelles est alignée sur celle de la personnalité juridique, attribuée aux personnes physiques leur vie durant. Conférer à chaque personne faculté de missionner un tiers pour protéger les données qui lui « survivent » n'est envisageable qu'en respectant l'ordre public, qui imprègne le nouveau texte et que le renforcement des obligations d'information tend à assurer (1). Le sort des données personnelles du défunt impose de réfléchir aux fondements mêmes de la protection des données. Le débat s'est segmenté autour de deux analyses, l'une centrée sur la personne, l'autre plus patrimoniale (2).

1) Réaffirmation du droit d'opposition et du droit à l'information

Le nouveau texte figurant à l'article 85 I de la loi du 6 janvier 1978 implique l'ordre public à un triple égard. Tout d'abord, il rappelle, dans son alinéa 5, que les directives prises par le défunt ne peuvent se heurter aux principes régissant les archives publiques comportant des données personnelles[85]. La volonté de la personne rencontre une limite, elle ne peut raisonnablement après son décès faire effacer des données à caractère personnel devant être conservées à des fins archivistiques ou historiques[86]. Ensuite, la personne qui rédige ses directives *post-mortem* doit respecter les droits des tiers sur leurs propres données, tels que prévus par la loi Informatique et liberté. Elle ne peut donc prévoir la communication de ses données que dans le respect des règles légales de communication de celles des tiers (Loi de 1978, art. 85 I al. 6), conformément à l'interprétation précédente des dispositifs protecteurs des données personnelles prônant l'articulation des droits individuels[87]. Enfin, la conformité à l'ordre public se manifeste encore en contraignant les responsables de traitement de données personnelles à respecter les

85 - Il s'en infère une restriction à l'exercice du droit d'opposition et de rectification, même si cette précision qui figurait à l'article 40 ancien de la loi de 1978 n'a pas été reprise à l'article 110 visant les restrictions légales.

86 - N. Mallet-Poujol, « Le droit à l'effacement des données personnelles », *in* S. Chatry, Th. Gobert (dir.), *Numérique – Nouveaux droits, nouveaux usages*, Éd. Mare & Martin, 2017, p. 83, spéc. p. 94-6.

87 - Groupe de travail « article 29 », *Avis 4/2007 sur le concept de données à caractère personnel*, p. 25.

prérogatives légales édictées à l'article 85 I de la loi de 1978, qui sont impératives suivant son alinéa 9. Elles sont impératives, puisqu'il est expressément retenu qu'un responsable de traitement ne pourrait valablement s'exonérer de l'application des directives de la personne par une clause contractuelle des conditions générales d'utilisation de ses services ; une clause restreignant la faculté pour la personne d'adopter des directives *post-mortem* serait réputée non écrite.

Pour assurer l'effectivité des nouveaux droits qu'elle introduit, la loi *pour une République numérique* a renforcé les obligations d'information des responsables de traitement. « 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 »[88]. L'article 32 de la loi de 1978, renuméroté 48, contenant les obligations générales d'information incombant au responsable de traitement[89], fut complété en ce sens. Tout responsable de traitement est dorénavant débiteur d'une nouvelle obligation d'information en faveur de la personne dont il collecte les données sur la possibilité d'organiser les conséquences de son décès sur les données recueillies. Il doit, en outre, prévenir la personne des droits qu'elle tient de la loi pour définir des directives relatives au sort de ses données à caractère personnel après sa mort. En pratique, ces informations devront être portées à la connaissance de l'ensemble des personnes concernées et faire notamment l'objet d'une mention sur tout

88 - Art. 85 III, loi de 1978. En ce sens, Étude d'impact, *op. cit.*, p. 112. On saluera la clarification terminologique issue de la consultation publique de 2015 permettant d'abandonner la terminologie de « prestataire de stockage de signaux », l'atelier Données personnelles de l'Association pour le Développement de l'Informatique Juridique ayant proposé le renvoi aux définitions légales des hébergeurs et acteurs d'Internet (Loi pour la confiance dans l'économie numérique, art. 6-I-2), <https://www.republique-numerique.fr/consultations/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees>.

89 - Le texte renvoie aux art. 12 à 14 du Règlement. Le responsable de traitement doit informer, art. 104 de la loi de 1978, les personnes auprès desquelles il recueille des données à caractère personnel les concernant de son identité, le cas échéant les coordonnées du délégué à la protection des données, de la finalité poursuivie, du droit d'introduire une réclamation auprès de la CNIL et leur exposer leurs droits à l'égard des traitements de données à caractère personnel (accès, rectification, effacement, droit de demander une limitation du traitement). Il doit encore lui fournir la base juridique du traitement, la durée de conservation des données, les catégories de destinataires des données et au besoin des informations complémentaires notamment en cas de collecte à l'insu de la personne.

formulaire de collecte de données personnelles[90]. Les responsables de traitement doivent créer une procédure permettant de recueillir les directives particulières des personnes, qu'ils devront mettre en œuvre en communiquant les données du défunt à la personne que celui-ci aura désignée, le cas échéant[91]. Par suite, la rédaction de directives particulières pour organiser le sort de ses données après son décès devrait s'en trouver encouragée et être plus accessible que l'élaboration de directives générales à concevoir seul.

2) Consécration de l'analyse personnaliste et relativisation de l'analyse patrimoniale

On connaît la controverse doctrinale sur la nature juridique des droits sur les données personnelles : se rapprochent-ils des droits de la personne ou du droit de la propriété[92] ? Rappelons les termes du débat dans lequel s'intègre la question de la protection des données *post-mortem*. En 2014, le Conseil d'État proposait de définir le droit des données personnelles comme un droit à l'autodétermination informationnelle « tendant à garantir en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel »[93]. Le Conseil rattachait le droit des données personnelles à la personne elle-même, estimant qu'il ne devait « pas entrer dans le champ du droit de propriété patrimonial de la personne »[94]. La loi *pour une République numérique* conféra l'onction légale à cette analyse personnaliste en renforçant les droits de la personne sur l'usage de ses données. Son contrôle sur les données collectées a été réaffirmé et son pouvoir de décider

90 - M. Bourgeois, A. Bounedjoum, « Les impacts de la loi pour une République numérique sur la loi Informatique et libertés », *JCP E* 2016, 1683, spéc. n°12-3.

91 - Étude d'impact, *op. cit.*, p. 112.

92 - J. Rochfeld, « Contre l'hypothèse de la qualification des données personnelles comme des biens », *in Les biens numériques*, E. Netter, A. Chaigneau (Dir.), Colloques Ceprisca éd., 2015, p. 221 ; V.-L. Benabou, J. Rochfeld, *À qui profite le clic ?*, éd. Odile Jacob, Corpus, 2015, p. 59-68 sur la position du problème, p. 69-103 sur les modèles alternatifs. Réorientation du débat vers la protection des données par les communs, V. A. Anciaux, J. Farchy, « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue int. dr. économique* 2015/3, t. XXIX, p. 307, spéc. p. 329-30 ; *Dictionnaire des biens communs*, M. Cornu, F. Orsi, J. Rochfeld (Dir.), PUF Quadrige, 2017.

93 - Conseil d'État, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 264-269 et proposition n°1.

94 - Rappr. A. Anciaux, J. Farchy, C. Méadel,

fut proclamé à l'article 1, alinéa 2 de la loi du 6 janvier 1978. Il en a été déduit le renforcement légal des droits de la personne dans une logique « *d'empowerment* »[95] ou « *d'empouvoirement* »[96] de l'internaute. Dans le contexte de renouveau insufflé par le règlement général sur la protection des données[97], les thèses fondées sur une analyse patrimoniale du droit des données personnelles furent défendues à nouveau[98]. Mais la mise en œuvre d'une « propriété sur les données » semble délicate[99]. Le Conseil national du numérique la repousse, car elle repose sur la négation du rapport de force existant avec les entreprises, alors même qu'elle ne pourrait générer que des revenus très faibles aux personnes et déboucherait sur un renforcement des inégalités entre citoyens quant à leur capacité de gérer, protéger et monétiser leurs données, fonctions qui seraient alors exercées par le marché[100].

On peut s'interroger sur le rattachement des articles 84 et 85 I de la loi de 1978 à une conception personnaliste ou patrimoniale de la protection des données. Ils se rattachent plutôt à une analyse personnaliste en

95 - L. Cluzel-Métayer, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA* 2017, p. 340, spéc. IIA) ; B. Thieulin, « Gouverner à l'heure de la révolution des pouvoirs », *Pouvoirs* 2018/1, n° 164, p. 19, spéc. p. 19-20 et p. 28.

96 - C. Berthet, C. Zolynski, « "L'empouvoirement" des citoyens de la République numérique (...) », *op. cit.*, n° 9-10.

97 - Sur l'autodétermination informationnelle *in* Règlement général sur la protection des données du 27 avr. 2016, *préc.*, v. considérants 7, 11 et 68 ainsi que les articles 7, 8, 12, 13, 14, 17, 18, 19 et 20.

98 - L. Castex, « Les éternités numériques un essai d'analyse prospective », *RLDI* 2016/11, p. 49, spéc. II ; I. Landreau, G. Peliks, N. Binctin, V. Pez-Pérard, *Mes data sont à moi. Pour une patrimonialité des données* personnelles, *Rapport* du Collectif génération libre, L. Léger (Dir.), janv. 2018, <https://www.generationlibre.eu/data-a-moi/>, spéc. p. 116-20 proposant la mise à disposition des données par des *smartcontracts* usant de signatures électroniques et *blockchain*.

99 - F. Mattatia, M. Yaïche, « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », *RLDI* 2015/6, p. 41, spéc. II ; A. Anciaux, J. Farchy, C. Méadel,

100 - Conseil national du numérique, *La neutralité des plateformes*, Rapport 2014, p. 37 ; *Avis relatif au projet de loi pour une République numérique*, 30 nov. 2015, p. 7 ; *Avis sur la libre circulation des données en Europe*, 28 avr. 2017, p. 4 retenant que la patrimonialisation des données pourrait n'apporter aucun bénéfice pour les personnes et plutôt « conduire à l'inscription de clauses de cession obligatoire dans les contrats entre opérateurs et, par voie de conséquence, à un plus grand risque de dépossession ». Comp. estimant que les données devraient être confiées à un nuage de dépositaires, des « dataires » notaires des données, et non à l'État, Google ou Facebook, B. Ferran, L. Ronfaut, M. Serres, « La question est de savoir qui sera le dépositaire de nos données », *op. cit.*.

prévoyant le maintien provisoire de l'exercice des droits d'accès, d'opposition et de rectification sur les données personnelles après le décès[101]. En effet, on pourrait voir une prorogation dans le temps du droit à l'autodétermination informationnelle dans le pouvoir d'organiser par des directives l'exercice *post-mortem* des droits sur des données. Ces droits n'appartiennent toutefois pas directement à la personne désignée, qui exerce le mandat de contrôler le sort dévolu aux données personnelles du mandant, qui peut librement le révoquer de son vivant.

Quant au II de l'article 85 de la loi de 1978, il n'appartient pas à un modèle pur. Il a été marqué par les deux tendances personnelle et patrimoniale, qui se sont manifestées durant les travaux parlementaires[102], dont il convient de rappeler les influences. Le texte voté fait usage d'un champ lexical empreint du droit successoral : il est renvoyé aux « héritiers », qui pourront « recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ». Organise-t-il ce faisant une succession anomale, justifiée par la nature originale des biens transmis[103] ? Ce mécanisme serait « le plus simple », « mais il cadre mal avec la dimension personnaliste du système juridique français et européen de protection des données personnelles », retenait Cécile Pérès[104]. Il restaurerait un régime unitaire aux photographies, lettres missives et autres journaux intimes... Observons que le Conseil supérieur du notariat était favorable à faire échapper les données personnelles aux règles ordinaires du partage successoral, au même titre que les souvenirs de famille[105] ; tandis que le Congrès

101 - A. Cousin, « La *Data* au cœur du projet de loi pour une République numérique », *D.* 2018, p. 2176 retenant que « le projet se refuse à affirmer la propriété de l'individu sur les données le concernant, mais lui donne le droit de décider des usages qui en sont faits, qui devient ainsi un attribut de la personnalité ».

102 - L. Castex, E. Harbinja, J. Rossi, « Défendre les vivants ou les morts ? Controverses sous-jacentes au droit des données *post mortem* à travers une perspective comparée franco-américaine », *Réseaux* 2018/4, p. 117, spéc. p. 134-9.

103 - Sur la notion, F. Terré, Y. Lequette, S. Gaudemet, *Droit civil, Les successions, Les libéralités*, Dalloz précis, 4e éd. 2014, p. 236-8, n° 242. Sur la nature des droits, v. supra sect. 2, §2 A2, b et c.

104 - C. Pérès, *op. cit.*, n°11-12 examinant le projet de loi à la lumière du droit américain à dominante successorale.

105 - Contribution du Conseil supérieur du notariat, observations sur la mort numérique (art. 20), *op. cit.*, en déduisant qu'il serait opportun de les considérer, avec le patrimoine numérique, comme des éléments de succession anomale. Rappr. *#Familles, #solidarité, #numérique*, 113e Congrès des notaires de France, 2017, p. 889.

des notaires de 2017 relevait que les données personnelles qui ne sont pas apparentées à des souvenirs de famille ne devraient pas être remises. Parallèlement, consultée sur le projet de loi, la Commission nationale de l'informatique et des libertés avait exprimé ses réserves sur la transmission globale des droits issus de la loi de 1978 aux héritiers, ces « droits personnels » ne devant être transférés qu'en présence de directives, à la différence des « droits réels » transférés automatiquement au décès en application des règles successorales du code civil[106]. Le législateur semble l'avoir entendue puisqu'il a pris quelques précautions de langage en prévoyant non une transmission, mais une simple communication des biens numériques et données s'apparentant aux souvenirs de famille, montrant les ambiguïtés du dispositif et de la nature des droits conférés. Ces biens numériques, dont la valeur peut être élevée, seront les plus difficiles à appréhender[107]. Notons que le II de l'article 85 de la loi de 1978 porte en germe un nombre important de difficultés en se rattachant à une thèse patrimoniale, qui fait douter de la capacité du défunt à transmettre des biens, sur lesquels son droit de propriété n'est pas si certain[108]. Si les « données » sont appropriables, leur propriétaire pourrait être le responsable du traitement, qui détient les droits sur la base de données, et non la personne dont les données ont été collectées. Pour épuiser le débat sur les aspects patrimoniaux, précisons que le parallèle avec le droit d'auteur n'est pas à même de justifier l'exercice des droits sur les données personnelles du mort. Premier obstacle, il n'y a pas d'œuvre à protéger ou à divulguer. Deuxième obstacle, le droit moral de l'artiste ne se limite pas à la protection de sa personnalité, il est perpétuel et défend également le patrimoine culturel[109].

106 - CNIL, Délib. n°2015-414, 19 nov. 2015 *avis sur un projet de loi pour une République numérique*, art. 23, 28.

107 - C. Pérès, *op. cit.*, n° 12 relevant la limite de l'approche personnalise avec la multiplication prévisible des actifs numériques, prônant une réponse issue du droit des biens et des successions sur les conditions de transmissibilité et une réponse contractuelle adaptée évitant de précariser la propriété.

108 - A. Favreau, « Mort numérique : précisions (...) », *op. cit.*, spéc. IA ; L'accès des proches (...), *op. cit.*, p. 74.

109 - *Loc. cit.* ; C. Pérès, *op. cit.*, n°12 examinant le projet avant le vote de la loi.

§ 2 : Administrer les données et l'identité numérique après la mort

Le nouveau dispositif intégré à la loi du 6 janvier 1978 tend à organiser les droits sur les traitements de données personnelles concernant le mort *via* des directives élaborées préalablement par celui-ci. Plus fondamentalement, leur fonction n'est autre que de permettre la mise en œuvre des droits d'opposition et de rectification, permis par l'accès aux données déjà traitées. Il s'agit d'administrer les éléments identifiants du défunt auprès des opérateurs ayant recours au traitement de données. Il s'en déduit une forme d'administration de l'identité numérique du défunt par ses proches, notamment sur les outils d'échange de l'Internet 2.0. Comment mettre ces droits en œuvre, déterminer le contenu des directives à rédiger ? (A) Prendre l'éclairage des mesures utilisées en France dans un passé récent (B) devrait orienter le contenu des démarches à entreprendre (C).

A. Diversité des pratiques numériques face à la mort

Contre toute attente, l'identité numérique *post-mortem* peut être sciemment gérée par l'internaute. On connaît les sites et profils d'hommage créés par des tiers postérieurement au décès, emblématiques de l'Internet participatif. Il est en outre fréquent que les profils créés du vivant d'une personne sur les réseaux sociaux numériques soient, dans un second temps, transformés par ses proches en lieu de recueillement et d'hommage au défunt. Toutefois, dès les années 1990, le détournement des services d'envoi de courriels programmés dans la perspective de son décès à venir a débuté la prise en compte de la mort, à la première personne[110].

Différentes solutions de prise en compte des aspects numériques de la mort d'une personne préexistaient donc au nouveau dispositif législatif. Le sort des traces numériques après décès pouvait déjà être organisé en prévoyant d'inscrire sur une simple feuille de papier les identifiants et mots de passe afin de conférer aux proches l'accès aux comptes en ligne ; si le document comprenant les dernières

110 - Sur ces trois types de présentation de défunts, v. F. Georges, « Identité numérique *post mortem* et nouvelles pratiques mémoriales en ligne. L'identité du créateur de la page mémoriale sur Facebook », *in Identité et multiplicité en ligne*, M. Bonenfant, C. Perraton (Dir.), PU Québec, Les cahiers du Gerse, 2015, p. 51, spéc. p. 55-7.

volontés numériques est écrit de la main de la personne, daté et signé, il constitue un testament olographe, qui pourrait être déposé auprès d'un notaire afin d'en faciliter la révélation *post-mortem*. Il était également envisageable d'employer les innovations du marché des offres de services relatives à la mort numérique[111]. Une étude de science de gestion les a classées en trois catégories suivant les prestations proposées : les services de transmission de mots de passe ou instructions, les coffres-forts numériques[112] testamentaires et les services créatifs d'organisation des traces en ligne[113]. On dénombre en premier lieu les services de transmission de mots de passe ou d'instructions, telles les clauses de transmission de données des acteurs institutionnels célèbres, comme le gestionnaire de compte inactif de la messagerie Google ou le contact légataire du réseau social Facebook[114]. Ou encore l'ange gardien désigné sur le site « *E my life* » pour gérer, contre rémunération, la clôture de certains comptes sur Internet. En second lieu, les coffres-forts numériques testamentaires, tels « Edeneo » et « *E my life* » permettent de déposer différents fichiers, y compris identifiants et mots de passe[115]. En troisième lieu, des prestataires organisent les traces en ligne, tels « Eternissim » et « *Stone story* » proposant la création d'un espace mémoire évolutif à destination des proches[116]. Derrière ces usages, une autoproduction de soi permet de s'assurer d'une forme d'immortalité numérique[117].

111 - S. Guillemot, A. Gourmelen, *op. cit.*, p. 134 recensant sept modes de sauvegarde des éléments identifiants de la personne : transfert des identifiants et mots de passe sur papier et *via* un notaire, impression des photos issues des profils de réseaux sociaux (et/ou autres sites Internet), emploi des fonctionnalités « biographiques » des sites fréquentés (ex : temps forts de l'année en photo), outre trois types de services en ligne étudiés ci-après.

112 - V. Décret n° 2018-418 du 30 mai 2018 *relatif aux modalités de mise en œuvre du service de coffre-fort numérique,* JO 31 mai 2018, n°0123, texte n°36 pris en application de la loi n° 2016-1321 du 7 oct. 2016 (article 87) prévoyant de compléter le titre Ier du livre III du code des postes et des communications électroniques.

113 - S. Guillemot, A. Gourmelen, *op. cit.*, spéc. p. 127.

114 - V. *supra* sect. 1, §2 C et sect. 2, §2 A2 et B1.

115 - V. le site <https://www.safeinheaven.be/fr/> ; dernier accès en septembre 2018 aux sites <http://www.e-mylife.fr> ; <https://secure.edeneo.fr/>, inaccessibles en février 2019.

116 - V. les sites <https://www.eternissim.com> et <http://www.stone-story.eu/fr>.

117 - F. Gamba, « Vaincre la mort : reproduction et immortalité à l'ère du numérique », *Études sur la mort* 2015/1, n° 147, p. 169, spéc. 174-6 ; *Id.*, *Mémoire* (...), *op. cit.*, p. 209-13 discernant cinq types de coffres-forts numériques selon les objectifs du souscripteur avec un poids symbolique croissant : *social*, *financial*, *relationship*, *creative*, *thanatological*.

En plus de ces sites, nous avons pu dénombrer quelques sites Internet commémoratifs, ou mémoriaux virtuels, qui combinent parfois les différents services sus-évoqués, ainsi de « Mon album de vie », « *After me* », « *Movieternity* », « En souvenir », « *GrantWill* »[118]. Certains sites s'affichent comme le moyen d'un hommage, apparemment plutôt proposé à l'ouverture pour les proches endeuillés, tels « Toujoursla. com », « *E-memoria* », « Dans nos cœurs », ou se présentent comme des cimetières virtuels, répondant aux déménagements des familles, comme « Jardin du souvenir », « Celesteo », « Cimetière virtuel »[119]. Existent en outre des sites destinés à expédier des messages aux proches si l'on n'y pointe pas régulièrement pour attester être en vie, comme « Après la mort », ou le site anglophone « *Safe beyond* »[120] permettant d'envoyer des messages pour des dates précises à ses proches. Les premiers sites Internet commémoratifs à caractère social ont été créés en Amérique du Nord, États-Unis et au Canada, à la fin des années 1990. En France, le phénomène est plus récent, il est très développé dans le secteur du souvenir des victimes et combattants de guerre, prolongeant le tourisme dit « kaki », des lieux d'histoire militaire[121] ; il se manifeste également pour les victimes de catastrophes ou d'attentats[122]. S'agissant de la commémoration du souvenir des proches décédés, les fermetures de sites Internet commémoratifs semblent fréquentes dans un marché encore

118 - V. les sites <http://monalbumdevie.com/> ; <https://www.after-me.com/> ; <http://www.movieternity.com> ; <www.en-souvenir.fr> ; <https://www.grantwill.com>. *Adde*, belge : <http://www.defunt.be> ; canadien : <https://www.inmemoriam.ca> ; anglo-phones : <http://dead social.org> ; <https://www.safebeyond. com/> ; <http://www.hereafterinstitute.com/welcome>.

119 - V. sites <https://www.toujoursla.com/> ; <https://www.e-memoria.fr/> ; <http://www.dansnoscoeurs.fr> ; <http://www.jardindusouvenir.fr> ; <http://www.celesteo.com/> ; <https://www.cimetiere-virtuel.fr/>. *Adde*, <https://www.jesuismort.com/> cimetière virtuel de 11.000 tombes, qui recense les personnalités ayant eu une influence sur l'Histoire du Monde ; A. Wrona, La vie des morts : jesuismort.com, entre biographie et nécrologie, Questions de communication 2011/19, p. 73.

120 - V. les sites <https://www.apreslamort.net/index.php> ; <https://www.safebeyond.com/>.

121 - Les sites et cénotaphes en ligne proposant informations et visites virtuelles de cimetières militaires sont légion.

122 - F. Quinche, « Faire mémoire (...) », *op. cit.*, spéc. « Le rôle des journalistes pour la commémoration en ligne » ; N. Paton, J. Figeac, « La commémoration des "mauvais morts" au sein de sanctuaires spontanés numériques », *Cahiers du numérique*, 2013/3, vol. 9, p. 241 ; G. Truc, « Témoigner (virtuellement) sa solidarité aux victimes. Les usages d'un dispositif informatique en gare d'Atocha après l'attentat du 11 mars 2004 à Madrid », *Réseaux* 2018/4, p. 21.

assez peu mature n'ayant pas encore conquis un public durable[123]. D'ailleurs, parmi les sites consacrés au deuil numérique recensés par des publications de 2012 et 2014 moins de la moitié sont toujours actifs[124]. Innovation récente, depuis 2016, une entreprise de pompes funèbres en ligne propose de se charger gratuitement d'effectuer différentes démarches posthumes, à titre accessoire de l'organisation de funérailles ; ainsi de la résiliation de divers services d'abonnements (Internet, électricité...) et de la clôture des comptes sur les réseaux sociaux numériques du défunt[125]. À ce jour, en dépit du développement de l'offre proposée, la population ne semble pas s'être encore approprié les différents services numériques dédiés à la mort.

B. Difficulté à préparer sa mort numérique

À l'ère digitale, la mort n'est pas qu'un processus physique, elle se double d'une dimension immatérielle. Une seconde mort dématérialisée implique de prendre le temps de s'y préparer. Ce d'autant que, non sans paradoxe, ses effets s'étirent dans le temps de l'éternité numérique. L'un des obstacles principaux à l'organisation du sort de ses propres données *post-mortem* est la

123 - S. Guillemot, A. Gourmelen, *op. cit.*, p. 126 notant que nombre de sites ont cessé leur activité (*lab109, For U Forever, Masaga, Memolane, Memory-life*), ne se développent pas ou ne sont plus actualisés (*Biobble)*.

124 - G. Bailly, « Les bonnes raisons d'investir dans l'économie du funéraire », 17 déc. 2012, <https://www.funeraire-info.fr/tag/mort-et-internet/> [disponible en septembre 2018 et à ce jour inaccessible] énumérait les sites suivants toujours consultables : <www.comemo.org> devenu <http://deuil.comemo.org> ; <www.toujoursla.com> ; <www.celesteo.fr> ; <www.jardindusouvenir.fr> ; <www.lecimetiere.net> devenu <https://www.cimetiere-virtuel.fr/index.php>. Sites cités en 2012 inactifs à ce jour : <www.osouvenir.com> ; <www.peoplememory.com> ; <www.memory-history.com> ; <www.peoplestory.org> ; <www.en-memoire.com> ; <www.memoiredesvies.com> ; <www.en-mémoirede.com> ; <www.nos-chers-disparus.com> ; <www.paradisblanc.com> fusionné avec <http://www.dansnoscoeurs.fr>. V. C. Béguin-Faynel, Pour un testament des dernières volontés numériques (...), *op. cit.*, p. 67, spéc. p. 82 renvoyant au site encore actif : <https://secure.edeneo.fr/> tandis qu'ont disparu : <http://www.laviedapres.com/> ; <http://www.e-mylife.fr/> ; <https://www.planneddeparture.com/> ; <http://www.deathswitch.com/> ; <http://legacylocker.com/> transféré vers un autre site supprimé <https://blog.passwordbox.com/> enfin le cimetière virtuel <http://www.tunousmanques.fr/> a été fermé. *Adde*, également clôturés : « *lifeafterme.com* », « etombe.net », « memoiredesvies.com », « netcropole.com ».

125 - A. Schwyter, « La start-up AdVitam veut vous aider à gérer votre mort numérique », 1er nov. 2017, <https://www.challenges.fr/start-up/comment-la-start-up-advitam-veut-gerer-votre-mort-numerique-sur-facebook-twitter-google-et-linkedin_510480>. V. le site <https://advitam.fr/prestations-obseques-en-details> prévoyant ces mesures pour attirer la clientèle des endeuillés en les soulageant des démarches administratives.

difficulté du passage à l'acte préparatoire. Plusieurs arguments ont été avancés pour expliquer l'absence d'anticipation de son propre décès, de personnes souvent sensibilisées aux problèmes posés par la mort numérique à travers la mort de leurs proches ou de personnalités[126]. Un mécanisme psychologique d'évitement peut être mis en place, la personne tentant par ce biais de gérer le stress provoqué par l'évocation de sa propre mort. En outre, tous les acteurs traditionnels de la mort connaissent ce phénomène d'inaction, ainsi des services de pompes funèbres pour l'organisation des obsèques ou des notaires au titre de la transmission du patrimoine. Les contours mouvant de l'identité numérique et sa co-construction en interagissant avec d'autres personnes connectées sont encore un obstacle relevé. Il a au demeurant pu être souligné que les individus peuvent préférer des actions dites manuelles comme la transmission orale ou écrite de mots de passe, ou l'impression des photos numériques, plutôt que de confier leurs données à une entreprise privée proposant ces services par voie numérique.

Deux auteurs ont d'ailleurs fait ressortir de la littérature sur la préparation à la mort dans un contexte numérique que « les pratiques *on-line* semblent fonctionner comme celles concernant les biens tangibles »[127]. Leur enquête a révélé que la situation de famille ou la catégorie socioprofessionnelle n'apparaissaient pas discriminantes pour établir des profils. Les variables significatives étaient « l'attachement aux contenus numériques, les motivations à transmettre la mémoire et l'expertise perçue en matière d'Internet ». « L'orientation temporelle » serait également déterminante. Elle correspondrait à une motivation à transmettre la mémoire qui résulterait en partie de l'attachement aux objets reflétant la mémoire et d'une projection dans le futur ; il apparaît que la perception subjective du temps et notamment du temps restant à vivre est plus signifiante que l'âge s'agissant de franchir l'étape de se mettre à préparer les conséquences de sa mort[128]. L'étude publiée en 2017 dégagea différents profils, seuls 26,8 % des internautes interrogés

126 - S. Guillemot, A. Gourmelen, *op. cit.*, p. 131.

127 - *Ibid.*, p. 140.

128 - *Ibid.*, p. 138 et 141 et p. 128-130 retenant qu'un « individu orienté futur aura davantage tendance à s'interroger sur l'avenir de ses traces en ligne et de ses contenus numériques qu'un individu orienté présent ».

sont rattachés à la catégorie des « réticents absolus », hermétiques aux problématiques liées à la mort numérique, appréhendée par les trois quarts des répondants[129]. Décrivant quatre autres profils d'utilisateurs potentiels de services de préparation à la mort numérique, les auteurs fournissaient une typologie et un argumentaire proposant de segmenter le marché et d'adapter leurs offres de services[130]. Au-delà du marketing objet de l'étude, les arguments avancés nous semblent tout aussi pertinents pour diffuser de l'information et favoriser la prise de conscience sur les enjeux de la mort numérique et révéler la nécessité de se positionner individuellement sur la question.

Confirmant le schéma classique de la préparation de la mort dans le monde physique, la difficulté à entreprendre des actions pour organiser leur mort numérique était marquée pour deux profils dégagés dans l'enquête de 2017. Les « prévoyants » et « bricoleurs » étaient jugés peu motivés, mais se sentant obligés de se pencher sur la question. Leur intérêt tenait essentiellement à des raisons qualifiées de « communales », faisant référence aux actions « motivées par le fait de préserver un sens commun et de laisser des traces qui pourront être utiles et servir les générations futures »[131]. Parmi les plus concernés, figuraient les « réservés » plutôt motivés pour des raisons dites agentiques, renvoyant à la « volonté de promouvoir sa propre personne à travers la transmission d'un objet porteur de mémoire. Les individus espèrent ne pas être oubliés après leur mort, ils cherchent alors à contrôler l'image qu'ils laisseront d'eux ». Tandis que les « *geeks* » se révélaient les plus intéressés, car possédant à la fois des motivations agentiques et communales.

Il était préconisé aux prestataires payants de services spécialisés dans la mort numérique (tels « Edenéo » et « la vie d'après ») ayant adopté un discours sacré sur le mort, de le compléter en insistant sur la transmission, l'idée de laisser une trace, et la maîtrise de son image *post-mortem*, arguments dits agentiques, en accord avec les motivations des deux profils les plus concernés par la question

129 - *Ibid.*, p. 135, 136 et 138 sur les « réticents absolus ».

130 - *Ibid.*, p. 142, spéc. conclusion.

131 - *Ibid.*, p. 130 et 140 définissant les motivations qualifiées d'agentiques et de communales. Sur les « prévoyants », i*bid.*, p. 136, 141 ; sur les « bricoleurs », *ibid.*, p. 138, 141 et tableau récapitulatif p. 143-4.

« *geeks* » et « réservés », représentant respectivement 14,6 et 21,8 % du panel sondé[132]. L'enquête soulignait que pour les grands acteurs du web, tels Google et Facebook, qui veulent encourager leurs utilisateurs à anticiper le devenir de leurs contenus numériques déposés chez eux un discours neutre sur la nécessité de la démarche devrait faire sens chez les profils « prévoyants » ; ces derniers, représentant 14,3% du panel, seraient plus sensibles aux arguments fondés sur l'alternative aux mots de passe éparpillés sur des papiers et l'aide pour éviter les tracas administratifs des héritiers. Une argumentation supplémentaire sur la maîtrise de l'image serait satisfaisante pour les catégories des « *geeks* » et « réservés », la moindre expérience numérique des seconds pouvant être contrée par des arguments sur la simplicité d'utilisation, relayée par des tutoriels vidéos, outre le fait de pouvoir laisser sa trace. De manière plus spécifique, les profils « *geeks* » caractérisés par leur aisance avec le numérique pourraient être sensibles aux arguments « fondés sur l'attachement sentimental aux contenus numériques couplés aux motivations agentiques et communales » précédemment évoquées. Pour le cinquième profil dit des « bricoleurs », ils pourraient « être impliqués en leur indiquant explicitement la possibilité de se passer de la plateforme, en formulant leurs directives anticipées directement à leurs proches, dans une perspective sociétale, à l'image des campagnes de communication pour le don d'organes ». Ils correspondaient à 22,5% du panel interrogé et semblaient devoir être sensibles à l'idée de transmission de l'essentiel pour les proches via les services numériques. Les trois profils les plus enclins à agir pour organiser sa transmission numérique représentent 58,9 % du panel. L'idée semble prête à germer sur le terreau des dispositifs légaux et contractuels disponibles.

C. Flexibilité des outils d'organisation numérique de sa mort

Prévoir des directives pour organiser de son vivant la mise en œuvre posthume de ses droits sur ses données présente des avantages de fond et de forme. Tout d'abord, sur le fond, les directives transmises devraient permettre de laisser une trace, de favoriser la transmission

132 - *Ibid.*, p. 134, 138, 141-2 et tableau récapitulatif p. 143-4 sur les « *geeks* » et « réservés ». L'enquête relevait, p. 142, que si ces prestataires rencontrent des difficultés pour se développer, c'est sans doute que ces arguments ne suffisent probablement pas à justifier le prix des prestations.

d'informations sur le parcours de vie jugées essentielles et publiées sur les réseaux sociaux de communication ou de partage de photos ou de vidéos, des blogs et vlogs, ainsi que des correspondances échangées... Ces informations rassemblées esquissent une identité numérique à défendre par une organisation spécifique. Les directives établies par la personne tendent à préserver son attachement sentimental à ses contenus numériques et sa volonté de le transmettre aux générations futures. Les directives générales de l'article 85 I de la loi de 1978 peuvent servir de véhicule aux identifiants en rendant plus sûre leur transmission rassemblée. Elles constituent une avancée incitant à transmettre des indications explicites aux héritiers ou aux proches destinataires des mesures à effectuer.

En rédigeant des « directives générales » conférant un mandat général d'agir, il reste utile de donner des éléments précis pour la mise en œuvre des prévisions du défunt. Les proches auraient ainsi une solide légitimité pour agir à l'encontre des opérateurs Internet et responsables de traitement de données. Faut-il clôturer tel compte ou tel autre, notamment sur les réseaux sociaux numériques ? Les comptes maintenus actifs pourront-ils être modifiés ou doivent-ils devenir des espaces mémoriaux laissés intacts ? Comment administrer les contenus s'y trouvant ? À qui conférer l'accès aux comptes sur les réseaux sociaux ou de messagerie ? Faut-il sauvegarder les contenus textuels, photographiques, audiovisuels enregistrés sur les comptes, espaces de stockage en ligne, et ordinateurs du défunt ? Faut-il effacer certains contenus identifiés par la personne organisant le sort de ses données *post-mortem* ? Le transfert de contenus de formats divers est envisageable *via* un site de commémoration ou une entreprise de coffre-fort électronique, mis en place par le défunt, qui faciliteront la mise en œuvre des directives qu'il a prévues. De surcroît, la mission peut consister uniquement à notifier au responsable d'un traitement de données personnelles que la personne est décédée, même s'il peut également être demandé de cesser le traitement à l'avenir en couplant l'exercice du droit de rectification et celui du droit d'opposition, des articles 50, 56, 106 et 110 de la loi du 6 janvier 1978. Les proches y procèdent généralement spontanément pour informer les administrations, l'employeur et les organismes versant des revenus à la personne ; tels la Direction générale des finances publiques, les organismes de protection sociale ou de retraite. On ne manquera pas de noter que s'il existe des directives, cela évite

un questionnement sur la volonté du mort et des choix difficiles[133]. L'autre avantage est de préparer un inventaire englobant des biens immatériels souvent négligés comme les noms de domaines acquis par le défunt ou les créances attachées aux comptes en ligne pouvant présenter un solde positif (compte de jeu : paris, *e-sport* vidéo ; comptes de paiement *PayPal* ; comptes de vendeur sur des plateformes de commerce en ligne, *marketplace*). En expliquant ses volontés, la personne peut désamorcer les conflits potentiels entre ses héritiers. Désigner une personne avec une mission précise peut s'avérer un meilleur choix que laisser une tâche à chacun des proches, laissant poindre des conflits sur la cohérence globale des mesures prises.

Quant à la forme, sans rédiger ni transmettre des directives au sens de l'article 85 de la loi du 6 janvier 1978, une simple communication orale ou écrite – sur papier ou via un accès à un service de stockage, *cloud* – des identifiants des différents comptes en ligne d'une personne – noms d'utilisateur et mot de passe – ou via une entreprise proposant un service spécifique peut se révéler une organisation efficace. On peut espérer la mise à disposition de modèles de directives établis par les avocats et les notaires[134]. Mais le coût à débourser pour obtenir un conseil pourrait constituer un frein au passage à l'acte de planification des conséquences numériques de sa mort. Il peut être négligeable s'il s'agit d'intégrer ses directives générales dans un testament authentique rédigé par un notaire, comprenant ses autres dispositions à cause de mort, sans frais spécifiques additionnels. La dépense serait quasi nulle, si l'on considère l'envoi de directives particulières par un courriel vers une entreprise du commerce électronique, un service de messagerie électronique, de réseau social en ligne, ou un hébergeur de blog. Une enquête récente a montré que 55 % de la vie numérique (*e-mail*, *e-commerce*, musique, vidéo, réseau social) d'un internaute moyen passe par les quatre plates-formes des GAFA (Google, Apple,

133 - F. Georges, V. Julliard, « Profilopraxie et apposition des stigmates de la mort : comment les proches transforment-ils la page Facebook d'un défunt pour la postérité ? », *Linguas e Instrumentos Lingüisticos* 2016/37, p. 231, spéc. p. 235.

134 - Les pouvoirs publics ont renoncé à établir un formulaire CERFA durant les débats parlementaires.

Facebook et Amazon)[135]. Ce sont donc ces quatre grands opérateurs auxquels souvent il faudra adresser des directives spéciales, sur le sort *post-mortem* des informations détenues, introduites par la loi du 7 octobre 2016. De telles mesures existaient déjà avec l'ajout des fonctionnalités de gestionnaire de compte inactif à la messagerie Google et de contact légataire au réseau social Facebook en 2015[136]. Mais si l'activité numérique est intense, le nombre d'entreprises à contacter peut se révéler très élevé et dissuader l'initiative ; on laissera alors à ses proches le soin de procéder à la réorganisation après-décès en s'abstenant d'agir ou en leur confiant expressément cette mission dans des directives générales sur le sort des données du mort précisant ses souhaits. Mettre en œuvre ces consignes constitue une mission d'importance.

Section II - Les mesures *post mortem* ouvertes aux héritiers

« Le mort n'est pas tout à fait mort... s'il a des héritiers ».
J.-D. Bredin, « Le droit, le juge et l'historien »,
Le débat, nov. 1984. 97, spéc. n°8.

Il apparaît pertinent d'envisager la question des données personnelles du mort du côté des personnes qu'il laisse à sa survivance. À quels accès aux données du défunt ces personnes peuvent-elles prétendre ? On rappellera que les tiers ne doivent pas avoir accès en principe aux données personnelles d'une personne, sauf si la loi le prévoit[137]. Quels proches pourraient se voir reconnaître un accès privilégié ? Le terme héritier est chargé d'une dimension juridique spécifique et renvoie à la dévolution juridique des biens transmissibles. Le rôle de continuateur de la personne du défunt est classiquement confié aux héritiers légaux pour la transmission du patrimoine, bien

135 - S. Guillemot, A. Gourmelen, *op. cit.*, p. 125. *Adde*, C. Pellet, « Décès : identité numérique et droit à l'oubli », *Petites Aff.,* 26 mars 2015, n° 61, p. 4 listant les procédures à suivre de Google, Facebook, Twitter... Pour des statistiques de la société de l'information, <https://ec.europa.eu/eurostat/web/digital-economy-and-society/overview>.

136 - V. <https://support.google.com/accounts/answer/3036546?hl=fr> ; <https://www.facebook.com/help/156801 3990080948> et *supra* sect. 2, §2 B1 sur les services de fourniture de contenus numériques d'Amazon et Apple.

137 - CJUE, 4 mai 2017, aff. C-13/16, *Rīgas satiksme*, *D. IP/IT* 2017 p. 552, obs. G. Rostama, E. Malaty retenant que la directive 95/46/CE n'impose pas l'obligation de communiquer à un tiers les données personnelles de l'auteur d'un dommage afin de saisir le juge d'une indemnisation et ne s'oppose pas à ce que le droit national le prévoit.

qu'il soit possible d'instituer, par une manifestation de volonté, qui l'on souhaite légataire universel ou de nommer un tiers exécuteur testamentaire[138]. Ne faudrait-il envisager les proches dans une vision plus élargie des continuateurs de la mémoire du défunt ? Quelle place pour les relations d'amitié, les contacts ou abonnés, qui suivent le compte d'une personne, sur les réseaux sociaux numériques ? Le rôle dévolu à de tels « héritiers spirituels » peut-être central. Mais la sécurité juridique empêche la loi de renvoyer à des situations de fait, délicates à mettre en œuvre. Par conséquent, ils ne pourront agir qu'en application des directives générales ou particulières données par le défunt sur ses données personnelles, leur conférant mandat d'agir après son décès, en vertu de l'article 85 I de la loi du 6 janvier 1978, sauf si la loi venait à leur ouvrir une action.

Ce texte prévoit, par ailleurs, des dispositions supplétives de volonté en l'absence de directives, qui ne jouent qu'en faveur des héritiers. Il est donc à souligner que le survivant du couple non marié, qui n'aurait pas été institué légataire universel, ne pourra donc pas s'en prévaloir. Le nouvel article comprend plusieurs mesures légales tendant à favoriser l'organisation et le règlement de la succession et faciliter l'actualisation des données de la personne décédée auprès des responsables de traitement. Les droits de la personne défunte sur ses données personnelles peuvent ainsi être mis en œuvre *post-mortem* par ceux qui lui survivent, articulant les droits et les rôles des vivants et des morts (§ 2). Le dispositif spécifique voté en 2016 ne doit pas occulter que le droit civil avait déjà organisé les droits des survivants en cas de décès de leurs parents, au fil de contentieux sur le respect de la vie privée et du droit à l'image, en matière de responsabilité ou de filiation (§ 1).

§1 : Articulation éprouvée entre droits du mort et des vivants

Il est important de concevoir la protection des données personnelles du mort à la lumière des autres pans du droit, au-delà de la seule loi du 6 janvier 1978. Le nouveau texte adopté en 2016 ne se substitue pas aux lois et constructions jurisprudentielles en droit des personnes, de la filiation et de la santé, qui aménagent une protection préservant le défunt, mais aussi les droits des héritiers

138 - C. civ., art. 720 et 1025 à 1034.

qu'il laisse à sa survivance. L'adoption d'une protection spécifique ne fait pas table rase du passé[139]. Les droits à l'image et à la vie privée furent invoqués de longue date à l'occasion de décès (A). En outre, afin de permettre aux héritiers d'une personne de faire valoir leurs droits le juge donna une interprétation large des textes sur la consultation des documents administratifs ou traitant des données du défunt ou encadrant la levée du secret médical sur ses données de santé (B). En cas d'accouchement secret, la volonté du parent de naissance est très largement préservée, mais l'accès à son identité et à des informations le concernant a été facilité *post-mortem* (C).

A. Respect dû au mort et vie privée des héritiers

Il est à peine besoin de rappeler que lorsqu'une personne trépasse, la fin de la personnalité juridique entraîne l'extinction des droits attachés à la personnalité ; « à l'heure de la mort, être humain, vie humaine et personnalité juridique s'éteignent ensemble » selon Gérard Cornu[140]. Il n'y a pas de protection de la vie privée du défunt[141]. Le respect du droit à la vie privée et à l'image[142] n'appartient qu'à la personne concernée et s'éteint à son décès[143], sans être transmissible

139 - T. Dautieu, É. Gabrié, A »nalyse de l'apport de la loi pour une République numérique à la protection des données à caractère personnel (1re partie). L'ouverture de l'accès aux données publiques et sa conciliation avec la protection des données à caractère personnel », *Comm. com. électr.* 2016, étude 22, spéc. n°6 estimant que « aucune modification n'a été apportée quant aux secrets relatifs à la vie privée » ou au secret médical par la loi de 2016.

140 - Cité *in* D. Dutrieux, « Du monde des vivants à l'immonde des morts ? », *Petites Aff.* 3 oct. 2013, n° 198, p. 12, spéc. *in fine*. V. D. Guerin-Seysen, « Approche juridique de la marchandisation de la mort », *Petites aff.* 10 sept. 2010, n° 181, p. 11, spéc. III le respect de la mémoire des morts.

141 - F. Dekeuwer-Defossez, « Rapport de synthèse : existe-t-il une définition unique et transversale de la notion de personne ? », *Dr. famille* 2012, étude 11 ; spéc. n°9 ; J. Hauser, « Les bornes de la personnalité juridique en droit civil ? », *Dr. famille* 2012, étude 4 ; spéc. n°36 et s. sur la personnalité virtuelle. Dans un premier temps, une « vie privée posthume » avait été affirmée, TGI Paris, 21 oct. 1980, *D*. 1981. 72, note R. Lindon.

142 - Sur leur application aux informations en ligne, M. Dupuis, « La vie privée à l'épreuve des réseaux sociaux », *RLDC* 2013/102, p. 39 ; *Id.*, « La vie privée à l'épreuve de l'Internet », *RJPF* 2001/12, p. 12 ; « Réseaux sociaux et vie privée », *RLDI* 2014/1, p. 108 ; A. Lepage, « Les droits de la personnalité confrontés à l'Internet », *in Libertés et droits fondamentaux*, R. Cabrillac, M.-A. Frison-Roche, T. Revet (Dir.), Dalloz, 24e éd. 2018, p. 269.

143 - Cass. 1ère civ., 14 déc.1999, n° 97-15.756 ; Bull. n°345 ; *RTDciv.* 2000. 291, obs. J. Hauser ; *D*. 2000. 372, obs. B. Beignier ; crim., 20 oct. 1998, n° 97-84621 ; Bull. crim. n°264 ; *D.* 1999. 106, obs. B. Beignier.

à ses héritiers[144]. Pour autant, une protection indirecte existe au travers de la préservation des sentiments d'affliction des personnes survivant au défunt. Lorsqu'une atteinte à la mémoire du défunt est perpétrée *post mortem*, ses héritiers peuvent en effet invoquer leur propre droit à la vie privée et familiale en tant que parents du défunt sur le fondement des articles 9 du Code civil et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales[145]. Ils devront démontrer que l'image ou les propos tenus à l'égard du défunt leur causait un préjudice personnel en raison d'une atteinte à sa mémoire ou au respect dû au mort[146]. Une appréciation de la situation concrète permettra de distinguer entre un cliché publié sur un réseau social « dans un cadre très restreint personnel ou familial » qui ne nécessite aucune autorisation et ne génère pas de préjudice spécifique [147], et la publication dans un journal d'une photographie de la dépouille mortelle, qui peut être constitutive d'un trouble pour la vie privée des proches, heurtés dans leur deuil [148]. Le juge, statuant au fond ou en référé, pourra « prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée » et ordonner paiement de dommages et intérêts en application des articles 9 alinéa 2 et 1240 du code civil.

Le droit de la presse organise une protection pénale de la mémoire des morts, qui se révèle également orientée pour préserver l'héritier,

144 - Cass. 2ème civ., 8 juil. 2004, n° 03-13260, Bull. n°390 ; *RTDciv.* 2004. 714, obs. J. Hauser ; 1ère civ., 15 févr. 2015, n° 03-18302, Bull. n° 86 ; 1ère civ., 31 janv. 2018, n° 16-23591.

145 - CEDH, 30 oct. 2001, *Pannullo c/ France*, n° 37794/97, § 35-6 ; RTDciv. 2002. 393, obs. J.-P. Marguénaud.

146 - Cass. 1ère civ., 1er juil. 2010, n°09-15479 ; Bull. n°151 ; RTDciv. 2010. 760, obs. J. Hauser ; JCP G 2010. 942, note G. Loiseau publication d'un cliché d'un homme torturé (même affaire, CEDH, 25 févr. 2016, *Soc. Conception et d'édition c/ France,* n° 4683/11 ; *Gaz. Pal.* 19 avr. 2016, p. 16, obs. A. Mâzouz) ; 22 oct. 2009, n° 08-10557 ; Bull. n°211 ; *RTDciv.* 2010. 79, obs. J. Hauser ; *Comm. com. électr.* 2010, comm. 7, obs. A. Lepage livre sur la vie d'un artiste décédé ; Rouen, 21 oct. 2009 ; JCP G 2010. 285, note C. Brière remise de clichés par un tiers pour publication.

147 - E. Pierrat, « Le droit à l'image sur l'autel des réseaux sociaux », *Lexbase Hebdo* éd. Privée 2011, n° 431.

148 - Cass. 1ère civ., 29 déc. 2000, n° 98-13875 ; Bull. n°341 ; JCP G 2001. II. 10488, concl. Av. gén. J. Sainte-Rose, note J. Ravanas ; *RTDciv.* 2001. 329, obs. J. Hauser ; CEDH, 14 juin 2007, n° 71111/01, *Hachette Filipacchi associés c/ France* ; RTDciv. 2007. 732, obs. J.-P. Marguénaud ; JCP G 2007. II. 10164, note E. Derieux.

continuateur de la personne du défunt, plus que le mort[149]. Restrictif, l'article 34 de la loi du 29 juillet 1881 *sur la liberté de la presse* ne prévoit en effet d'action judiciaire qu'à supposer établi que les auteurs des diffamations ou injures supposées aient eu l'intention de porter atteinte aux héritiers (légaux ou testamentaires) ou au conjoint survivant du défunt. Même si cet élément intentionnel de l'infraction n'était pas caractérisé, les « héritiers, époux ou légataires universels vivants » peuvent toujours exercer un droit de réponse pour protéger la mémoire de leurs morts à l'encontre des auteurs des diffamations ou injures. Est-il besoin de préciser que « l'honneur des personnes réelles est nécessairement protégé dans les univers virtuels » à supposer réunis les éléments constitutifs de l'infraction[150] ? Au demeurant, trois délits protègent spécifiquement la mémoire des morts. D'abord, l'article 14 de l'ordonnance du 2 février 1945 interdit de publier toute information relative à l'identité et à la personnalité d'un mineur délinquant. Générale et absolue, cette prohibition perdure après la mort du mineur, conférant une large portée à l'infraction[151]. Par ailleurs, la diffusion de toute information relative à l'identité ou permettant d'identifier un mineur s'étant suicidé est réprimée par l'article 39*bis* de la loi de 1881. Tandis que l'article 39*quater* de la même loi préserve trente ans après sa mort la mémoire de l'adopté plénièrement contre la publication d'informations relatives à la filiation d'origine de quelque manière que ce soit, notamment par voie de presse, publication de livre, diffusion radio ou cinématographique. Si les héritiers peuvent sauvegarder leurs droits sur le terrain des droits de la personnalité [152], en restreignant la diffusion des informations personnelles et d'images du défunt, ils peuvent en outre défendre leurs droits patrimoniaux.

149 - B. Beignier, Y. Puyo, « Respect et protection du corps humain – Le mort », JCl. Civil Code, Art. 16 à 16-4, fasc. 72, 2013, spéc. n° 51 ajoutant que les héritiers ne peuvent agir sur le terrain de la responsabilité civile.

150 - A. Latil, « La diffamation dans les univers virtuels », *RLDI* 2010/63, p. 99, spéc. introduction.

151 - Cass. crim., 24 sept. 2002, n° 01-85890 ; Bull. Crim. n° 175 ; *Comm. com. électr.* 2003, comm. 79, note A. Lepage ; Dr. pénal 2003, comm. 5, note M. Véron.

152 - F. Terré, Y. Lequette, S. Gaudemet, *Les successions (...), op. cit.*, p. 60, n°50 sur les droits extrapatrimoniaux.

B. Actions en réparation intentées par les héritiers

Afin de préserver les droits patrimoniaux des héritiers, la jurisprudence leur a reconnu le droit de se prévaloir des données personnelles d'un défunt pour exercer leur droit d'agir, ils pourront solliciter l'indemnisation de leurs propres préjudices ainsi que de ceux subis par le défunt (1). Souvent, ils seront contraints de solliciter la levée du secret médical couvrant les données de santé du défunt pour faire valoir un droit à indemnisation né du fait du décès (2).

1) Préservation des intérêts patrimoniaux des héritiers

Les héritiers peuvent exercer le droit à réparation du préjudice subi par leur auteur. La Cour de cassation, suivie du Conseil d'État, décide que le droit à réparation du préjudice éprouvé par la victime avant son décès, né dans son patrimoine, se transmet à ses héritiers[153]. Est ainsi recevable l'action en indemnisation des préjudices liés à la création d'un faux profil Facebook intentée *post-mortem* par les héritiers d'un professeur d'histoire qui s'est suicidé[154]. Pour saisir le juge d'un tel contentieux ou poursuivre l'action déjà engagée par le défunt, l'accès aux données personnelles du mort peut se révéler crucial pour l'issue du litige. La question ne se posera en termes de données personnelles que, lorsque pour faire valoir un droit, l'héritier aura besoin d'accéder à un document à communication restreinte, détenu par une administration ou un responsable de traitement.

Le système d'accès aux documents administratifs, initialement imaginé au profit du citoyen personnellement concerné, autorise néanmoins l'accès par des tiers, dans les conditions prévues par

153 - Cass. ass. plén., 9 mai 2008, n° 06-85751, 05-87379 ; Bull. ass. plén. n° 2 ; M. Sanchez, *Dr. pén*. 2008, étude 12 ; ch. mixte, 30 avr. 1976 ; Bull. crim. n° 135, 136 ; *D*. 1977, jur. p. 185, note M. Contamine-Raynaud ; CE, 29 mars 2000, n° 195662 ; Lebon p. 147 ; *JCP G* 2000, II, 10360, note A. Derrien ; *D.* 2000. 563, note A. Bourrel ; CE, 27 mars 2015, n° 368440 ; Lebon T. 2005, p. 714 ; CE, 20 juin 2018, n° 408819.

154 - Angers, 20 juin 2017, n° 14/01233 ; *JurisData* 2017-013103 indemnisation du préjudice moral du professeur, dont l'identité a été usurpée, avant l'incrimination de cet agissement, et de celui de ses héritiers.

l'article 6 de la loi du 17 juillet 1978 désormais codifié[155]. Cependant seul « l'intéressé » peut prendre connaissance de documents administratifs « dont la communication porterait atteinte à la protection de la vie privée, au secret médical et au secret en matière commerciale et industrielle »[156]. La Commission d'accès aux documents administratifs interprète la notion de personne intéressée en s'appuyant sur les caractères du document, qui, par son objet, son contenu, sa fonction, la touchent personnellement et directement et en prenant en compte l'existence ou l'absence de conséquences sur les droits patrimoniaux des ayants droit[157]. En sorte qu'elle a pu ordonner communication à la requérante du dossier de pension de sa mère décédée ou à la veuve du récapitulatif des versements effectués par une Caisse de prévoyance au mari décédé[158]. Est encore communicable aux ayants droit de la victime d'un accident au travail le rapport d'enquête établi sur ses circonstances, diligenté par la Caisse régionale d'assurance maladie[159]. Mais, la communication d'un document couvert par le secret de la défense nationale est exclue[160].

Lorsqu'il s'agit d'accéder à des données personnelles du défunt auprès d'un responsable de traitement, les articles 49 et 105 de la loi du 6 janvier 1978 autorisent la personne qui justifie de son identité à recevoir « communication des données à caractère personnel en

155 - Loi n° 78-753 du 17 juil. 1978 *portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal*, JO 18 juil. 1978, p. 2851 ; texte intégré depuis le 1er janv. 2016 au nouveau code des relations entre le public et l'administration (CRPA).

156 - CRPA, art. L. 311-6 dérogeant au principe de libre communication des documents posé à l'article L 311-1.

157 - Commission d'accès aux documents administratifs, *L'accès aux documents administratifs, deuxième rapport d'activité, 1981-1982*, p. 16-7 s'appuyant sur « l'atteinte au "secret de la vie privée" que la personne décédée aurait souhaitée préserver [et] d'autre part, l'aide pratique que ces documents pouvaient apporter aux demandeurs, pour faire valoir un droit ou engager des démarches soit administratives, soit juridictionnelles » ; J.-B. Auby, « Données publiques – Droits d'accès. Étendue », Fasc. 109-60, JCl. Administratif, 2018, n° 88.

158 - *Ibid.*, citant deux avis du 14 janv.1982 *Mme Saint-André* et *Mme Bretel*.

159 - CE, 20 nov. 1995, n° 119944 ; Lebon T. p. 796 jugeant les exceptions légales de refus non caractérisées en l'espèce, la Caisse n'ayant pas expliqué une atteinte au secret commercial ni allégué l'impact sur d'autres personnes.

160 - CE, 30 oct. 1989, n° 100268 ; Lebon p. 221 refus de consultation d'un enregistrement couvert par le secret lors d'un accident entre un pilote de l'armée et les contrôleurs au sol pour élucider les conditions de la mort de son fils.

cours de traitement ainsi que toute information disponible quant à leur source »[161]. Aucun droit d'accès spécifique n'existait en faveur des héritiers avant l'entrée en vigueur du nouvel article 40-1 inséré en 2016 ; le nouveau texte ne semble pas leur fermer la possibilité de se revendiquer personne concernée par le traitement[162]. Saisi à trois reprises, le juge administratif dut déterminer suivant l'espèce si l'héritier pouvait être considéré comme « personne concernée » par le traitement des données du mort[163]. La réponse fut affirmative lorsqu'il s'était agi, en 2011, d'accéder au fichier recensant les données bancaires (FICOBA) pour les « ayants droit héritant des soldes des comptes bancaires de leur tante »[164]. On notera que le but invoqué du règlement d'une dette fiscale[165] montrait l'intérêt patrimonial direct des héritiers à connaître les références des comptes tenus au nom de la défunte.

Plus récemment, par deux arrêts du 8 juin 2016 et 7 juin 2017, le Conseil d'État a affirmé que « la seule qualité d'ayant droit d'une personne à laquelle se rapportent des données ne confère pas la qualité de "personne concernée" par leur traitement au sens des articles 2 et 39 de la loi du 6 janvier 1978 ». En 2016, il estima bien fondé le refus d'accès opposé aux héritiers par la Commission nationale de l'informatique et des libertés pour obtenir les données téléphoniques de la personne décédée adressée à son employeur,

161 - L'article 49 de la loi du 6 janv. 1978 renvoie à l'article 15 du Règlement, qui prévoit la fourniture d'une copie des données traitées, contre une éventuelle rétribution compensant le coût de copie. Notons que, suivant l'art. 2 de la loi de 1978, la personne concernée « est celle à laquelle se rapportent les données qui font l'objet du traitement ».

162 - CNIL, Délib. n°2015-414, *op. cit.*, art. 28 étudiant le projet de loi de 2015, art. 20, estimait qu'il faudrait accorder l'accès aux données du mort aux héritiers, si leur dénier leur cause un préjudice réel, direct et certain. En 2004, un droit de rectification avait été reconnu aux héritiers « si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées » (Loi de 1978, art. 40 ancien, al. 5 et 6). Une telle formule souligne l'absence de droit personnel d'accès.

163 - Le refus du responsable de traitement d'exercice des droits issus de la loi de 1978, ou deux mois sans réponse, ouvre droit à plainte auprès de la CNIL, dont la décision ou le silence permet un recours devant le Conseil d'État.

164 - CE, 29 juin 2011, n° 339147 ; Lebon T. p. 937 ; *RLDC* 2015/4, p. 66, note A. Favreau ; *RLDI* 2015/3, p. 42, note E. Florestal, R. Perray ; *JCP E* 2012, 1489, chr. M. Vivant, N. Mallet-Poujol, J.-M. Bruguière, n°11. V. *supra* §2 A2.

165 - Ce motif convainc la Commission, mais le fisc avait résisté. En ce sens, CADA, avis n° 20170608, 6 avr. 2017.

dans le but de déterminer le nombre et la durée des échanges avec le corps médical *ante mortem*[166]. Il a été relevé que les « données téléphoniques de la personne décédée n'avaient pas de lien direct avec les droits patrimoniaux des ayants droits », à la différence des données sur la titularité de comptes bancaires, pour les héritiers liquidant une succession dans l'arrêt de 2011[167]. Le lien entre les données du mort et ses héritiers semblait insuffisamment caractérisé en l'espèce, ce qui peut être discuté puisque paraît poindre une possible contestation en justice pour faire valoir les droits des héritiers. Dans l'affaire jugée en 2017, tout en énonçant le principe d'absence de transmission automatique aux ayants droit du défunt du droit d'accéder à ses données, le Conseil d'État a posé une dérogation[168]. Reprenant explicitement le principe dégagé par la Cour de cassation, de transmissibilité aux héritiers de l'exercice du droit à réparation entré dans le patrimoine du défunt, le Conseil en déduisit que « Par suite, lorsque la victime a engagé une action en réparation avant son décès ou lorsque ses héritiers ont ultérieurement eux-mêmes engagé une telle action, ces derniers doivent être regardés comme des "personnes concernées" au sens des articles 2 et 39 de la loi du 6 janvier 1978 pour l'exercice de leur droit d'accès aux données à caractère personnel concernant le défunt ». Une limitation intéressante à ce transfert était ajoutée, il ne joue que « dans la mesure nécessaire à l'établissement du préjudice que ce dernier a subi en vue de sa réparation et pour les seuls besoins de l'instance engagée ». Il en ressort que pour conférer aux héritiers l'accès aux données personnelles du mort en leur reconnaissant la qualité de personne concernée, l'utilité présentée par ces informations pour lesdits héritiers s'avère déterminante, notamment lorsqu'elles sont la condition pour la reconnaissance de leurs droits patrimoniaux. L'élaboration d'une casuistique complexe pourrait perdurer pour préciser la notion de personne concernée. Rappelons que selon le Groupe de travail de l'article 29, le fils d'une personne décédée est une personne concernée au regard des

166 - CE, 8 juin 2016, n° 386525 ; Lebon ; *Comm. com. électr.* 2016, comm. 74, note N. Metallinos ; *RLDI* 2016/11, p. 16, obs. P.-D. Vignolle ; *LEFP* sept. 2016, n° 8, p. 2, obs. T. Douville.

167 - P. Cossalter, *RGD on line* 2016, n° 23948.

168 - CE, 7 juin 2017, n° 399446 ; Lebon T. statuant sur les données, qui fondaient l'action en indemnisation d'un défunt, détenues par sa complémentaire santé, sollicitées par ses héritiers continuant son action *post-mortem*.

données de santé du défunt s'ils sont atteints de la même maladie ; en ce cas, les données peuvent apparaître « pluripersonnelles »[169]. En résumé, pour le juge, la proximité avec le défunt n'est pas le seul critère pour lever la protection attachée à ses données, il en va de même pour sa santé.

2) Levée du secret médical du mort dans l'intérêt des héritiers

Les héritiers d'une personne pourraient avoir besoin d'accéder à son dossier médical. Aussi, la levée occasionnelle du secret médical est-elle prévue par la loi dans trois cas, lorsque les données de santé du mort sont nécessaires pour leur permettre de connaître les causes de la mort, pour défendre la mémoire du défunt ou faire valoir leurs droits[170]. Il en va ainsi pour faire établir un décès lié à un accident du travail ou de maladie professionnelle ou pour obtenir versement des sommes dues au titre d'un contrat d'assurance sur la vie, d'assurance emprunteur ou accidents corporels prévoyant le versement de prestations en cas de décès accidentel de l'assuré. L'article L. 1110-4, V du code de la santé publique prévoit en effet que ne contrevient pas au secret médical la transmission d'informations concernant une personne décédée à ses ayants droit. Or, définir ces ayants droit a donné lieu à contentieux. Dans un établissement exerçant une mission de service public hospitalier, public ou privé, ils sont les « successeurs légaux du défunt, conformément au code civil »[171], qui sont en rang éligible pour recevoir la succession[172], tandis que dans les autres établissements de santé, les ascendants,

169 - Groupe de travail « article 29 », *Avis 4/2007 sur le concept de données à caractère personnel*, p. 24-5.

170 - CSP, art. L. 1110-4, I al. 2 posant que seule la loi peut prévoir des dérogations au secret médical. V. CSP, art. L. 1111-7, R. 1111-7 sur le principe de l'accès au dossier médical par la personne et après son décès par ses ayant droits, son concubin ou son partenaire lié par un pacte civil de solidarité.

171 - Arrêté du 3 janv. 2007 *portant modification de l'arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès*, JO 16 janv. 2007, p. 982, texte n° 32, art. 1.

172 - Il ne faut donc ne pas être primé dans l'ordre de succession ou par un successeur testamentaire, V. CADA, avis n° 20114359, 17 nov. 2011 ; avis n° 20121675, 5 avr. 2012 ; avis n° 20094325, 22 déc. 2009.

descendants et le conjoint sont inclus[173]. Pour faciliter leur accès, le concubin, le partenaire lié par un pacte civil de solidarité[174], et le mineur ont été ajoutés à la liste en 2016[175]. Il est à noter que la Commission d'accès aux documents administratifs s'est montrée favorable à la transmission de données de santé enregistrées numériquement pour connaître la cause du décès d'un proche, père ou enfant[176]. Seules les informations du dossier médical nécessaires à l'objectif poursuivi peuvent être communiquées aux ayants droit ou au survivant du couple d'une personne décédée[177]. Par suite, la requête du demandeur devra préciser le motif pour lequel il « a besoin d'avoir connaissance de ces informations », tandis que le refus d'accéder à la requête devra être motivé ; un certificat médical pouvant néanmoins être transmis sans comprendre d'information portant atteinte au secret médical[178]. De son vivant, la personne a pu valablement faire obstacle à une telle communication en s'opposant à la levée du secret médical après sa mort, comme le lui permet

173 - D. Poisson, « Que devient le secret médical après le décès d'une personne ? », *Laennec* 2007/1, Tome 55, p. 49, spéc. p. 56 renvoyant à la jurisprudence de la Cour de cassation.

174 - Les couples non mariés se heurtaient à l'exigence d'avoir la qualité d'ayant droit ou de légataire universel pour avoir accès aux informations médicales V. CADA, avis n°20024128, 17 oct. 2002 ; CADA, avis n° 20041100, 18 mars 2004 ; Cass. 1ère civ, 1er juin 2016, n° 15-16486 ; obs. A. Bodénès-Constantin, *RDS* 2016, p. 929. Cette extension devrait résorber en partie la difficulté posée aux bénéficiaires d'assurance sur la vie, qui ne peuvent justifier de la qualité d'ayant droit, V. Défenseur des droits, déc. 26 nov. 2013, n° MSP 2013-209 portant recommandations relatives aux conditions d'accès pour les bénéficiaires de contrat d'assurance sur la vie.

175 - Loi n° 2016-41 du 26 janv. 2016 *de modernisation de notre système de santé*, JO 27 janv. 2016, n°0022, texte n° 1, art. 96. Déjà pour les mineurs, CADA, avis n° 201000382, 28 janv. 2010 ; n° 20140747, 27 mars 2014.

176 - CADA, avis n° 20141338, 19 juin 2014 favorable à la communication à l'enfant des données médicales contenues dans le défibrillateur cardiaque du père, refusée par le centre hospitalier ; avis n° 20140747, 27 mars 2014 favorable à la communication des informations contenues dans les dossiers médicaux d'une mère et de son enfant décédé, prenant acte de l'intention de l'hôpital de lui communiquer les échographies sous forme numérique.

177 - CE, 26 sept. 2005, *Conseil national de l'ordre des médecins*, n° 270234 ; Lebon 2005, p. 395 ; *AJDA* 2006, p. 308, note J.-P. Markus ; *RDSS* 2006, p. 53 note D. Cristol mettant fin à la pratique antérieure de communication de l'ensemble du dossier médical, annulant les dispositions de l'arrêté du 5 mars 2004 *portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, JO* 17 mars 2004, p. 5206. V. D. Poisson, *op. cit.*, p. 55-7.

178 - CSP, art. R. 1111-7, modifié par le Décret n° 2016-994 du 20 juil. 2016, art. 2.

le code de la santé publique[179]. La mère accouchant secrètement dispose également de la faculté de faire obstacle à l'accès à ses données *post-mortem*.

C. Accès aux origines tenues secrètes après le décès des père et mère de naissance

L'identité civile de la personne, à finalité identificatoire, est organisée par l'État au travers de l'état civil des personnes[180]. Cette identité civile, qui la singularise à l'égard des autres, se double d'une identité psychologique, autrement appelée ipséité, dont la visée est identitaire[181]. La volonté des géniteurs de dissimuler leur identité et leurs données personnelles doit s'articuler avec les droits reconnus à l'enfant né sous le secret. En parallèle du lien juridique étatique s'est donc construit un droit à une information sur des éléments de son histoire individuelle, contribuant à se définir personnellement. Ce droit à la connaissance d'éléments identitaires importants s'articule alors avec l'identité civile[182]. Ces deux plans sont présents en droit positif.

En premier lieu, l'article 326 du code civil permet de conserver le secret de l'identité d'une femme admise en vue de son accouchement dans un établissement de santé. Afin d'éviter la condamnation de ce dispositif par la Cour européenne des droits de l'homme, la loi du 22 janvier 2002 instaura la réversibilité du secret de l'identité de la mère et du père biologique, dont la parenté avait été tenue

179 - CSP, art. L. 1110-4, V ; V. CADA, avis n° 20140311, 27 mars 2014 favorable à la communication du dossier médical au fils, en raison du doute sur l'authenticité de l'opposition de la mère transmise par l'établissement de santé.

180 - Convention des nations Unies relative aux droits de l'enfant, signée à New-York le 20 nov. 1989, art. 7 à 9 posant que tout enfant est enregistré dès sa naissance, dispose du droit à un nom et à acquérir une nationalité.

181 - D. Deroussin, Éléments pour une histoire de l'identité individuelle, *L'identité, un singulier au pluriel*, B. Mallet-Bricout, T. Favario (Dir), Dalloz coll. Thèmes et commentaires, 2015, p. 7, spéc. p. 7 citant P. Ricoeur relevant que « contrairement à la mêmeté que le droit aborde, l'ipséité consiste dans la construction par le récit, d'une identité personnelle qui est le résultat d'une "interprétation de soi" » et notant une évolution d'une conception objective vers une conception subjective, prenant en compte la volonté de l'individu ; P. Murat, L'identité imposée par le droit et le droit à connaître son identité, *L'identité (...)*, *op. cit.*, p. 51, spéc. p. 51-2.

182 - P. Murat, *op. cit.*, spéc. p. 56.

secrète[183]. Elle autorise expressément la transmission de l'identité du géniteur après sa mort. En d'autres termes, la loi présume l'accord implicite du parent de naissance pour la communication de son identité après son décès, si l'enfant devenu majeur en demande communication ; par exception, le géniteur aura pu exprimer une volonté contraire lors d'une demande d'accès aux origines en s'y opposant valablement. Ce système a été considéré comme ne contrevenant à aucun droit ou liberté garantis par la Constitution[184]. En 2003, la Cour de Strasbourg a conclu, à la conventionnalité de la législation française, qui tentait par ces dispositifs d'atteindre un équilibre et une proportionnalité suffisante entre les intérêts en cause. Examinant le droit au respect de la vie privée prévu à « l'article 8 [de la Convention, elle proclama qu'il] protège un droit à l'identité et à l'épanouissement personnel », dans « l'intérêt vital à obtenir des informations nécessaires à la découverte de la vérité concernant un aspect important de son identité personnelle » pour l'enfant né d'un accouchement secret[185]. Pour épuiser la discussion, notons que le droit français renforce l'accès à la connaissance des éléments identitaires importants, tout en l'isolant explicitement d'une action civile pour faire établir un lien de filiation, dont l'application reste autonome[186]. Gardons-nous de pousser le « droit à connaître son ascendance », dégagé de l'article 8 de la Convention par le juge de Strasbourg, vers l'absolutisme biologique du droit de faire reconnaître légalement le lien de filiation lui-même à l'encontre des

183 - Loi n° 2002-93 du 22 janv. 2002 *relative à l'accès aux origines des personnes adoptées et pupilles de l'Etat,* JO 23 janv. 2002, p. 1519, texte n° 2. V. CASF, art. L. 147-6.

184 - Cons. Const. 16 mai 2012, QPC 2012-248, obs. critique C. Neirinck, « Le Conseil constitutionnel, l'accouchement secret et l'accès aux origines personnelles de l'enfant », *Dr. famille* 2012, comm. 120, soulignant le caractère éminemment politique de la législation, préservant la volonté hégémonique de la mère.

185 - CEDH, gde ch.,13 févr. 2003, *Odièvre c/ France,* nº 42326/98, § 29 mettant en balance, § 44-5 et 49, l'intérêt de l'enfant, avec celui d'une femme à conserver l'anonymat pour sauvegarder sa santé en accouchant dans des conditions médicales appropriées, et la protection des tiers, parents adoptifs, père et famille biologique, outre l'intérêt général de protéger le droit à la vie. Comp. CEDH, 25 sept. 2012, *Godelli* c/ *Italie,* n° 33783/09, § 66, 68, 70, 71 jugeant la législation italienne sur l'accouchement secret non conforme à la protection de la vie privée, comme excluant toute réversibilité du secret de l'identité de la mère de naissance et tout accès aux informations non identifiantes.

186 - CASF, art. L. 147-7 posant que « L'accès d'une personne à ses origines est sans effet sur l'état civil et la filiation. Il ne fait naître ni droit ni obligation au profit ou à la charge de qui que ce soit ».

textes législatifs[187]. En pratique, pour favoriser l'accès à l'identité des géniteurs, en 2014, un rapport a proposé de renforcer le dispositif en organisant le recueil systématique de l'identité maternelle lors de l'accouchement, au lieu de la simple invitation actuelle[188] ; *de facto*, si son nom n'est pas enregistré, elle ne peut jamais être contactée pour une éventuelle levée du secret de son vivant ou après son décès. Du reste, une atteinte à la mémoire de la personne décédée peut résulter de la divulgation soudaine à ses proches de l'existence d'un enfant, dont il ne pourra expliquer les circonstances de la naissance et de l'abandon[189].

En second lieu, la modification du dispositif légal opérée en 2012 montre un glissement de l'accouchement secret vers le droit à connaître des éléments identitaires importants. Le législateur avait décidé de renforcer les informations transmises à la parturiente en insistant sur « l'importance pour toute personne de connaître ses origines et son histoire » et la possibilité de transmettre, si elle l'accepte, son identité sous pli fermé, dès la naissance ou ultérieurement, et celle du père de naissance. En outre, il lui est proposé de confier des « renseignements ne portant pas atteinte à l'identité des père et mère de naissance », qu'elle pourra par la suite compléter[190]. En ce sens, le Ministère de la Santé a prévu un modèle type de document, sous la forme d'un questionnaire, sur lequel le correspondant du Conseil national pour l'accès aux origines personnelles recueille les

187 - P. Murat, *op. cit.*, p. 62-3 relevant l'oscillation du juge de Strasbourg entre ces positions ; F. Chénedé, P. Deumier, « L'œuvre du Parlement, la part du Conseil constitutionnel en droit des personnes et de la famille », *op. cit.*, spéc. IV.

188 - A. Gouttenoire, I. Corpart, *Quarante propositions pour adapter la protection de l'enfance et l'adoption aux réalités d'aujourd'hui*, Rapport remis en févr. 2014 à Mme Bertinotti, ministre déléguée à la famille, p. 96-8.

189 - M.-C. Le Boursicot, « L'accès aux origines personnelles », *RLDC* 2004/5, p. 43, spéc. IIB.

190 - CASF, art. L. 222-6 ; art. L. 147-6 et R. 147-16 prévoyant le recueil de ces éléments auprès des père et mère de naissance, par un membre du Conseil national pour l'accès aux origines personnelles (CNAOP), une personne mandatée par lui, ou les établissements de santé et services départementaux, dans le respect de la vie privée des personnes et de la confidentialité des informations. Sur les conditions de traitement et de conservation des données collectées par le CNAOP, Décret n° 2003-671 du 21 juil. 2003, JO 24 juil. 2003, p. 2487, texte n° 29.

informations[191]. De manière très intéressante, la Cour de Strasbourg a observé, dans l'affaire jugée en 2003, que si la requérante française n'avait pu obtenir l'identité maternelle, elle avait eu « accès à des informations non identifiantes sur sa mère et sa famille biologique lui permettant d'établir quelques racines de son histoire dans le respect de la préservation des intérêts des tiers »[192]. On peut y voir une forme de réponse – certes limitée – à sa quête identitaire. Mais la qualification de données non identifiantes employée par le juge est équivoque. Au contraire, les informations sur la santé, la situation de famille, les caractéristiques physiques peuvent être indirectement identifiantes par recoupements. Elles présentent la nature de données personnelles, s'intégrant dans la catégorie des données sensibles spécifiquement protégées pour les antécédents de santé[193].

§2 : Articulation rénovée des droits du mort et des vivants sur les données

L'article 85 de la loi de 1978 protège tout individu. Son champ n'est pas restreint à ceux qui auraient développé une notoriété particulière dans les arts et spectacles, la politique, les affaires, ou encore les popularités nouvelles issues de l'Internet. Il s'agit de protéger la majorité de la population française, qui a désormais une présence

191 - Arrêté du 14 févr. 2005 *fixant le modèle du document établi en application de l'article 23 du décret n° 2002-781 du 3 mai 2002 relatif au Conseil national pour l'accès aux origines personnelles et à l'accompagnement et l'information des femmes accouchant dans le secret*, JO 3 mars 2005, p. 3740, texte n° 12 renvoyant au document type publié au Bulletin officiel du ministère de la Santé n° 2005/3, p. 268-70, <http://solidarites-sante.gouv.fr/fichiers /bo/2005/05-03/bo0503.pdf>, y figure sur la mère et le père de naissance des questions sur la santé, les antécédents familiaux, âge, nationalité, pays d'origine et pays de résidence, situation de famille, enfants déjà nés, présence d'une famille proche, aspect physique (taille, couleur des yeux, des cheveux), profession ou niveau d'études et une rubrique libre à renseigner intitulé « autres ». Un espace libre pour indiquer « les raisons et circonstances de la remise de l'enfant », figure encore des questions portant sur l'information du père : « le père était-il informé : de la grossesse ? de la date présumée de l'accouchement ? de la décision prise par la mère à la naissance ? ».

192 - *Ibid.*, § 48. La loi les nomme « renseignements ne portant pas atteinte à l'identité des père et mère de naissance ».

193 - Groupe de travail « article 29 », *Avis 4/2007 sur le concept de données à caractère personnel*, p. 6-7 et 13.

en ligne sur les réseaux numériques[194] et pour certains une activité intense dans l'Internet dit participatif, *web* 2.0. La loi n'opère de distinctions sur le sort des données après le décès d'une personne, que selon qu'elle a ou non anticipé son trépas. Le nouveau dispositif prévoit la transmission des directives volontairement adoptées par le défunt *ante-mortem*, mais il a entrepris d'organiser en faveur de ses héritiers un accès *post-mortem* aux données du défunt en l'absence de mesures prises par lui. Après son décès, entrent en application l'organisation volontariste du sort des données personnelles du mort dans le cadre annoncé par la loi (A), ainsi que l'organisation supplétive les régissant en l'absence de toute prévision ou pour les pans que le défunt n'aurait pas envisagés (B).

A. Les missions définies par la loi : protection et accès aux données *a minima*

L'article 85 II de la loi de 1978 instaure des règles générales destinées à permettre aux héritiers d'intervenir sur les données personnelles de leur auteur décédé, s'il n'a pas pris de mesures spécifiques. Plutôt que l'ordre du texte, retenons une approche chronologique du renforcement des droits sur les données. Dès 2004, des droits avaient été ponctuellement reconnus aux héritiers pour faire prendre acte du décès de la personne concernée par un traitement par le responsable de celui-ci, ces mesures dans l'intérêt du défunt sont reconduites et approfondies (1). Progressivement, certains dispositifs financiers avaient pris en compte le décès d'une personne et le besoin de récupérer les avoirs de leur auteur pour ceux laissés à sa survivance. L'innovation principale de la loi est de prévoir des mesures dans l'intérêt des héritiers en leur accordant des droits d'accès en vue du règlement successoral. Il est complété d'une disposition innovante sur la communication des biens numériques et le renvoi aux souvenirs de famille, qui mérite attention (2), tandis qu'est précisée la compétence juridictionnelle en cas de conflits entre héritiers (3).

194 - Montée du taux d'utilisation régulière d'Internet de 55 % à 83% entre 2007 et 2017 (de 51 à 79% dans l'Union) et des réseaux sociaux (Facebook, Linkedin...) de 38 à 45 % des 16 à 74 ans entre 2011 et 2017 (de 40 à 56 % de l'Union), 78 % des 16-24 ans français s'y connectaient en 2017 (Union : 88 %). <https://ec.europa.eu/eurostat/ statistics-explained/index.php?title=Category:Digital_economy_and_society_statistics_by_area_and_region>.

1) Promouvoir la prise en compte du décès par le responsable de traitement

Première étape dans la prise en compte de la continuation du traitement de données *post-mortem*, la loi du 6 août 2004 avait ajouté les alinéas 5, 6 et 7 à l'article 40 de la loi du 6 janvier 1978 afin de permettre aux héritiers, justifiant de leur identité, d'intervenir pour faire actualiser un traitement de données à caractère personnel concernant une personne décédée[195]. Cependant, aucun droit d'accès aux données ne leur était reconnu. Il était attendu du responsable d'une plateforme « qu'il ferme ou désactive le compte en question » d'après Maître Cahen, mais sans que les héritiers ne puissent l'imposer selon la Commission nationale de l'informatique et des libertés ; les réseaux sociaux et fournisseurs de messageries électroniques les plus connus avaient mis en ligne des plateformes de suppression ou de désactivation des profils des personnes décédées à destination de leurs proches[196]. Reformulant la faculté de « faire procéder » à la « mise à jour » des données, le nouvel article 85 II de la loi de 1978, confirme le droit des héritiers de contrôler l'actualisation des données de la personne défunte, en enjoignant au responsable de traitement de justifier qu'il a rempli sa mission, sans avoir à débourser de frais[197]. Pour le responsable de traitement, il n'en ressort pas forcément la partition entre données des personnes vivantes et décédées dans son architecture informatique[198].

195 - Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JO 7 août 2004, p. 14063, texte n° 2 si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées les héritiers pouvaient exiger du responsable de traitement qu'il prenne acte du décès et procède aux mises à jour.

196 - M. Cahen, « Identité et mort numérique », <https://www.murielle-cahen.com/publications/mort-numerique.asp>, spéc. IIA ; CNIL, *Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ?*, 29 oct. 2014,<https://www.cnil.fr/fr/mort-numerique-peut-demander-leffacement-des-informations-dune-personne-decedee-0> citant les liens vers certaines procédures de suppression de comptes ; v. *supra* sect. 2, §2 A2, B1.

197 - C. pén., art. R. 625-12 punissant d'une contravention de 5e classe le fait pour un responsable de traitement de ne pas procéder aux demandes de rectification, mise à jour, effacement émanant d'une personne ou de son héritière.

198 - Groupe de travail « article 29 », *Avis 4/2007 sur le concept de données à caractère personnel*, p. 24-5 notant qu'en pratique il sera plus facile de traiter « les données relatives aux personnes décédées dans les conditions imposées par les règles de protection des données, plutôt que de séparer les deux ensembles de données ».

En outre, allant bien plus loin que le dispositif primitif abrogé (Anc. art. 40, al. 5 à 7), la loi innove en introduisant un droit d'opposition *post-mortem,* permettant aux héritiers de déclarer « s'opposer à la poursuite des traitements de données à caractère personnel » concernant le défunt[199]. Le droit d'opposition au traitement des données personnelles s'analysant comme un droit attaché à la personne elle-même, on comprend la tiédeur du législateur, qui considéra longtemps comme « incertaine » la légitimité des héritiers à l'exercer, et ce bien que le traitement des données d'une personne décédée puisse affecter la vie privée de ses ayants droit[200]. Enfin, à l'invitation de la Commission nationale de l'informatique et des libertés[201], fut encore ajouté un droit de rectification pour « faire procéder à la clôture des comptes utilisateurs du défunt » par les héritiers. Cet absolutisme, qui pourrait surprendre en l'absence de directives explicites d'y procéder, répond à la problématique du « droit d'être oublié *post-mortem* »[202]. Faire clôturer le compte reste un pouvoir minimal de protection du défunt lorsque l'héritier n'est pas investi de la faculté d'accéder à son contenu par le défunt. L'héritier n'en récupérera pas le contenu sauf si les prévisions légales le lui permettent au titre du règlement successoral ou de la communication des biens numériques.

2) Favoriser l'organisation et le règlement de la succession pour les héritiers

Avant l'introduction de l'article 40-1 dans la loi informatique et liberté en 2016, un accès des héritiers aux données du mort se rapportant à ses avoirs financiers avait pu émerger de différents textes et de décisions leur conférant la qualité de « personnes concernées » par le traitement de données (a). Si la loi nouvelle entérine ce mouvement en édictant le maintien temporaire des droits proclamés par la loi de 1978 en l'absence de directive de la personne décédée, encore

199 - E. Florestal, R. Perray, obs. sur CE, 29 juin 2011 ; *RLDI* 2015/3, p. 42, spéc II en faveur d'une « autonomisation d'un droit des héritiers à s'opposer aux traitements des données personnelles du défunt ».

200 - J. Frayssinet, Ph. Pedrot, *op. cit.*, n°20. Sur le droit d'opposition, v. *infra* sect. 1, §1 C1.

201 - CNIL, Délib. n°2015-414, *op. cit.*, art. 28 étudiant le projet de loi de 2015, art. 20, suggérant de les autoriser à clore comptes et profils du défunt : messageries, réseaux sociaux, sites de e-commerce ou de paiement en ligne.

202 - CNIL, Mort numérique (...), *op. cit.* ; J. Groffe, La mort numérique, *op. cit.*, n° 5-8.

faut-il déterminer les hypothèses successorales visées (b) et le sens à donner au transfert des « biens numériques et données apparentées aux souvenirs de famille » (c).

a) Accès préexistant des héritiers aux données concernant les avoirs financiers du défunt

Dans le secteur bancaire, il est fréquent d'employer procuration, mandat et convention de compte-joint pour faciliter l'accès d'un tiers au compte d'une personne de son vivant et même *post-mortem*. Trois limites s'imposent alors : respecter les stipulations contractuelles, l'ordre public successoral[203] et qu'il n'y ait pas de contestation judiciaire des héritiers[204]. Le principe du secret bancaire auquel est tenu un établissement de crédit ne disparaît pas à la mort du client et perdure au profit des personnes munies de procurations, pour faire fonctionner le compte ; le banquier ne révèlera pas leur nom aux tiers[205]. Les difficultés se dressent au décès pour les héritiers qui ne disposent pas d'un tel mandat de gérer le compte ou de l'accès aux identifiants[206]. Néanmoins, continuateurs de la personne du défunt, les héritiers désignés par la loi sont, de plein droit, investis des biens, droits et action du défunt, par l'article 724 du code civil. Le secret bancaire leur sera inopposable, sauf pour les documents que la banque détiendrait relativement à la vie privée du défunt[207] et ils devraient obtenir sans entrave communication des contrats d'assurance sur la vie qu'il a souscrits[208]. Différents

203 - Cass. 1ère civ., 28 juin 1988, n° 86-13639, *préc.* jugeant qu'un mandat *post-mortem* ne peut contrevenir à l'ordre public successoral en prévoyant que la compagne du défunt retirera les fonds en compte à son décès.

204 - Cass. ass. plén., 4 juill. 1985, n° 83-17155 ; Bull. ass. plén. n° 4 ; JCP G 1985. II. 20457, rap. A. Ponsard jugeant que le conjoint survivant fait fonctionner le compte-joint sauf opposition des héritiers (C. civ., art. 221).

205 - CMF, art. L. 511-33 ; Cass. com., 25 févr. 2003, nº 00-21184 ; Bull. n° 26 rejetant la demande de la Caisse nationale d'assurance vieillesse envers une banque de fournir les coordonnées d'une personne ayant procuration sur le compte d'un défunt, sur lequel elle virait sa retraite, pour agir en répétition de l'indu.

206 - D. Guérin, « Les procurations bancaires données par les personnes âgées », *Revue de Droit bancaire et financier* 2016, étude 22, spéc. n°36 relevant que souvent après décès d'un époux les enfants ont procuration sur les comptes.

207 - Douai, 8 févr. 2018, n°17/04470 ; *LEDB* avr. 2018, n° 111f5, p. 2, obs. J. Lasserre Capdeville.

208 - P. Cénac, N. Laurent-Bonne, C. Mochkovitch, « Contentieux de l'assurance-vie Regards croisés avocat-notaire », *JCP E* 2018, 1146, spéc. n°8-12 favorables à la levée du secret bancaire.

aménagements facilitèrent l'exercice des droits des héritiers, tels la faculté de prélever les frais de funérailles sur le compte bancaire du défunt, de le clore parfois, d'interroger le fichier des comptes bancaires, ou de rechercher les fonds non attribués.

Dans l'arsenal législatif des mesures de facilitation du deuil, l'accès aux données bancaires et aux comptes du défunt présente un enjeu de politique familiale[209]. Depuis 2013, la loi autorise la « personne ayant qualité pour pourvoir aux funérailles du défunt » d'obtenir le débit sur les comptes de paiement du défunt des sommes exposées pour l'organisation des obsèques[210]. Renforçant encore les droits des héritiers, la loi leur permet en outre de clôturer le compte bancaire du défunt pour les successions les moins élevées lorsqu'il n'existe ni testament, ni contestation sur la qualité d'héritier[211]. Les héritiers peuvent donc dans les cas énoncés exercer les prérogatives d'accès et de rectification des données personnelles de leur auteur mort.

Par ailleurs, dès 2011, le Conseil d'État avait reconnu qualité de « personne concernée », au sens des articles 2 et 39 de la loi de 1978, aux héritiers qui recevaient les soldes des comptes bancaires de leur tante défunte, et tentaient d'établir la « dette fiscale de la succession et de liquider celle-ci »[212]. Ils pouvaient donc demander par l'entremise de la Commission nationale de l'informatique et des libertés à accéder au Fichier des comptes bancaires (FI.CO.BA), tenu par un service de l'administration fiscale, qui répertorie les établissements teneurs de comptes et leurs titulaires, sans communiquer les soldes de provision. La loi a consacré cette avancée, depuis le 1er janvier 2016, pour liquider une succession, les héritiers en rang éligible, ainsi que les notaires mandatés par eux, peuvent saisir directement l'administration fiscale d'une demande de communication de la liste des comptes détenus

209 - Rép. Min. n°73229, JOAN Q, 15 juil. 2015, p. 5455.

210 - Loi n° 2013-672 du 26 juil. 2013 de séparation et de régulation des activités bancaires, JO 27 juil. 2013, p. 12530, texte n° 1, art. 72. V. CMF, art. L. 312-1-4 exigeant trois conditions, production d'une facture, honorée dans le respect de la double limite du solde créditeur du compte et d'un montant maximal fixé à ce jour à 5.000 €

211 - Loi n° 2015-177 du 16 févr. 2015 *relative à la modernisation et à la simplification du droit et des procédures dans les domaines de la justice et des affaires intérieures*, JO 17 févr. 2015, p. 2961, texte n° 1, art. 4 insérant quinze nouveaux alinéas à l'article L. 312-1-4 du code monétaire et financier.

212 - CE, 29 juin 2011, *préc*. Tout ayant droits du défunt n'est pas une personne concernée, *infra* sect. 2, §1 B1.

par la personne décédée[213]. Notons que les héritiers ne pourront pas établir la consistance de l'actif successoral en sollicitant le dossier de contribuable du défunt[214], dont la communication n'est prévue qu'à l'intéressé. Le secret professionnel s'impose à tout intervenant au titre du calcul, recouvrement et du contentieux fiscal au sens du code général des impôts[215]. À titre exceptionnel, les héritiers y auront néanmoins accès s'il leur est demandé de s'acquitter du passif fiscal du défunt et que les documents sollicités permettent d'établir l'existence et le montant de la dette fiscale afin de liquider la succession[216]. Deux mécanismes facilitant le règlement successoral et la transmission des biens après décès sont encore à relever : la recherche centralisée des avoirs financiers du défunt – comptes bancaires, produits d'épargne, assurance sur la vie – et celle des bénéfices de contrats d'assurance sur la vie non réclamés après décès de l'assuré[217]. Ces mesures favorisant l'accès aux avoirs financiers du défunt relativisent nettement l'intérêt des dispositions nouvelles de l'article 85 II de la loi de 1978 pour faciliter le règlement successoral.

b) Nouvelles mesures habilitant les héritiers du défunt

L'hybridation du nouveau dispositif légal entre deux objectifs distincts de protection des données attachées à la « personne » et de transmission de « biens » numériques montre une nouvelle fois ses limites. Avant 2016, il était acquis que les droits reconnus par la loi *Informatique et libertés* aux personnes concernées par un traitement de leurs données personnelles – accès, rectification et suppression,

213 - Loi n° 2014-617 du 13 juin 2014 *relative aux comptes bancaires inactifs et aux contrats d'assurance vie en déshérence*, JO 15 juin 2014, texte n°1, art. 8 modifiant LPF, art. 151 B. Pour les titulaires de comptes eux-mêmes, l'accès reste indirect, soit 1729 saisines en 2017, v. CNIL, *38ème Rapport annuel 2017*, mai 2018, p. 68-9.

214 - CADA, avis n° 20045390, 3 mars 2005 ; avis n° 20070219, 11 janv. 2007 (affaire jugée par CE, 29 juin 2011).

215 - LPF, art. 103 renvoyant à C. pen., art. L. 226-13 et 14. Les tiers, y compris le conjoint, essuieront un refus s'ils sollicitent communication des éléments fiscaux d'un contribuable, v. CADA, avis n° 20014972, 20 déc. 2001.

216 - CADA, avis, 15 oct. 1981, 2ème rapport d'activité 1981-1982, p. 17.

217 - V. le dispositif Ciclade, issu de la loi du 13 juin 2014 pour rechercher les avoirs financiers du défunt, <https://ciclade.caissedesdepots.fr/quest-ce-que-ciclade>. Et déjà, la consultation de l'association AGIRA pour connaître l'existence de tout contrat d'assurance sur la vie souscrit par le défunt en faveur de la personne formulant la requête, <http://www.formulaireassvie.agira.asso.fr/> ; un notaire peut être mandaté à cette fin (LPF, art. L. 151 B).

opposition – sont des droits de nature personnelle viagers en sorte qu'ils s'éteignent par la mort. Rappelant ce principe d'extinction au décès des droits sur les données personnelles, l'article 84 de la loi de 1978 maintient toutefois « provisoirement » leur exercice. Ce caractère temporaire interroge, s'expliquerait-il pour leur survie limitée au temps du règlement successoral, si aucune directive n'a été prise par le défunt *ante-mortem*[218] ? Il est à souligner que le législateur a fortement encadré l'exercice de droits « personnels » du défunt par ses héritiers, s'il n'avait pas pris de directives, suivant les recommandations de la Commission nationale de l'informatique et des libertés[219]. Selon la loi nouvelle, en l'absence de directives volontairement prises par la personne concernée par le traitement de données, ses héritiers ne « peuvent exercer après son décès les droits mentionnés à la présente section [que] dans la mesure nécessaire : - à l'organisation et au règlement de la succession du défunt ». Et de préciser « 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 ». Cette faculté est attribuée à la catégorie juridique des héritiers, à savoir au légataire universel tenant ses droits d'un testament ou aux héritiers suivant l'ordre légal. Lors des débats législatifs, il fut un temps proposé de classer les héritiers comme pour divulguer les œuvres posthumes, faute d'exécuteur testamentaire[220]. Mais, l'ordre du modèle était daté, faisant primer les descendants sur l'époux marié non divorcé, ignorant tant le renforcement des droits du conjoint survivant depuis 2001 que les couples non mariés. De surcroît, il était inadéquat pour les données personnelles, ne révélant aucune œuvre et supposant, au contraire, d'administrer les informations déjà dévoilées.

218 - Pourquoi ce maintien des droits est-il aussi dit provisoire si le défunt prend des directives supposées durables ?

219 - CNIL, Délib. n°2015-414, 19 nov. 2015, *op. cit.*, art. 28 étudiant le projet de loi de 2015, art. 20, ayant prévu sans restriction que les « héritiers peuvent exercer après son décès les droits mentionnés à la présente section », jugeant qu'un accès trop ouvert causerait des difficultés liées à la révélation de secrets (vie privée, professionnelle). L'accès aux données devrait être admis quand il est nécessaire pour identifier l'actif successoral d'une personne.

220 - Proposition issue de la Contribution du Conseil supérieur du notariat, observations sur la mort numérique (art. 20), *op. cit.*, renvoyant à CPI, art. L. 121-2. V. C. Pérès, *op. cit.*, n°13-14 critiquant la version du projet l'ayant retenue.

Seuls des droits minimaux d'accès aux données du défunt sont accordés par la loi aux héritiers pour régler la succession. Il n'y a pas de transmissibilité de l'accès à toutes les données du mort, en l'absence de directives[221]. Bien plus, on s'interroge sur la nature des droits reconnus par le nouveau texte. Est-ce que les héritiers exercent leurs droits propres sur les données du défunt qu'ils administrent ? Seraient-ils investis d'un mandat légal, solution plus conforme au caractère personnel des informations[222], que la transmission au titre du droit des biens par succession ? On craint de gauchir la nature personnelle des droits exercés sur les données.

Il est délicat d'établir la ligne de partage entre les données pertinentes ou non pour le règlement successoral. Prenons deux illustrations avec les soldes financiers en faveur du défunt et ses correspondances. Tout d'abord, il pourra être excipé de l'article 85 II de la loi de 1978 au soutien du paiement d'une dette contractuelle à la succession du défunt, pour le paiement de laquelle serait invoquée la continuation de la personne défunte sur le terrain du code civil[223]. L'absence d'identifiant et mot de passe pourrait être opposée par le site à titre dilatoire sans remettre en cause les suites contractuelles, toutefois délicates à mettre en œuvre[224]. Ainsi devraient pouvoir être récupérés par les héritiers les soldes financiers créditeurs des comptes sur les sites de commerce ou de paiement en ligne (rechargement d'une somme sur un compte *Amazon* pour régler les achats, solde d'un compte de revendeur sur un site en ligne (*market place*, *Paypal*), un compte de jeu (pari, *e-sport* vidéo...), une application de téléphone mobile, ou les fonds placés sur une *fintech* proposant des services de gestion de patrimoine. La pratique dira si les opérateurs jouent le jeu de la République numérique en remboursant les sommes ou si les juridictions devront être saisies en cas de refus persistant. En outre, le blocage pourra-t-il être dépassé

221 - L. Castex, E. Harbinja, J. Rossi, « Défendre les vivants ou les morts ? » (...), *op. cit.*, p. 137.

222 - Sur le modèle du droit matrimonial laissant le conjoint agir à la place de son époux empêché, pour exercer des droits qui ne lui appartiennent pas sous contrôle judiciaire ou sur son mandat tacite (C. civ., art. 217 à 219).

223 - En paiement des créances du défunt, les héritiers peuvent toujours se prévaloir de la continuation de la personne de l'article 720 du code civil ; l'article 1122 du code sur la stipulation pour soi et ses ayants droit fût abrogé en 2016.

224 - C. Béguin-Faynel, « Pour un testament des dernières volontés numériques (...) », *op. cit.*, p. 67, spéc. p. 77.

en l'absence de directives quand il n'existe pas de pouvoir centralisé pouvant déverrouiller l'accès au compte sans les codes d'accès, comme pour les comptes de cryptomonnaies (*Bitcoin*, *Ether, Ripple*...)[225] ou coffre-fort numérique[226] ? Ensuite, si le règlement successoral dépendait du contenu des courriels du défunt, ses héritiers pourraient-ils y accéder sans avoir été investis du droit d'accès au compte de messagerie électronique par des directives du défunt sur le sort de ses données *post-mortem* ? Loin d'être pure conjecture, le refus d'accès opposé par l'opérateur est probable. La politique des entreprises américaines dominant l'Internet est de refuser l'accès aux héritiers en dehors des cadres qu'elles ont organisés dans leurs conditions d'utilisation. En 2017, la Cour suprême de l'État américain du Massachusetts a considéré que la loi fédérale, *Stored Communications Act*, opposée par l'opérateur de messagerie Yahoo, ne faisait pas obstacle à ce que les représentants de l'hérédité d'une personne aient accès à son compte de courrier électronique ; il revenait à la *Probate court*, tribunal en charge des successions, de déterminer si Yahoo devait ou non conférer cet accès en l'espèce[227]. Le 12 juillet 2018, la Cour fédérale allemande a également permis aux parents d'une jeune fille décédée d'accéder à son compte Facebook, estimant que les données dont le réseau refusait la consultation appartenaient à un « compte utilisateur » et non à une personne spécifique. Ce faisant, elle censure l'arrêt de la Cour d'appel de Berlin qui les avaient déboutés en faisant

225 - B. Cormier, « Un milliard de dollars de cryptomonnaie disparaissent avec leur propriétaire », 28 mai 2018, <https://www.tomshardware.fr/articles/cryptomonaie-mort-proprietaire-password,1-67636.html> relevant que la famille, de M. Mellon, milliardaire en cryptomonnaie, n'avait pu revendiquer sa fortune, faute des mots de passes des comptes « impossibles à décrypter autrement ». Sur le cours de 198 monnaies, <https://crypto-monnaie.pro/>.

226 - Décret n° 2018-418 du 30 mai 2018 *relatif aux modalités de mise en œuvre du service de coffre-fort numérique, préc.*, art. 55 permettant de prévoir l'accès au coffre à des personnes désignées.

227 - N. Raymond, *Massachusetts court : Yahoo can give dead man's emails to siblings*, 16 oct. 2017, <https://www.reuters.com/article/us-massachusetts-yahoo/massachusetts-court-yahoo-can-give-dead-mans-emails-to -siblings-iduskbn1cl2j4>, citant *Massachusetts Supreme Judicial Court*, 16 oct. 2017, *J. Ajemian's estate*.

prévaloir le secret des télécommunications.[228] En France, le secret des correspondances protège tant les lettres missives que les communications électroniques et s'impose aux opérateurs exploitant un réseau de communications électroniques ouvert au public, ainsi qu'à tous les « fournisseurs de services de communication au public en ligne permettant à leurs utilisateurs d'échanger des correspondances » depuis la loi du 7 octobre 2016. Il se conjugue en outre avec la répression pénale des atteintes au secret et la protection civile de la vie privée pour interdire la production de courriers émanant d'une personne défunte sans l'accord du destinataire[229]. Il n'est pas certain qu'en l'absence de directives expresses, le nouvel article 85 II de la loi du 6 janvier 1978 suffise à permettre l'accès des héritiers aux courriels du mort. Un argument de poids pourrait toutefois être trouvé dans la jurisprudence récente ayant dégagé un droit à la preuve dans des contentieux de règlements successoraux. La Cour de cassation a admis que le secret des correspondances et le respect de la vie privée puissent être mis en balance avec les droits des héritiers ayant survécu au défunt. Produire en justice une note de la personne décédée portant atteinte à la vie privée de personnes vivantes se révèle admissible, à supposer « la nécessité de la production litigieuse quant aux besoins de la défense et sa proportionnalité au but recherché »[230]. La production d'une lettre missive du défunt n'est envisageable que de manière très dérogatoire, le juge doit rechercher si la production litigieuse était « indispensable à l'exercice de son droit à la preuve, et proportionnée aux intérêts antinomiques en présence »[231]. La demande devra être

228 - T. Vallat, « La Cour fédérale allemande donne raison à des parents qui pourront accéder au compte Facebook de leur fille décédée », 12 juillet 2018, <http://www.thierryvallatavocat.com/2018/07/la-cour-federale-allemande-donne-raison-a-des-parents-qui-pourront-acceder-au-compte-facebook-de-leur-fille-decedee.html> ; A. Favreau, « Mort numérique en Allemagne interrogations sur la transmissibilité du contrat de fourniture de services de réseaux sociaux », *RLDC* 2017/11, p. 47, à propos de CA Berlin, 31 mai 2017, spéc *in fine* exprimant des réserves sur la transmissibilité du compte en France.

229 - CPCE, art. L. 32-3 couvrant du secret « le contenu de la correspondance, l'identité des correspondants (...) l'intitulé du message et les documents joints à la correspondance » ; C. pén., art. 226-15 ; C. civ., art 9. V. *supra*, sect. 2, §2 A2 c sur l'appartenance des courriels à la catégorie des biens numériques et souvenirs de famille.

230 - Cass. 1ère civ., 16 oct. 2008, n° 07-15778 ; Bull. n° 230 ; *RTDciv*. 2009, p. 167, note R. Perrot ; *Comm. com. électr.* 2009, comm. 70, obs. A. Lepage dans un litige sur la cession des parts sociales du mort par les héritiers.

231 - Cass. 1ère civ., 5 avr. 2012, n° 11-14177 ; Bull. n° 85 ; *Comm. com. électr.* 2012, comm. 83, obs. A. Lepage ; *Dr. famille* 2012, comm. 159, obs. M. Nicoletti ; *D.* 2012, p. 2826, D. Brezner dans un contentieux successoral.

très solidement motivée, mais un accès aux comptes de messagerie semble admissible à des fins successorales. Pour convaincre le juge, demander la nomination d'un expert pourrait être utile afin de trier le contenu de messageries dédiées ou incluses sur les réseaux sociaux numériques pour garantir une atteinte proportionnée à la vie privée des destinataires des messages toujours vivants. Pour épuiser la discussion, en octobre 2016 le législateur n'a pas créé *ex nihilo* des droits pour liquider la succession du défunt. Ces droits minimaux d'accès aux données du défunt viennent plutôt entériner les évolutions juridiques sur les avoirs financiers de la dernière décennie, qu'ils cherchent à systématiser. Un auteur averti a ainsi pu retenir qu'il aurait été plus cohérent de reconnaître aux héritiers la qualité de personne concernée si les données l'affectent[232].

c) Recevoir communication des biens numériques et données apparentées aux souvenirs de famille

Dans sa première mouture, le projet de loi *pour une République numérique* ne prévoyait pas de régir les biens numériques de la personne[233]. Toutefois, en décembre 2015, l'étude d'impact se demandait « Que deviennent les « actifs numériques » (photos, livres électroniques, musique numérique...) du défunt ? »[234]. Lors de la consultation publique sur le projet législatif en octobre 2015, le Conseil supérieur du notariat retenait que les données personnelles devraient échapper aux règles ordinaires du partage successoral, au même titre que les souvenirs de famille[235]. Des dispositions ont complété le projet, car il se révélait intéressant de déterminer

232 - A. Favreau, « L'accès des proches (...) », *op. cit.*, p. 79. Sur la qualité de personne concernée, v. *infra*, sect. 2, §1 A1.

233 - Art. 32 du projet de loi ; Art. 28 du projet de loi examiné par la CNIL, *in* Délibération n° 2015-414 du 19 nov. 2015 portant avis sur un projet de loi pour une République numérique.

234 - Étude d'impact, *op. cit.*, p. 109. Rappr. A. Favreau, « Accueil nuancé du projet de loi République numérique sur la protection des données à caractère personnel des personnes décédées », *RLDC* 2016/6, p. 26.

235 - Contribution du Conseil supérieur du notariat, observations sur la mort numérique (art. 20), *op. cit.*, déduisant qu'il serait opportun de les considérer, avec le patrimoine numérique, comme des éléments de succession anomale. Rappr. *#Familles, #solidarité, #numérique*, 113e Congrès des notaires de France, 2017, p. 889 précisant que les données personnelles qui ne sont pas apparentées à des souvenirs de famille ne devraient pas être transmises.

que faire des actifs immatériels composant le patrimoine du défunt, enrichi par « les actes de consommation dématérialisés (jeux, musique, films, jeux vidéo) »[236]. Il convenait de rétablir les équilibres en évitant l'application exclusive des conditions générales d'utilisation des services en ligne rédigées par l'opérateur numérique, dont on sait que le contractant doit les accepter en bloc sans négociation[237]. L'étude d'impact relevait que dans le silence du contrat, les héritiers ne pouvaient imposer aux gestionnaires des comptes de leur transférer les données personnelles détenues[238].

Au nouvel article 85 II de la loi du 6 janvier 1978, le législateur a finalement prévu, que les héritiers pourraient « recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers », laissant planer quelques incertitudes sur leur contenu. Ils se définissent d'abord négativement en ce que ne sont visés que ceux « transmissibles aux héritiers »[239]. Est ainsi évincée la question des biens culturels numériques, objets d'un contrat de location dont les stipulations empêchent le transfert aux héritiers. Les plateformes de téléchargement permettent la constitution de bibliothèques numériques individuelles d'œuvres musicales, cinématographiques et littéraires relevant de licences d'utilisation, conformément au droit de la propriété intellectuelle. Leur modèle économique repose sur un droit d'usage financé éventuellement par une redevance financière, et non sur l'acquisition d'un bien. En sorte qu'aucune transmission à un tiers n'est admise. Il en va ainsi des services prestataires de téléchargement des géants du Net, *Apple* ou *Amazon*[240]. Toutefois, ils tendent à être dépassés par d'autres plateformes, fournisseurs de contenus à la demande,

236 - A. Favreau, « Accueil nuancé du projet de loi République numérique (...) », *op. cit.*, p. 26.

237 - Comm. cl. abusives, *recomm. n° 2014-02, 7 nov. 2014, relative aux contrats proposés par les fournisseurs de réseaux sociaux*. V. A. Debet, RDC 2015, p. 496.

238 - Étude d'impact, *op. cit.*, p. 109 et p. 96.

239 - Rép. Min. n°13422, JO Sénat Q, 1er déc. 2016, p. 5198 ; n°94520, JOAN Q, 29 nov. 2016, p. 9844.

240 - Sur le service *Kindle*, liseuse de la firme *Amazon*, S. Michaux, « Amazon, des bibliothèques inaccessibles par-delà la mort ? », 31 mai 2012, <http://www.lettresnumeriques.be/2012/05/31/amazon-des-bibliotheques-inaccessibles-par-dela-la-mort/>. Sur le service *Itune*s, accès musical de la firme Apple, < https://www.apple.com/legal/internet-services/terms/site.html>. Sur les biens numériques et la mort, J. Groffe, *op. cit.*, n° 15-7.

streaming, permettant contre abonnement l'accès illimité aux contenus culturels de leur catalogue[241]. Ce modèle de service de médiation de biens, conférant un simple droit d'usage, supplante la propriété ou la possession d'un bien[242]. Il s'agit des plateformes *Amazon* ou *Price Minister* ou encore des services audios en ligne proposés par *Deezer*, *Spotify*, *Fnac music*, ou encore de visionnage de vidéos procuré par *Netflix*. Aucune transmission de propriété n'a lieu au profit de l'utilisateur du service et donc *a fortiori* en faveur de ses héritiers. Cette solution sera probablement celle applicable aux jeux vidéos en réseau. Les actifs immatériels générés par l'habileté du joueur ou achetés par lui, comme l'avatar, ses accessoires et ses outils de guerre, ne devraient pas pouvoir être transmis aux héritiers, sauf prévision spécifique des conditions générales d'utilisation[243]. Aucune transmission ne semble possible s'agissant en outre d'autres services d'abonnement conclus *intuitu personae*, à un service de bibliothèque de contrats, de base de données numérique ou une *Legaltech*, dont les stipulations contractuelles sont précises sur l'objet de la prestation fournie par le professionnel. Ces différents services reposent sur la personnalisation réalisée par un algorithme analysant les préférences du client, qu'il conseille ; ils détiennent un important volume de données personnelles outre ceux relatifs à l'identité et aux coordonnées bancaires de l'utilisateur, qui pourra faire l'objet d'une protection en notifiant le décès, que devra prendre en compte le responsable de traitement.

Positivement, les « biens numériques ou des données s'apparentant à des souvenirs de famille » seront les photographies numériques ou numérisées et « diverses contributions partagées sur un réseau

241 - Le service repose sur une mise en accès gratuite de fonctions limitées et contre rémunération de fonctionnalités plus évoluées ; ce dispositif à deux niveaux est appelé *freemium*.

242 - C. Castets-Renard, « Des biens aux services numériques : de l'ère de la propriété à l'âge de l'accès », *in Les biens numériques*, coll. Colloques Ceprisca éd., 2015, E. Netter, A. Chaigneau (Dir.), p. 203, spéc. p. 208.

243 - Forum des droits sur l'Internet, Recomm., *Jeux vidéo en ligne : quelle gouvernance ?*, 9 nov. 2007, p. 41-3 <http://www.globenet.org/IMG/pdf/pdef_forum_droits_internet_jeux_en_ligne_surligne.pdf> relevant que l'avatar du joueur ne sera protégé au titre du droit d'auteur que si l'apport de l'éditeur du logiciel de jeu est limité. Comp. J. Sabbah, « L'appréhension de l'identité sur Internet », *RLDI* 2014/2, p. 99, spéc. IB clamant la propriété de l'avatar.

social »[244]. Il peut s'agir de photographies prises par le défunt, dont l'usage lui a été conféré par le titulaire des droits ou détenues légalement par acquisition d'une licence. Sociologiquement, l'attachement aux contenus numériques tient à ce qu'ils emprisonnent des souvenirs ou la personnalité d'un individu[245] ; ils constituent un patrimoine symbolique, car ils matérialisent l'histoire familiale, individuelle et collective par des photographies et aussi les profils de réseaux sociaux numériques et des fichiers au format numérique (texte, illustration, document audio ou vidéo) en raison du temps et des efforts consacrés à les faire évoluer, les préserver. Alors que l'attachement aux contenus numériques est en général moins fort qu'aux objets physiques, il est plus net pour les jeunes générations, pour lesquelles ils sont plus naturels. On songe dès lors à l'importance de récupérer les photographies présentes sur les réseaux sociaux d'échange (*Facebook, Twitter, Tumblr, Google+, WhatsApp, Snapchat*), réseaux de partage photographique (*Instagram, Pinterest, Flickr, Picasa* devenu *Google photos*...) et sur les *cloud* de sauvegarde liés à l'utilisation d'appareils photo intégrés dans des téléphones, ordinateurs ou tablettes via la *webcam*. Pourraient encore constituer des biens numériques visés par le dispositif les fichiers contenus dans un blog ou un vidéoblog, dit vlog, mis en ligne par le défunt, avatars modernes du journal intime. Il devrait, à notre sens, en aller de même des vidéos intégrées sur un site Internet de partage, tel *Youtube*, récupérables par les héritiers, sauf contrefaçon. La question de l'appartenance des correspondances à la catégorie des biens numériques est plus délicate en ce qu'elles sont libellées à des destinataires spécifiques. La triple protection pénale, civile et par le code des postes et télécommunications du secret des correspondances a été rappelée[246]. Elle ne paraît pas céder avec la cessation de la personnalité juridique d'un correspondant, mais perdurer en faveur du ou des autres destinataires. En 2014, la Commission nationale de l'informatique et des libertés estimait « [qu']un profil sur un réseau social ou un compte de messagerie est

244 - M. Bourgeois, A. Bounedjoum, « Les impacts de la loi pour une République numérique (...) », *op. cit.*, n°12.

245 - S. Guillemot, A. Gourmelen, *op. cit.*, p. 130.

246 - V. *infra*, sect. 2, §2 A2b. Sur le secret des correspondances corollaire du respect de la vie privée, F. Terré, D. Fenouillet, *Droit civil, Les personnes, Personnalité, Incapacité, Protection*, Dalloz précis, 8e éd. 2012, p. 132-3, n°117 ; Cass. Soc. 2 oct. 2001, *Nikon*, Bull. n° 291.

strictement personnel et soumis au secret des correspondances. A ce titre, le droit d'accès n'est pas transmissible aux héritiers »[247]. On doute qu'en l'absence de directives du défunt, les courriels puissent être transmis automatiquement à ses héritiers, au titre des biens numériques. Par contre, admettre que les directives générales ou spéciales puissent autoriser les héritiers à y accéder, sous réserve de la protection des droits des destinataires, permettrait d'aligner le régime des courriers électroniques et postaux. Interprétée ainsi la loi nouvelle supprimerait toute distinction entre les formats corporels ou numériques, et remédierait à la critique de l'absence de régime unitaire au décès de la personne des photographies, courriers et journaux intimes[248].

Pour atteindre son objectif, fallait-il que le législateur de 2016 renvoie à la notion prétorienne de souvenir de famille forgée au XIXe siècle ? Cette construction jurisprudentielle avait eu pour but de faire échapper au droit commun de la dévolution successorale et des libéralités certains biens chargés de la mémoire familiale, afin d'éviter leur dispersion et d'en assurer la conservation au sein de la famille[249]. À ce titre, le facteur central était le rattachement à l'histoire familiale et non dans la nature de l'objet, qui pouvait correspondre à tous types de biens meubles ou immeubles[250]. La jurisprudence étant relative à des correspondances, des tableaux, voire des bijoux, une dimension de durée de conservation familiale a été mise en avant[251], de même que le caractère de bien corporel des souvenirs

247 - CNIL, *Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ?*, 29 oct. 2014, <https://www.cnil.fr/fr/mort-numerique-peut-demander-leffacement-des-informations-dune-personne-decedee -0>. *Adde*, CE, 5 mars 2018, n° 414859, Lebon T. posant que « les données archivées par M. B. sur ses comptes de messagerie électronique [documents contenant des données personnelles dont il n'a pas de copie] doivent être regardés comme des biens personnels » à propos d'un détenu demandant une mesure pour les sauvegarder pendant sa détention, car ils seront clôturés faute d'accès pendant une durée prolongée d'après les conditions générales d'utilisation.

248 - C. Pérès, *op. cit.*, n°11-12.

249 - J.-F. Barbiéri, « Les souvenirs de famille : mythe ou réalité juridique ? », *JCP N* 1985, 100926, spéc. n° 1 renvoyant à Cass. req., 14 mars 1939, *D.H.* 1939, 260 ; *Gaz. Pal.* 1939, 2, 5 ; *D.P.* 1940, 1, 9, note R. Savatier et Cass. req., 30 juin 1942, *JCP* 1943, II, 2254, note R.S. ; *D.A.* 1943, 3.

250 - *Id.*, n° 5 retenant que « le qualificatif « souvenir » pourrait s'appliquer *a priori* à tout type de bien, meuble ou même immeuble : documents tels que correspondances, diplômes, certificats, manuscrits, papiers et registres domestiques, armes et décorations, portraits peints, sculptés ou photographiés... ».

251 - *Id.*, n° 7-10.

de famille[252]. Deux critères assez peu transposables à l'univers numérique, puisque le développement de l'Internet interactif, dit *web 2.0*[253], demeure récent et qu'il comprend en grande partie des actifs immatériels. Les souvenirs de famille échappent en outre aux règles du partage établies par le code civil, en sorte « qu'en l'absence d'accord de tous les membres de la famille sur le sort des souvenirs de famille (...) il appartient au juge de déterminer celui d'entre eux qui est le plus qualifié pour se les voir confier » dans l'exercice de son pouvoir souverain[254]. Quand bien même les souvenirs de famille disposeraient d'une valeur vénale, le membre qui en est dépositaire et non propriétaire, ne peut seul décider de leur vente ; les autres membres de la famille pourraient alors solliciter une saisie-revendication pour éviter leur vente aux enchères[255]. Les archives de famille, sans valeur patrimoniale, disposent d'une valeur essentiellement morale, le rattachement à la catégorie des souvenirs de famille tend à éviter leur dispersion[256]. La finalité de la notion de souvenir de famille est de conserver intègre une masse de biens disposant d'un intérêt pour la famille envisagée collectivement[257], de « faire prévaloir pour l'avenir les intérêts extrapatrimoniaux que la famille a attachés dans le passé à ces biens »[258]. Cela a justifié de leur conférer un statut exorbitant du droit commun en sorte que leur définition doit rester restrictive[259]. En recueillant l'onction

252 - J.-B. « Donnier, Partage – Dispositions communes – Demandes en partage », JCl. Civil Code, Art. 816 à 824, fasc. unique 2016, n° 12.

253 - C. Castets-Renard, *op. cit.*, p. 210.

254 - Cass. 1ère civ., 29 nov. 1994, n° 92-21993 ; Bull. n° 354 ; *RTDciv*. 1995, p. 663, obs. J. Patarin. Sur la détermination judiciaire du dépositaire d'un album de photographies de famille, Caen, 22 janv. 2004, Juris-Data n°2004-235822, *Dr. famille* 2005, comm. 86, obs. B. Beignier.

255 - Cass. 1ère civ., 29 mars 1995, n° 93-18769 ; Bull. n° 115.

256 - Montpellier, 10 sept. 2002, Juris-Data n°2002-199856, *Dr. famille* 2003, comm. 53, obs. B. Beignier retenant une indivision forcée, désignant un héritier attributaire devant « les placer à ses frais à la Société des Lettres, Sciences et Arts de l'Aveyron, habilitée à les recevoir et à en assurer la garde matérielle, afin que ces archives soient maintenues dans le département où elles ont leur origine et leur intérêt, et que les autres membres de la famille puissent » y accéder.

257 - Sur les débats sur la qualification : indivision forcée, copropriété et en son temps la personnalité morale de la famille, J.-B. Donnier, *op. cit.*, n° 13; J.-F. Barbiéri, *op. cit.*, n° 19-22, proposant, n° 23, de retenir un droit de propriété individuelle de l'attributaire sur les souvenirs familiaux assorti d'une interdiction de disposition volontaire, sauf en faveur d'un membre de la famille ou une collection publique, n° 26-30 une fondation privée à affectation familiale.

258 - J.-F. Barbiéri, *op. cit.*, n° 19.

259 - *Id.*, n° 15.

légale pour un cas spécifique de souvenirs de famille de nature numérique, on s'interroge sur les contours de la notion et l'utilité de son dévoiement. L'article 85 II de la loi de 1978 nous semble renvoyer à la nécessité pour les héritiers de s'entendre pour conserver des archives numériques familiales, notamment les photographies et vidéos. Il est douteux que pour atteindre cet objectif il faille remettre en cause la construction jurisprudentielle séculaire sur les souvenirs de famille. N'aurait-il pas suffi de laisser agir les proches (couple, famille, amis) et en cas de conflit de renvoyer au juge la détermination du dépositaire le plus apte ?

3) Régler les conflits entre héritiers devant le tribunal de grande instance

Après avoir organisé les prérogatives laissées aux héritiers en l'absence de directives du défunt, l'article 85 II alinéa 5 de la loi de 1978 entend régler la compétence juridictionnelle s'ils entraient en conflit sur les mesures adoptées. Il retient que les désaccords entre héritiers sur l'exercice des droits qu'il prévoit en l'absence de directives devront être portés devant le tribunal de grande instance compétent. Plusieurs observations peuvent être faites. Tout d'abord, le tribunal de grande instance étant la juridiction de droit commun en matière civile, le contentieux entre héritiers devait logiquement lui échoir[260]. Prendre le soin d'attribuer une compétence matérielle d'exception à cette juridiction, pour les litiges qui opposeraient les héritiers, était redondant. L'objectif était-il d'éviter les doutes du justiciable sur l'application des textes attribuant compétence exclusive de ce tribunal en matière successorale, ou de répondre aux observations sur le projet de loi[261] ? Pour clarifier les éventuels contentieux, il aurait, de surcroît, été souhaitable de préciser la compétence territoriale à retenir pour les conflits entre héritiers sur les mesures prises au titre du texte sur la mort numérique[262]. Les

260 - COJ, art. L. 211-3.

261 - C. Pérès, *op. cit.*, n° 13-4 regrettait le silence du texte sur le concours de bénéficiaires et leur éventuel désaccord ? ; Master 2 Droit du numérique Paris 1, <https://www.republique-numerique.fr/projects/projet-de-loi-numerique /consul tation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/observations-sur-la-mort-numerique> prônait d'opérer renvoi vers le droit des successions lors de conflits.

262 - COJ, art. R. 211-16 posant « Les règles relatives à la compétence territoriale du tribunal de grande instance statuant en matière civile sont déterminées par le code de procédure civile, ainsi que par les autres lois et règlements ».

hésitations les plus importantes portent sur cette question, n'ayant pas été envisagée par la loi du 7 octobre 2016. Est-ce la juridiction du domicile du défendeur qu'il faudra saisir, conformément au principe des articles 42 et 43 du code de procédure civile ? La similarité de la formulation terminologique et la convergence des dispositifs pourraient encourager à choisir la compétence territoriale dérogatoire prévue à l'article 45 dudit code posant que « les demandes entre héritiers » « sont portées devant la juridiction dans le ressort de laquelle est ouverte la succession » ? Il convient de noter que la loi attribue expressément compétence matérielle et territoriale en matière successorale, au tribunal de grande instance du dernier domicile du défunt[263] ; celui-ci est considéré comme l'endroit où les intérêts matériels de la personne étaient centralisés, ce qui écarte la compétence territoriale du lieu du décès et le fait parfois primer sur la compétence en matière mobilière et territoriale d'autres tribunaux[264]. Un régime juridique plus abouti aurait donc été souhaitable pour le nouveau texte inséré dans la loi de 1978, même s'il est utile d'en avoir envisagé la mise en œuvre pratique. Les dispositions décrétales en attente règleront-elles ce point ? Les mêmes règles de compétence juridictionnelle devraient être applicables aux litiges opposant les personnes investies d'un pouvoir d'action par les directives laissées par le défunt et ses héritiers.

D'autres contentieux, non régis par les prévisions de l'article 85 II de la loi de 1978 pourraient survenir entre héritiers. L'attribution de la qualité d'héritier pouvant se prévaloir du nouveau dispositif pourrait être débattue devant le tribunal de grande instance, statuant comme juge de droit commun, dans le cadre de sa compétence résiduelle en matière civile. Il lui appartiendra alors de décider qui pourra faire prévaloir ses positions auprès des responsables de traitement. Le texte voté par le parlement avait en effet renoncé à classer l'ordre des ayants droit pouvant se prévaloir du dispositif d'accès, que prévoyait le projet de loi[265]. Par ailleurs, pourra être envisagée la saisine du juge pénal par citation directe en cas de diffamation d'un héritier ayant

263 - C. civ., art. 720 ; CPC, art. 45 ; COJ, art. L. 211-4 et R. 211-4. Rappr., C. civ., art. 841 et 1379 à 1381 lui attribuant compétence en matière de partage.

264 - A. Le Bayon, Compétence territoriale en matière civile, JCl. Procédure civile Fasc. 600-80, 2018, n° 123-6.

265 - V. C. Pérès, *op. cit.*, n°13-14 et *infra*, sect. 2, §2 A2b reprise de l'ordre pour la divulgation des œuvres posthumes.

agi au détriment des intérêts du défunt avec « l'intention de porter atteinte à l'honneur ou à la considération des héritiers, époux ou légataires universels vivants », sur le terrain du droit de la presse[266]. En l'absence d'héritiers, avoir organisé des directives devient un enjeu plus fort… celui de la survie numérique.

B. Les directives du défunt : préservation de l'identité numérique du défunt *a maxima*

La personne désignée par le défunt pourrait se voir chargée des missions décrites par la loi en l'absence de mesure volontaire. Les directives données par le défunt détermineront les fonctions à exercer suivant les aptitudes de chacun de ses proches. À peine est-il besoin de souligner l'utilité de directives explicites pour les personnes très actives sur les réseaux sociaux numériques, et spécifiquement pour les productions sur Internet des « influenceurs », qui génèrent des effets sur les comportements en société ou les décisions d'achat. Ce néologisme, en plein essor dans le secteur marketing[267], renvoie généralement à l'influence digitale sur les réseaux sociaux de partage de vidéos, comme *Youtube*, ou d'images, comme *Instagram* ; le site de micro-blogage *Twitter* apparaissant souvent comme relais complémentaire de ces deux médias. Point besoin d'être très exposé médiatiquement pour que l'activité sociale d'une personne soit à préserver après son trépas. Dès 1991, il avait été relevé que « La considération pour la mémoire du mort mérite d'être pleinement reconnue comme un droit de la personnalité » ; il est « un droit qu'il est difficilement admissible de refuser au mort : celui qu'on se souvienne de lui », ne protège-t-on pas d'un point de vue patrimonial ses souvenirs de famille ? « il serait trop frustrant que la mémoire des êtres soit ignorée par le droit »[268]. Encore faut-il explorer sa portée. Revenons sur quelques points délicats relatifs à la conservation des comptes du défunt sur les réseaux sociaux numériques, à l'image du mort, ainsi qu'à ses avatars et hologrammes.

266 - V. *infra* sect. 2, § 1 A.

267 - V. les définitions accessibles aux adresses <https://www.definitions-marketing.com/definition/influenceur/> et <https://www.journalducm.com/dictionnaire-marketing/influenceur-influenceuse/>.

268 - F. Ringel, E. Putman, « Après la mort », *D.* 1991, p. 241, spéc. n° 3.

1) Administration des comptes du mort sur les réseaux sociaux numériques

Les proches sont dans un conflit de loyauté lorsqu'ils doivent supprimer ou ne plus interagir avec le compte d'un défunt sur les réseaux sociaux numériques[269]. Les réactions peuvent être différentes face à la mort, tandis que paraît en filigrane l'idée de ne pas trahir l'identité du défunt, à tout le moins son identité assignée. Mieux vaudrait que chaque personne prépare une liste la plus exhaustive possible de ses comptes sur les réseaux sociaux numériques, de messagerie, blog, chaines et autres pages personnelles sur Internet... et du devenir, qui lui semble devoir leur donner.

La mise en pratique des directives du défunt, introduites par la loi du 7 octobre 2016, pourrait prendre appui sur les travaux en sciences de l'information et de la communication mettant en lumière les usages numériques autour de la mort. Selon une enquête sur le sort de leurs données en ligne après leur décès, 26,7 % des 766 répondants jugeaient qu'elles devraient être détruites, tandis que pour 26,3 % des interrogés elles devraient être accessibles à leur famille et pour 15 % en accès à leurs amis ; le reste du panel se partageait entre 14 % des avis estimant que leurs données devraient en partie être détruites et certaines conservées, 11 % qu'elles devraient continuer d'exister et une minorité de 2,7 % des sondés pensant que leurs données devraient être accessibles à tous[270]. La suppression trop rapide du compte du défunt sur les réseaux sociaux sans mesurer sa symbolique pourrait être regrettée par les endeuillés[271]. Mais, souvent, de tels profils ne sont pas supprimés par les proches, soit qu'ils les trouvent insuffisamment signifiants et restent passifs, soit qu'ils s'y rendent via leur propre profil et y laissent des publications, soit qu'ils continuent à « l'animer » en lieu et place du titulaire défunt

269 - H. Bourdeloie, « Usages des dispositifs socionumériques et communication avec les morts », *op. cit.*, p. 116-7.

270 - H. Bourdeloie, V. Brun, *Le deuil numérique en chiffres, Rapport de recherche*, Université Sorbonne Nouvelle - Paris 3, 2018, <hal-01698125v2>.

271 - F. Georges, « De l'identité numérique aux éternités numériques : la mort extime (...) », *op. cit.*, p. 21.

avec ses identifiant et mot de passe[272]. Accéder au compte d'un tiers après sa mort contrevient aux conditions générales d'utilisation du service des géants d'Internet (GAFA) qui limitent les possibilités d'action des survivants, cantonnés aux comptes mémoriaux, légataires et autres mesures tendant à limiter leurs demandes *post-mortem*. On peut espérer que les directives du défunt, revêtues de la force de la loi, seront respectées par les entreprises, car le défunt a bien consenti au transfert de l'exercice de ses droits sur ses données[273].

Dans les sociétés contemporaines, l'hybridation du deuil permet de le traverser de façon intime, mais aussi collective au travers des services numériques. Internet favorise la communication avec les morts dans une logique double pour les « deuilleurs », au sens d'acteurs de leur deuil[274]. Il leur faut préserver l'identité numérique du défunt et gérer ses traces numériques, mais il s'agit également d'interagir avec lui dans le monde numérique en forgeant sa propre exposition de soi. Le profil du défunt sera modifié pour « rentrer en conformité avec l'idée que s'en font les endeuillés et/ou à l'apposition de stigmates de la mort », notamment par des suppressions ; laisser un profil intact peut nécessiter une surveillance constante du profil du défunt[275]. La « gestion des contenus » en ligne, traces numériques et données personnelles numériques du défunt, a pu

272 - H. Bourdeloie, V. Brun, *op. cit.*, quantifiant les usages numériques du deuil les plus fréquents : compte Facebook, toujours actif du défunt (15,4 %), pages web d'hommage (consultation 23,2 % et création 21.40%), forums (18,2 %). *Adde*, notant 4 suppressions sur 46 comptes Facebook de défunts analysés entre 2014 et 2016, F. Georges, V. Julliard, Profilopraxie (…), *op. cit.*, p. 240-2 ; V. Julliard, F. Georges, P »roduire le mort. Pratiques d'écriture et travail émotionnel des deuilleurs et des deuilleuses sur Facebook », *Réseaux* 2018/4, vol. 210, p. 89, spéc. p. 98 ; *Id.*, « Quand le web inscrit le mort dans la temporalité des vivants », *in Temporalités et dispositifs de médiation*, A. Lamy, D. Carré (Dir.) Paris, L'Harmattan, 2017, p. 105, spéc. p. 111-2.

273 - V. *infra*, sect. 2, §2 A2b, sur le refus d'accès aux proches de Yahoo aux États-Unis et Facebook en Allemagne.

274 - H. Bourdeloie, *op. cit.*, p. 102, 113 et 121. *Adde*, V. Julliard, F. Georges, « Quand le web (…)», *op. cit.*, p. 105-116 ; E. Bornand, « La présence numérique des morts », 13 janv. 2018, <https://zsociologie. hypotheses.org/1293> ; L. Jérôme, C. Biroté, J. Coocoo, « Images de la mort et ritualisation du deuil sur les réseaux socionumériques : des usages de *Facebook* en contexte autochtone », *Frontières*, 2018/2, n° 29, <http://id.erudit.org/iderudit/1044157ar>.

275 - F. Georges, V. Julliard, Profilopraxie (…), *op. cit.*, p. 251 ; V. Julliard, F. Georges, Quand le web (…), *op. cit.*, p. 111-2 relevant que la moitié du corpus analysé ne présente pas de publications publiques ou ont été supprimées.

être rapprochée des rituels des thanatopracteurs, transfigurant par leurs soins le cadavre en mort serein[276]. Il n'est pas possible de léguer ses contacts sur un réseau social[277], qu'une nouvelle personne ne va pas s'approprier. Il s'agit de veiller sur les comptes des morts plus que de s'en emparer. La prise en main du profil du défunt sur les réseaux sociaux n'est pas exclusive et peut s'accompagner « de la création d'une page "groupe" à visée mémoriale »[278] ; elle intervient notamment en cas de conflits entre les proches sur le contrôle des publications sur le profil du mort sur un réseau social pour produire une représentation du défunt paraissant plus conforme pour la postérité[279]. Ces interactions, même « l'apposition du stigmate de la mort (...) reste finalement une façon d'alimenter l'identité numérique du défunt, [font que] Facebook semble le lieu du déni de la mort »[280]. Une séparation d'avec les morts toujours numériquement présents pourra intervenir à plus long terme par une désaffection du compte en ne le consultant plus pour s'éloigner du rappel de la perte du mort, ou en le supprimant[281]. Le devenir des comptes en ligne de défunts est à forger.

2) Exploitation de l'image du mort

L'image d'une personne est classiquement considérée comme de nature à l'identifier, ce qui en fait une donnée personnelle protégée tant que dure la personnalité juridique. On sait déjà que l'image de la personne constitue un intérêt patrimonial à caractère personnel, objet d'un droit dérivé de la personnalité et que l'image n'est pas

276 - F. Georges, « De l'identité numérique aux éternités numériques (...) », *op. cit.*, p. 21-2.

277 - Orianne (*sic*), « Léguer ses followers : et si c'était possible ? », 28 déc. 2015, <http://blog.testamento.fr/leguer-ses-followers-et-si-cetait-possible/> évoquant une entreprise anglaise, créée en 2012, qui le proposait, mais à ce jour, le nom de domaine du site <https://www.planneddeparture.com/> a été repris pour une autre activité et le blog n'a pas été réactualisé depuis 2016 : < https://planneddeparture.wordpress.com/>.

278 - F. Georges, V. Julliard, Profilopraxie (...), *op. cit.*, p. 235 et 240-1. V. F. Quinche, « Faire mémoire sur internet » (...), *op. cit.*, spéc. « Créer une page *Facebook* suite à un décès ».

279 - *Id.*, p. 252 ; H. Bourdeloie, *op. cit.*, p. 115.

280 - *Id.*, p. 252 ; H. Bourdeloie, *op. cit.*, p. 106-7 ; V. Julliard, F. Georges, « Produire le mort (...) », *op. cit.*, p. 111 déduisant des pratiques d'écriture en ligne autour du mort l'invitation à interroger l'idée « d'internaute défunt.e ».

281 - H. Bourdeloie, *op. cit.*, p. 111-2 et 114 citant le désabonnement aux notifications du fil d'actualité.

une œuvre[282]. Sa protection est assurée par l'article 9 du code civil, dans le cadre prévu par les conditions contractuelles de la cession d'image, et non par le droit moral conféré à un auteur par le code de la propriété intellectuelle[283]. La question de l'exploitation commerciale de l'image du mort ne manquera pas de se poser lorsqu'elle donne lieu à un stockage sur support numérique. Dès 2007, le groupe de l'article 29 retenait que « La législation nationale sur le droit au respect de l'image et de l'honneur peut également prévoir une protection de la mémoire de la personne décédée »[284]. Ce sont évidemment les héritiers qui percevront, au titre du partage de succession, les revenus générés en ligne *post-mortem* en application des conventions conclues par la personne disparue de son vivant (rémunération due au titre la fréquentation du compte pour une chaîne *Youtube* ou liée aux partenariats commerciaux...). Concernant l'exploitation de l'image *post-mortem*, des décisions du fond ont considéré qu'une certaine forme de transmission aux héritiers pouvait être admise. En faveur de la survie d'un droit de la personnalité relativement à l'image, il a en effet été jugé que l'image est une valeur susceptible d'appropriation et qu'un monopole peut se transmettre aux héritiers[285]. Néanmoins, une telle position n'a jamais été retenue par la Cour de cassation, affirmant au contraire, en 2005, s'agissant de l'utilisation de l'image d'un père défunt que « le droit d'agir pour le respect de la vie privée ou de l'image s'éteint

282 - J.-C. Saint-Pau, « Jouissance des droits civils – Droit au respect de la vie privée », JCl. Civil Code, Art. 9, fasc. 10, 2016, spéc. n° 90.

283 - Cass. 1ère civ., 11 déc. 2008, n° 07-19494 ; Bull. n° 281 ; *Contrats, conc. consom.* 2010, comm. 68, note L. Leveneur ; *RTDciv.* 2009, p. 295, obs. J. Hauser et 342, obs. T. Revet. Rappr. Paris, pôle 5, 4e ch., 6 nov. 2013, n° 11/22839 ; JurisData n° 2013-027583 excluant cependant que ses héritiers puissent autoriser l'exploitation d'une image le représentant sur son lit de mort lorsqu'il n'y a pas préalablement consenti.

284 - Groupe de travail « article 29 », *Avis 4/2007 sur le concept de données à caractère personnel*, p. 24-5.

285 - En ce sens, C. Caron, « Lutte du droit moral post mortem de l'artiste-interprète contre la publicité, obs. sur Paris, 28 avr. 2003, *affaire Ventura »*, *Comm. com. électr.* 2003, comm. 83 ; R. Ollard, *Droits de la personnalité*, J.-C. Saint-Pau (Dir.), LexisNexis Traité 2013, p. 341-4, n° 564-6. V. not. TGI Aix-en-Provence, 24 nov. 1988, *affaire Raimu*, *RTDciv.* 1990, p. 126, obs. J. Patarin ; *JCP G* 1989, II, 21329, note J. Henderycksen confirmé par Aix-en-Provence, 21 mai 1991, I*mages juridiques,* 1er oct. 1991, p. 3 ; Paris, 10 sept. 1996, *affaire Coluche*, RIDA 1997/1, n° 171, p. 345 ; *D.* 1998, somm. p. 87, obs. Ch. Bigot.

au décès de la personne concernée, seule titulaire de ce droit »[286]. Cela a conduit un éminent auteur à réfléchir plus largement à la redéfinition des droits patrimoniaux de la personne et à suggérer leur nouvelle classification au sein des droits de la notoriété[287]. Dans cette catégorie devrait s'intégrer, à notre sens, la protection de l'image numérique et de l'honneur du défunt, qui devraient être défendus par ses ayants droit *post mortem*. La protection relative à l'exploitation de l'image préexistante sera-t-elle étendue à la création de nouvelles images de synthèse générant un avatar du mort ?

3) Résurrection numérique du mort par un avatar ou un hologramme

En prévoyant le devenir de ses données, une personne pourrait prendre des directives sur l'usage de son image après son décès et plus spécifiquement s'opposer ou approuver la création d'un avatar ou d'un hologramme la représentant. Techniquement possible, la résurrection numérique estompe les frontières entre vie et trépas, en entretenant par-delà la mort un échange au quotidien avec le défunt. Depuis quelques années, des pionniers ont créé des logiciels s'appuyant sur l'intelligence artificielle pour simuler une conversation avec une personne morte. Ces robots de conversation, *chatbot*, exploitent les courriels, messages téléphoniques et documents émanant du disparu pour construire des messages à destination des proches[288]. Ces

286 - Cass. 1ère civ., 15 févr. 2005, n° 03-18302 ; Bull. n° 86 ; D. 2005. 2643, obs. A. Lepage ; *RTDciv.* 2005. 363, obs. J. Hauser ; 2ème civ., 8 juill. 2004, n° 03-13260 ; Bull. n° 390 ; *RTDciv.* 2004. 714, obs. J. Hauser. Rappr. Cass. 1ère civ., 31 janv. 2018, n° 16-23591 écartant l'atteinte au droit à l'image d'un chanteur défunt dont un cliché fut pris pour illustrer une compilation musicale ainsi que l'atteinte à son droit d'interprétation.

287 - J.-M. Bruguière, « "Droits patrimoniaux de la personnalité", Plaidoyer en faveur de leur intégration dans une catégorie des droits de la notoriété », *RTDciv.* 2016 p. 1, spéc. n° 20 et 28 balayant les arguments sur l'intransmissibilité, notamment celle sur la création d'un marché de l'exploitation commerciale des morts en relevant que la protection de l'image ne devrait pas être moindre que celle du droit d'auteur.

288 - Charlène (sic), « Il parle avec son père décédé via un dispositive de communication très spécial », 17 mai 2018, <http://www.letribunaldunet.fr/insolite/pere-decede-dispositif-video.html> et la vidéo <https://www.dailymotion. com/video/x6galqp> ; Fred (sic), « En Suède, il sera bientôt possible de "Parler" avec des morts », 28 févr. 2018, <http://www.fredzone.org/suede-parler-avec-des-morts-332> ; Y. Eudes, « Replika, Le double d'un défunt dans une application mobile », 28 juil. 2017, <https://www.lemonde.fr/festival/article/2017/07/28/replika-le-double-d-un-defunt-dans-une-appli-mobile_5165889_4415198.html> ; A. Laurent, « "Parler aux morts" sera, dans le futur, aussi naturel qu'ouvrir Facebook », 28 oct. 2016, <https://www.20 minutes.fr/culture/1946791-20161028-parler-morts-futur-aussi-naturel-ouvrir-facebook> citant <www.eterni.me>.

avatars numériques du défunt générés *post-mortem* le font renaître dans un format dématérialisé constitués de l'ensemble des données personnelles de la personne physique[289]. Ces services de discussion avec un défunt, brouillant les repères, pourraient freiner l'acceptation du deuil. Pour autant, n'étant accessibles qu'aux personnes endeuillés qui l'organiseraient, ils ne semblent pas importuner les autres proches, ne pouvant s'en plaindre que si la diffusion du dispositif avait des répercussions négatives sur leur vie privée.

Plus radicalement, on songe aux thèses transhumanistes ayant poussé à leur paroxysme l'idée de concevoir un avatar. Ray Kurzweil, expert en intelligence artificielle affilié à *Google*, exposait son projet « initiative 2045 » de permettre à l'être humain de télécharger son esprit dans un ordinateur, voire le faire survivre en s'incarnant dans un robot[290]. Techniquement, il est possible de faire « revivre » le défunt par le biais d'un hologramme, image en trois dimensions qui l'imiterait[291]. Dans un futur proche, cela pourrait ne pas être l'apanage des seuls chanteurs décédés mis en scène dans un spectacle ou de résurrections d'acteurs de sagas cinématographiques[292]. À cet égard, l'utilisation d'un hologramme, a pu être considérée comme générant le « double informationnel » de la personne[293]. Sa « réincarnation »

289 - D. Bourcier, « De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique ? », *Droit et société* 2001/3, vol. 49, p. 847, spéc. p. 867-8 voyant la personnalité virtuelle tel un droit sur un profil, sur des données ; A. Latil, « La diffamation dans les univers virtuels », *op. cit.*, spéc. I liant droits de la personnalité et droits sur l'avatar.

290 - F. Solari, *L'homme qui vivra 200 ans est-il déjà né ?*, Le Pommier 2017, p. 108-110 ; J.-Cl. Heudin, *op. cit.*, p. 155-62 chap. « téléchargement de l'esprit » ; *Interview PBS Newshour, Ray Kurzweil on Bringing Back the Dead*, 12 juil. 2012, <http://www.kurzweilai.net/pbs-newshour-ray-kurzweil-on-bringing-back-the-dead> confiant le vœu de faire revivre son père. Rappr. Transcendance, film de W. Pfister, 2014 sur un scientifique défunt dont l'épouse use des travaux pour transcender son esprit vers un ordinateur ; série télévisée suédoise *Real humans : 100 % humain* (*Äkta människor*), 2012 sur des robots humanoïdes, l'un ayant l'apparence d'un défunt et téléchargé ses souvenirs.

291 - M. Soulez, « Hologramme : la redécouverte d'un mode de communication », 9 févr. 2017, <https://www.alain-bensoussan.com/avocats/hologramme-statut-legal/2017/02/09/> posant qu'il constitue « une prouesse technique qui, par l'usage minutieux de surfaces réfléchissantes, de lumière, de lasers et de fins calculs, permet qu'une simple projection d'image en 2D génère l'illusion optique d'une image en 3D : l'hologramme) ».

292 - V. les exemples cités *in* A. Bensoussan, M. Soulez, « L'hologramme sur tous les fronts ? », *Revue pratique de la prospective et de l'innovation* mars 2017, entretien 2 ; M. Soulez, *op. cit.* ; L. Neuer, Carrie Fisher, Tarkin, « Cloclo : l'hologramme a-t-il tous les droits ? », 2 févr. 2017, <http://www.lepoint.fr/pop-culture/cinema/carrie-fisher-tarkin-cloclo-l-hologramme-a-t-il-tous-les-droits-01-02-2017-2101547_2923.php>.

293 - A. Bensoussan, M. Soulez, *op. cit.*, citant Bruno Bonnell.

holographique pourrait soulever différentes questions ayant trait au droit à l'image[294] ainsi qu'à la protection de ses données personnelles collectées pour l'alimenter et le façonner. Maître Tayer, avocat, soulignait que l'usage de l'image de la personne devient libre après son décès, sous réserve du respect de la vie privée familiale, du respect du deuil et la dépouille mortelle. Les « abus holographiques » pourraient être néanmoins neutralisés, car « Les héritiers peuvent s'opposer à l'exploitation de l'image du défunt et faire valoir leur préjudice personnel s'ils démontrent une atteinte à sa mémoire et au respect de sa personne. Par exemple, si l'acteur est (re)présenté dans une scène que la morale des héritiers réprouve, entraînant ainsi une souffrance personnelle insoutenable »[295]. La protection du droit d'auteur pourrait être invoquée par les héritiers de l'artiste en cas de dénaturation de l'œuvre considérée ; on retrouve ici la décision par laquelle les héritiers de l'acteur Lino Ventura ont pu se prévaloir de l'exercice posthume du droit moral de l'artiste pour s'opposer à la postsynchronisation d'une scène d'un de ses films pour une publicité, que ses proches n'avaient pas autorisée[296]. Droit à l'image et droit moral de l'artiste défunt constituent une protection très importante, qui n'existe pas aux États-Unis[297]. Il serait sans doute prudent d'indiquer dans les directives générales de la personne pour le sort de ses données personnelles, si elle souhaite s'opposer à une résurrection numérique[298].

294 - X. Labbée, « L'hologramme, la téléprésence et l'être immatériel », *Gaz. Pal.* 20 sept. 2012, n° 264, p. 11 évoquant la contestation par les ayants droit de Marylin Monroe de l'utilisation par l'entreprise Digicon Media des images de synthèse de l'artiste. Rappr. L. Neuer, *op. cit.*, soulignant que le droit américain ne leur a pas donné gain de cause.

295 - Cité par L. Neuer, *op. cit.*, et donnant l'exemple qu'en se fondant sur le droit moral « les héritiers de Gustave Eiffel pourraient empêcher toute initiative consistant à associer la tour Eiffel à une œuvre ou à un objet pornographique ».

296 - Paris, 28 avr. 2003, *préc.*.

297 - *Id.*, *The Right of publicity* laisse l'image de la personne dans le domaine public à sa mort. Par testament, l'acteur Robin Williams s'était opposé à la réutilisation de son image dans des publicités jusqu'en 2039 et interdisait toute « insertion numérique » ou utilisation d'un hologramme le représentant au cinéma ou à la télévision. Certains États américains « conditionnent l'exploitation *post mortem* de l'image d'un acteur à l'autorisation de ses ayants droit pendant une certaine durée, qui est par exemple, en Californie, [est] de "70 ans après la mort de l'acteur"».

298 - Rappr. G. Marraud des Grottes, « Notaire 2.0, *human* 3.0 : plongée dans les réflexions prospectives du notariat », *RLDC* 2017/10, p. 46, spéc. *in fine* évoquant un « être 100 % numérique, avec lequel certains sites proposent, par exemple, de discuter virtuellement » et l'opposition dans un testament à « être ressuscité numériquement ».

***

Pour conclure, insistons sur l'évolution du droit des données personnelles conçu, dans les années 1970, comme une protection spécifique de la personne dans un monde en cours d'informatisation. La mort en constituait la limite temporelle. Cependant, après décès différentes dispositions juridiques pouvaient être invoquées au secours de la protection des données du défunt. Un champ d'études novateur apparut avec le besoin d'étendre *post-mortem* la protection des informations sous format numérique, qui survivent au défunt. L'émergence de la protection des données personnelles après la mort résulte de la généralisation des traitements de données, de la croissance du nombre d'applications numériques relatives à la mort et du vieillissement de la population, qui laissera une activité numérique inédite et volumineuse. Le nouvel article 40-1 adopté en 2016, repris aux articles 84 et 85, de la loi du 6 janvier 1978, tente de résoudre les difficultés relatives aux données de la personne défunte. Texte de compromis, très long, détaillé sur certains aspects, laconique sur d'autres, sans décret d'application plus de deux ans après son adoption, il suscite de nombreuses interrogations. Les mesures pourraient apparaître finalistes, évitant de résoudre les questions complexes sur la nature juridique des droits conférés. Les recherches des différents domaines des sciences humaines (sociologie, philosophie, anthropologie, sciences de la communication et de gestion) analysant les interactions entre la mort et les phénomènes numériques donnent un utile éclairage sur le contenu et la mise en œuvre des directives susceptibles d'être anticipées par les personnes. Dans la société, les cimetières[299] et les rites funéraires se transforment. S'appuyant sur les évolutions sociologiques et techniques, les pratiques numériques se révolutionnent. Les réseaux sociaux numériques utilisés en France depuis une décennie ont d'ores et déjà beaucoup évolué. Les nouvelles générations ne

299 - P. Moreaux, « Naissance, vie et mort des cimetières » , *Études sur la mort* 2009/2, n° 136, p. 7, spéc. p. 21 relevant que comme « les hommes : ils naissent, grandissent, changent d'aspects et sont appelés aussi à mourir tôt ou tard ».

s'y inscrivent plus autant[300]. Fuyant l'afflux récent de publicités, les utilisateurs se déportent vers les messageries instantanées offrant les mêmes possibilités d'échanges en direct, de transmission de photographies et vidéos, telles *WhatsApp*, *Wechat*, *Line* ou encore *Facebook messenger*[301]. Alors, abandonnera-t-on à l'avenir ces « nécropoles de l'Internet » ? En présence de nombreux « comptes survivants » sur la toile, la question de l'usurpation d'identité numérique, réprimée spécifiquement depuis 2011[302], ne manquera pas d'évoluer. Par ailleurs, le secteur du stockage numérique pourrait se recomposer en considération de la transmission *post-mortem* de contenus dématérialisés. Début 2018, le *Chief Digital Officer* de la mutuelle d'assurance MAIF, Romain Liberge, relevait qu'à l'avenir « Au même titre que nous assurions les domiciles physiques, il faudra désormais assurer les domiciles numériques et permettre aux proches d'une personne décédée de récupérer son patrimoine immatériel »[303]. Les débats sur la protection des données personnelles se renouvellent donc sans cesse depuis 40 ans[304]...

300 - B. Dekonink, « Les réseaux sociaux affrontent une panne de croissance des utilisateurs », 8 août 2018, <https://www. lesechos.fr/tech-medias/hightech/0302090479545-les-reseaux-sociaux-affrontent-un-recul-du-nombre-de-leurs-utilis ateurs -2196992.php>. V. M. McCrindle théorisant la génération alpha des enfants nés après 2010 (année où Ipad, et Instagram furent introduits), <https://mccrindle.com.au/insights/in-the-media/meet-alpha-the-next-next-generation/>.

301 - A. Treguer, « Moins de réseaux sociaux, plus de messageries privées : voilà ce que cela signifie pour les marques », 27 mars 2018, <https://www.frenchweb.fr/les-reseaux-sociaux-qui-deviennent-prives-quels-impacts-pour-les-marques/320451>.

302 - J. Giusti, A. Ndiaye, « L'identité numérique, monnaie (...) », *op. cit.*, spéc. II A « Le vol d'identité numérique ».

303 - E. Trujillo, « Envoyer des messages après sa mort pour léguer un "héritage numérique" », 9 févr. 2018, <http://www.lefigaro.fr/secteur/high-tech/2018/02/09/32001-20180209ARTFIG00002-envoyer-des-messages-apres-sa-mort-pour-leguer-un-heritage-numerique.php>. Rappr. S. Abiteboul, V. Peugeot, *Terra data*, *op. cit.*, p. 299-303 exposant le projet MesInfos de La Maif investissant 3 millions d'euros avec un service de *cloud* français, Cozy Cloud.

304 - V. récemment, *European data protection supervisor*, *Opinion* 3/2018 *on online manipulation and personal data*, *march* 2018, <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf>.

LE RÈGLEMENT 2016/679/EU À LA LUMIÈRE DU DROIT AMÉRICAIN : À LA RECHERCHE D'UN FONDS COMMUN ENTRE L'UNION EUROPÉENNE ET LES ÉTATS-UNIS

Céline Castets-Renard
Membre de l'Institut Universitaire de France (IUF)
Professeur, Université Toulouse 1 Capitole
Directrice du Master Droit du numérique
Directrice adjointe de l'IRDEIC - Centre d'Excellence Jean Monnet

Objectifs du règlement européen de protection des données. Il est peu de dire qu'était attendue l'adoption du règlement 2016/679/UE 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 95/46/CE* (règlement général sur la protection des données dit RGPD)[1]. Quatre ans après la proposition de règlement faite par la Commission européenne[2], marqués par d'interminables négociations, obstructions (plus de 4000 amendements...) et rebondissements en tous genres, le règlement est entré en vigueur et s'appliquera le 25 mai 2018 (art. 99). À cette date, l'abrogation de la directive 95/46/CE prendra effet (art. 94). Le règlement a pour vocation d'établir « des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données » (art. 1§1). Plus particulièrement, le règlement « protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel » (art. 1§2). Cependant, l'alinéa 3 de l'article 1er ajoute que « la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ». Un équilibre doit donc s'établir entre, d'une part, la protection des données personnelles et, d'autre part, leur libre circulation. Ce double objectif se retrouve dans l'intitulé même du règlement, identique à celui de la directive 95/46.

1 - V. not. Fabienne Jault-Seseke et Celia Zolynski, « Le règlement 2016/679/UE relatif aux données personnelles », *D.* 2016, p. 1874 ; Ioana Gheorghe-Badescu, « Le nouveau règlement général sur la protection des données », *Rev. UE* 2016. 466 ; Guillaume Desgens-Pasanau, *Dalloz IP/IT*, 2016 p. 335-339.

2 - COM(2012) 11 final.

Droit fondamental à la protection des données personnelles *versus* vision économique. Si la protection des droits fondamentaux des personnes concernées est un objectif que l'on trouvait déjà dans la directive 95/46, l'adoption du Traité de Lisbonne et de la Charte des droits fondamentaux de l'Union européenne, entrés en vigueur en 2009, lui donnent désormais un fondement renforcé à l'article 8 de la Charte. Ce droit fondamental à la protection des données personnelle s'accompagne en outre du droit à la protection de la vie privée consacré à l'article 7. Enfin, l'article 16 du Traité de Fonctionnement de l'Union européenne (TFUE) reconnaît aussi le principe de la protection des données personnelles. Ces nouveaux fondements viennent en renfort de l'article 8 de la Convention européenne des droits de l'homme et de la jurisprudence de la Cour européenne. En comparaison, bien qu'une protection constitutionnelle ait été accordée dès les années 1960[3], les États-Unis ne considèrent pas la protection des informations personnelles sous l'angle des droits fondamentaux, mais sous celui du commerce et de sa fluidité. Les législations sur les informations personnelles se préoccupent essentiellement de remédier aux préjudices des consommateurs, tout en garantissant l'efficacité des transactions commerciales. Cependant, le droit de l'Union européenne n'est en réalité pas exclusivement orienté vers la protection des droits fondamentaux des individus. Si l'objectif de protection est mis au plus haut sommet de la hiérarchie des normes, ces droits fondamentaux ne sont pas pour autant absolus et doivent se concilier avec les libertés fondant la construction du marché intérieur, telle la libre circulation des biens, incluant les biens immatériels comme les données. Dès lors, les considérations commerciales ne sont pas étrangères à la matière, même si la protection des droits fondamentaux pourra primer sur ces dernières. En résumé, les deux intérêts contradictoires mis en balance sont les mêmes des deux côtés de l'Atlantique , mais le point d'équilibre n'est certainement pas mis au même endroit.

3 - *Griswold v. Connecticut*, 381 U.S. 479 (1965). Voir aussi le test de « l'attente raisonnable de vie privée » (*reasonable expectation of privacy*) fondé sur le 4e amendement dans *Katz v. United States*, 389 U.S. 347 (1967).

Données personnelles *versus* "*Personally Identifiable Information*". Par ailleurs, des différences conceptuelles sont aussi notables. La notion de "donnée personnelle" retenue dans le RGPD est similaire à celle de la directive 95/46/CE et vise « toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (RGPD, art. 4§1).

En comparaison, les États-Unis retiennent la notion de "*Personally Iientifiable information*" (PII) qui est l'un des concepts les plus centraux de la règlementation de la *privacy* aux États-Unis. Cette notion permet en effet de définir le champ d'application et les frontières d'une grande partie des lois et règlementations fédérales et étatiques (mais pas toutes)[4]. On la trouve par exemple dans le *Children's Online Privacy Protection Act (COPPA)* (1998), le *Gramm-Leach-Bliley Act (GLBA)* (1999), le *Health Information Technology for Economic and Clinical Health Act (HITECH)* (2009) et le *Video Privacy Protection Act (VPPA)* (1988). Or, en dépit de l'importance accordée à cette notion, elle ne reçoit pas la même définition selon les textes envisagés[5]. On peut ainsi dénombrer trois conceptions prédominantes pour la définir[6]. Selon une première approche dite tautologique, la PII est définie comme « toute information qui identifie une personne ». La loi *VPPA* adopte cette vision qui n'apporte finalement aucun guide sur la façon de caractériser la donnée. Suivant une deuxième approche, la PII est une "information non-publique". La loi *GLBA* retient ainsi la notion de "*personally identifiable financial information*" ("information financière personnellement identifiable") comme étant une "*nonpublic personal information*"

4 - Daniel J. Solove et Paul M. Schwartz, *Information Privacy Law*, 6e éd. p. 794.

5 - W. Gregory Voss, « Le concept de données à caractère personnel : divergences transatlantiques Safe Harbor et Privacy Shield », *Dalloz IP/IT* 2016, p. 119.

6 - Paul M. Schwartz et Daniel J. Solove, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (December 5, 2011). *New York University Law Review*, Vol. 86, p. 1814, 2011; UC Berkeley Public Law Research Paper No. 1909366; GWU Legal Studies Research Paper No. 584; GWU Law School Public Law Research Paper No. 584. Available at SSRN: https://ssrn.com/abstract=1909366.

("information personnelle non publique"). Le problème est alors que la loi défaille en ne précisant pas ce qu'est la notion de "non publique" , mais on peut supposer qu'elle vise une information hors du domaine public. Cette définition ne se préoccupe cependant pas de savoir si l'information est en fait identifiable. Enfin, la troisième approche consiste à énumérer des données spécifiques, considérées comme des PII. Si une information tombe sous le coup de l'énumération, elle devient une sorte de PII "*per se*". Par exemple, la loi *COPPA* cite notamment les noms et prénoms, numéros de téléphone et de sécurité sociale. L'énumération se veut exhaustive, mais risque d'oublier des données qui devraient y figurer. Cette diversité conceptuelle rend plus difficile encore la comparaison avec le RGPD. En dépit d'efforts de réconciliation des notions par la doctrine américaine[7], force est de constater qu'aucune de ces trois approches de la "*Personally Iientifiable information*" ne correspond à l'approche européenne qui est bien plus englobante.

Données personnelles, vie privée et *privacy*. Plus généralement, des différences conceptuelles se logent aussi dans l'appréhension même de la matière. Le droit de l'Union européenne distingue la vie privée et la protection des données personnelles, comme en attestent les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Les deux notions sont néanmoins proches puisque la Cour européenne des droits de l'homme a pu protéger les données personnelles sur le fondement de l'article 8 de la Convention relatif au droit à la vie privée et à la vie familiale. Mais aux États-Unis, la notion de "*privacy*" est bien plus large, en ce qu'elle regroupe la protection des individus dans un espace privé, mais aussi la collecte et l'utilisation des "*Personally Iientifiable information*", ainsi que la sphère intime des individus[8]. La *privacy* ne se réduit donc pas à la vie privée du droit européen.

7 - Paul M. Schwartz et Daniel J. Solove, « Reconciling Personal Information in the United States and European Union » (September 6, 2013). *102 California Law Review 877* (2014); UC Berkeley Public Law Research Paper No. 2271442; GWU Legal Studies Research Paper No. 2013-77; GWU Law School Public Law Research Paper No. 2013-77. Available at SSRN: https://ssrn.com/abstract=2271442 or http://dx.doi.org/10.2139/ssrn.2271442 .

8 - Daniel J. Solove et Paul M. Schwartz, *Information Privacy Law, op. cit.* (voir l'introduction).

En résumé, alors que la notion de "donnée personnelle" est plus englobante que celle de *Personally identifiable information*", la notion de "vie privée" est plus étroite que celle de "*privacy*". Les traductions littérales sont trompeuses et, en l'absence d'équivalence conceptuelle, la comparaison est rendue complexe.

Règlementation sectorielle *versus* règlementation *omnibus*. Tout comme la directive qu'il abroge, le règlement a un champ matériel « *omnibus* » dans le sens où la règlementation consacrée s'applique à tous les secteurs d'activité et vise les acteurs publics comme privés. Plus précisément, l'article 2§1 prévoit que le règlement « s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». À l'inverse, aux États-Unis, la règlementation est sectorielle et ne vaut que pour certains secteurs d'activité[9], par exemple la santé (*Health Insurance Portability and Accountability Act*) (1996) ou la banque (*Fair Credit Reporting Act* (1970) et *Fair and Accurate Credit Transactions Act* (2003). D'autres règlementations sont encore plus ciblées, à l'image du *Video Privacy Protection Act* (1988) qui protège les informations personnelles détenues par les loueurs de vidéocassettes[10]. La mise en œuvre de chaque loi spécifique sur la *privacy* oblige à se demander notamment quelles sont les données concernées, les acteurs visés et l'autorité de contrôle compétente. Une telle approche, empreinte de libéralisme, tend à laisser faire et à ne prôner une intervention législative qu'en présence de dysfonctionnements sur un marché donné ou de risques importants pour la protection des individus. L'émergence d'une difficulté nouvelle suppose alors une intervention du Congrès et donc nécessairement un temps de réactivité qui laisse, dans cette attente, les individus sans protection, à supposer que la nécessité de cette dernière soit admise par une majorité de membres du

9 - Sur ces différences, voir aussi : Francesca Bignami et Giorgio Resta, « Transatlantic Privacy Regulation: Conflict and Cooperation » (2015). *Law and Contemporary Problems*, Vol. 78, Fall 2015; GWU Law School Public Law Research Paper No. 2015-52; GWU Legal Studies Research Paper No. 2015-52. Available at SSRN: https://ssrn.com/abstract=2705601.

10 - Le Congrès adopta cette loi en 1988 dans un contexte très particulier, lorsqu'un journaliste révéla la liste de vidéocassettes louées par Robert Bork, candidat finalement malheureux à la Cour Suprême.

Congrès. Un autre inconvénient tient au risque de ne pas englober tous les acteurs concernés d'un secteur d'activité visé et de créer une distorsion de concurrence. Cette difficulté est accrue à l'ère numérique où les acteurs dominants ont tendance à diversifier leurs services et pénétrer différents marchés, suivant une stratégie d'intégration verticale[11]. Ils ne sont alors pas considérés comme les acteurs traditionnels dudit marché et seront exclus des contraintes de la règlementation, alors même qu'ils peuvent avoir un impact fort sur ce marché. Par ailleurs, la tâche est rendue d'autant plus difficile qu'il n'a pas été jugé utile d'imposer une autorité de régulation unique du respect des lois sectorielles, compétent en toutes matières.

À l'évidence, cette différence de champ d'application de la règlementation constitue une des principales pommes de discorde entre la Commission européenne et les autorités américaines pour reconnaître adéquat le niveau de protection des lois fédérales.

Fédéralisme et foisonnement normatif. Par ailleurs, le fédéralisme accroît ce foisonnement normatif. Au niveau fédéral, la protection de la vie privée est garantie par la Constitution des États-Unis[12] et les nombreuses législations sectorielles adoptées à partir du début des années 1970. Également, la *common law* a permis de réparer les préjudices liés aux atteintes de la *privacy* sur la base de la *tort law*[13]. La *contract law* donne la possibilité aux parties de

11 - Sur cette question, voir les références : Céline Castets-Renard, « Des biens aux services numériques : de l'ère de la propriété à l'âge de l'accès », *in Les biens numériques*, dir. Emmanuel Netter et Aurore Chaigneau, PUF, coll. CEPRISCA, 2015 : http://www.ceprisca.fr/wp-content/uploads/2016/03/2015-CEPRISCA-BIENS-NUMERIQUES.pdf.

12 - Essentiellement sur le fondement du 4e amendement qui, selon l'interprétation faite par la Cour Suprême, « protège les personnes et non les lieux » (*Katz v. United States*, 389 U.S. 347 (1967)). Également, le 1er amendement a pu assurer une certaine protection de la vie privée au travers de la liberté d'expression et d'association qui prévient la divulgation des informations personnelles des membres d'une organisation (*NAACP v. Alabama*, 357 U.S. 449 (1958) ; *See Shelton v. Tucker*, 364 U.S. (1960). Le 3ème amendement protège la sphère privée du domicile en prévenant l'intrusion de soldats du gouvernement. Le 5ème amendement relatif au droit de ne pas s'incriminer soi-même protège aussi la vie privée en restreignant la capacité du gouvernement à forcer les individus à divulguer certaines informations sur eux-mêmes.

13 - Tel que suggéré dans le fameux article de Samuel D. Warren et Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). Willima Prosper, dans son article *Privacy* (48 Cal. L. Rev. 383 (1960)) identifie quatre catégories de préjudices : 1) la révolution publique de faits privés ; 2) intrusion dans la vie privée ; 3) divulgation d'informations sur une personne qui la place sous un "faux jour" ("false light") ; 4) usurpation d'identité.

prévoir des clauses de protection de vie privée ("*privacy policies*") mais elles ne sont pas qualifiées de contrat en toutes circonstances. Au niveau des États fédérés, certains d'entre eux, comme l'Alaska[14] et la Californie[15], ont explicitement prévu de protéger la vie privée dans leur Constitution. Des lois étatiques sur la *privacy* (*states statutory laws*) complètent la protection. Elles copient parfois les dispositions fédérales, mais peuvent aussi être totalement propres. Comme la dernière réglementation californienne *(California Consumer Privacy Act)*. Elles couvrent des sujets très variés : données collectées dans le cadre de l'emploi, données médicales, données des étudiants... Par ailleurs, les États sont parfois précurseurs pour l'adoption de certaines mesures, comme ce fut le cas pour créer l'obligation des opérateurs de notifier les failles de sécurité impactant les données personnelles.

Éclatement normatif *versus* unification. Finalement, alors que l'on dit souvent trop rapidement que le droit américain ne protège pas la vie privée et qu'il n'y a pas de loi, il s'agit plutôt en réalité d'un trop-plein ! En dépit de ce foisonnement normatif, force est de constater, il est vrai, que la règlementation reste parcellaire et la protection lacunaire. L'approche ciblée sectorielle empêche la mise en œuvre d'une règlementation claire et complète. Est ici privilégié un interventionnisme minimaliste de protection, mais qui engendre, de manière contradictoire, une suractivité législative et judiciaire. En tout état de cause, ce patchwork normatif ne facilite pas la compréhension de la *privacy* américaine par les Européens.

Pour sa part, l'Union européenne tend, à l'inverse, à réduire les divergences entre les États membres, ce qui constitue un des objectifs d'adoption d'un règlement, en lieu et place d'une directive qui laissait trop de latitude aux États membres. Cependant, à y regarder de plus près, on comprend que le règlement est « *sui generis* », en ce sens où il laisse une marge de manœuvre importante aux États membres. La réforme actuellement en cours en France de la loi dite informatique et libertés, qui assure l'intégration du règlement[16], ressemble à

14 - Alaska Const. Art. I § 22 (Right of Privacy) : « *The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section* ».

15 - Cal. Const. Art. I, § 1 : « *All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy* ».

16 - Projet de loi n° 490 : http://www.assemblee-nationale.fr/15/projets/pl0490.asp.

s'y méprendre à une loi de transposition d'une directive, tant des choix doivent encore être faits par le législateur français. Dès lors, l'unification normative au sein des États membres progressera grâce au RGPD, mais restera incomplète. Aucun des deux systèmes n'est donc satisfaisant sur ce point.

Culture, dialogue et influences mutuelles. À l'évidence, la protection des données personnelles est intimement liée à l'histoire[17] et à la culture d'un pays[18], aussi les différences entre les États-Unis et l'Union européenne sont-elles loin d'être négligeables[19]. Mais au-delà de ce constat, l'ère numérique renforce la circulation des données personnelles et les systèmes juridiques sont nécessairement conduits à se confronter, mais aussi à dialoguer, à s'influencer. En dépit des divergences incontestables entre les modèles législatifs des États-Unis et de l'Union européenne, l'adoption du RGPD est l'occasion de chercher à créer des ponts entre les systèmes[20] ou à relever des influences mutuelles[21]. L'objectif des rapides observations qui suivent est de montrer que les différences peuvent être relativisées, grâce à une meilleure compréhension du droit fédéral américain et la quête d'un fonds commun[22], tant dans le choix des instruments normatifs (I) et des règles adoptées (II) que du rôle des parties prenantes (III).

17 - S'agissant des États-Unis, voir Daniel J. Solove, « A Brief History of Information Privacy Law ». *PROSKAUER ON PRIVACY*, PLI, 2016; GWU Law School Public Law Research Paper No. 215. Available at SSRN: https://ssrn.com/abstract=914271.

18 - Vincent Gautrais, « Différences culturelles en matière de vie privée : point de vue canadien », *Dalloz IP/IT* 2016, p. 128.

19 - James Q. Whitman, « The Two Western Cultures of Privacy : Dignity Versus Liberty », *113 Yale L. J. 1151* (2004).

20 - Voir le document élaboré lors de la *37ème International Privacy Conference* qui s'est tenue en 2015 à Amsterdam sur « Privacy Bridges : EU and US Privacy Experts in Search of Transatlantic Privacy Solutions » : https://privacybridges.mit.edu.

21 - See Bilyana Petkova, « Domesticating The 'Foreign' in Making Transatlantic Data Privacy Law » (February 20, 2017). *International Journal of Constitutional Law*, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2920412.

22 - Céline Castets-Renard, « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? » (Dossier spécial : regards croisés transatlantiques sur la protection des données personnelles), *Dalloz IP/IT* 2016, p. 115.

§1 : À la recherche d'un fonds commun dans le choix des instruments normatifs

Protection internationale et influence des États-Unis : le choix de principes généraux souples. Si l'on considère aujourd'hui que le modèle européen de la directive 95/46/CE s'est globalement imposé dans le monde, rappelons que les États-Unis ont été les premiers à insuffler des principes à l'échelle internationale, démontrant leur intérêt pour la question, dès les années 1970. Ils ont très tôt joué un rôle en la matière, dans l'objectif essentiellement de ne pas poser d'obstacle au commerce et à la circulation de l'information. C'est ainsi qu'ils ont activement participé à la rédaction des premiers textes internationaux que sont les *Fair Information Practices (FIP)*[23] élaborés en 1973, ainsi que les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, adoptées en 1980 par l'OCDE[24] et révisées en 2013. Naturellement, il ne s'agit là que de principes généraux très peu contraignants pour les opérateurs, bien loin des règles précises et strictes de la directive 95/46/CE qui crée des droits en faveur des personnes concernées et des obligations à la charge des responsables de traitement. Ces mesures sont loin également de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, adoptée en 1981 par le Conseil de l'Europe et à laquelle les États-Unis n'ont pas voulu adhérer. Cependant, ces principes généraux ont constitué une première approche dont le mérite était de mettre en œuvre une réflexion globale et des règles faciles à faire accepter en différents endroits du monde. Ces principes généraux souples (FIP) ont été d'ailleurs repris par les États-Unis en droit interne [25].

Directive 95/46/CE comme « modèle » des règlementations nationales : le choix de règles précises au travers des flux transfrontaliers. L'adoption en Europe de la directive 95/46/

23 - *The Code of Fair Information Practices on Automated Personal Data Systems, Records, computers, and the Rights of Citizens* a été élaboré en juillet 1973 par le Département américain de la santé et de l'éducation : https://epic.org/privacy/consumer/code_fair_info.html.

24 - http://www.oecd.org/fr/sti/ieconomie/lignedirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieres dedonneesdecaracterepersonnel.html

25 - Marc Rotenberg, « Fair Information Practices an the Architecture of Privacy (What Larry doesn't get) », *Stan. Tech. L. Rev.* 1, 44 (2001).

CE a profondément modifié les relations internationales dans la protection des données personnelles. La libre circulation des données personnelles, évoquée précédemment, s'arrête au territoire de l'Union européenne. Au-delà, les flux transfrontaliers de données vers des États tiers obéissent à des règles strictes, consacrées précédemment par la directive (art. 25), et amplement renforcées aux articles 44 et suivants du RGPD. L'objectif est d'éviter que les exigences de la directive soient contournées par l'envoi des données hors UE. Au contraire, les États-Unis ont fait le choix de ne poser aucune limite aux transferts de données avec les pays tiers[26]. L'Union européenne exige ainsi que le pays destinataire des données personnelles garantisse un « niveau de protection adéquat » [27], reconnu par décision de la Commission européenne. Ce système d'adéquation a constitué un véritablement « instrument de coercition »[28] pour les partenaires de l'Union européenne. En effet, le droit de l'UE imposant le niveau de protection le plus élevé au monde, *a fortiori* avec le RGPD, il a nécessairement été suivi par les nombreux États désireux de faire du commerce avec les entreprises et consommateurs européens[29]. Cette prise de pouvoir s'est confirmée à l'ère numérique où les échanges transfrontaliers de données se sont considérablement accrus[30]. En conséquence, les législations nationales de protection des données personnelles se sont multipliées partout dans le monde sur le modèle de la

26 - Le Congrès américain a considéré cette possibilité dans les années 1970, mais n'est finalement pas parvenu à adopter une règle de limitation : P. M. Schwartz, « The EU-US Privacy Collision: a turn to institutions and procedures », 1*26 Harv. L. Rev. 1966 2012-2013*, p. 1967.

27 - Pour mémoire, ont bénéficié d'une décision d'adéquation : Andorre, Argentine, Canada (uniquement les organisations commerciales), îles Féroé, Guernesey, Israël, île de Man, Jersey, Nouvelle Zélande, Suisse et Uruguay.

28 - Paul M. Schwartz and Karl-Nikolaus Peifer, « Transatlantic Data Privacy ». *106 Georgetown Law Journal 115* (2017) ; UC Berkeley Public Law Research Paper : SSRN: https://ssrn.com/abstract=3066971.

29 - Fabrice Naftalski, « L'impact du nouveau règlement sur les stratégies de transferts internationaux des données personnelles », *Dalloz IP/IT* 2016, p. 340.

30 - Et ce n'est pas fini. Pour une prise de conscience politique, voir la Communication de la Commission européenne au Parlement européen et au Conseil du 10 janvier 2017 sur « Échange et protection de données à caractère personnel à l'ère de la mondialisation » (COM(2017) 7 final).

directive 95/46/CE, en particulier en Amérique du Sud, en Afrique, en Asie et dans le Pacifique[31].

Ont aussi été mises en place des autorités nationales de protection des données personnelles dans tous ces pays, à l'image de ce qu'impose la directive aux États membres. L'entrée en application du RGPD en mai 2018 entraîne logiquement une nouvelle vague de réflexions des pays partenaires de l'UE, en particulier ceux considérés comme adéquats sous l'empire de la directive, souhaitant préserver ce statut sous le RGPD. La réflexion est lancée au Canada, reconnu partiellement adéquat pour les transferts vers les seules organisations du secteur privé sur le fondement de la loi sur la protection des renseignements personnels (*Personal Information Protection and Electronic Documents Act* dite *PIPEDA*). De son côté, la Suisse est en cours de modification de sa loi fédérale de protection des données (LPD) du 19 juin 1992 (RS 235-1), en vue de se rapprocher des exigences du RGPD, mais aussi de la directive 2016/680/UE en matière pénale à laquelle elle est tenue par l'accord de Schengen.

Flux transfrontaliers entre l'UE et les US : la conclusion d'accords bilatéraux. Dans ce contexte, et en dépit de l'importance des flux de données entre ces deux zones géographiques[32], la Commission européenne a refusé de reconnaître que le droit des États-Unis présente un « niveau de protection adéquat », eu égard à

31 - See Anu Bradford, « The Brussels Effect » (2012). *Northwestern University Law Review*, Vol. 107, No. 1, 2012; *Columbia Law and Economics* Working Paper No. 533. Available at SSRN: https://ssrn.com/abstract=2770634. P. M. Schwartz, *Ibid*. Pour se convaincre de l'influence de la directive 95/46/CE sur les législations nationales du monde entier, voir la revue législative de 63 pays réalisée en mars 2013 (2e éd.) par le cabinet DLA Piper : http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf. Pour une illustration concrète de la convergence normative sur le droit à l'oubli, voir : W. Gregory Voss and Céline Castets-Renard, « Proposal for an International Taxonomy on the Various Forms of the 'Right to Be Forgotten': A Study on the Convergence of Norms » (June 26, 2016). *14 Colorado Technology Law Journal 281* (2016) (Issue 14.2) (pp. 281-344). Available at SSRN: https://ssrn.com/abstract=2800742.

32 - Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy,* ,*op. cit.* spéc. p. 175.

son caractère parcellaire et sectoriel[33]. Afin de permettre l'échange de données entre ces deux zones géographiques, un outil spécifique a alors été élaboré, mis à la disposition des entreprises états-uniennes, sur la base d'un accord bilatéral dit « safe harbor » entre la Commission européenne et le Département du Commerce (US DoC)[34]. Sans revenir sur le faible niveau de protection conféré dans les faits par cet accord, son invalidation par la Cour de justice de l'UE en octobre 2015 dans le fameux arrêt *Schrems*[35] a entraîné de nouvelles négociations et son remplacement par le *Privacy Shield*[36] dont le niveau de protection a été considéré comme adéquat par la Commission européenne[37].

***Privacy Shield* : un fond commun US-EU à l'avenir ?** Malgré cette décision d'adéquation de la Commission européenne, des doutes ont été émis dès l'origine sur la vigueur du *Privacy Shield*[38]. La première

33 - Pour une compréhension globale du droit fédéral américain de protection de la vie privée et des données : D. J. Solove et P. M. Schwartz, *Information Privacy Law*, Wolters Kluwer, 6th Ed., 2017. Des mêmes auteurs : *An Overview of Privacy Law* (October 5, 2015). Chapter 2 of *PRIVACY LAW FUNDAMENTALS* (published by IAPP, 2015); *GWU Law School Public Law* Research Paper No. 2015-45; *GWU Legal Studies* Research Paper No. 2015-45. Available at SSRN: https://ssrn.com/abstract=2669879. Axel Tschentscher, Privacy and Data Protection by Rules Rather than Principles (August 4, 2017). Available at SSRN: https://ssrn.com/abstract=3013830. Chris Jay Hoofnagle, US Regulatory Values and Privacy Consequences, 2 Eur. Data Prot. L. Rev. 169-177 (2016); *UC Berkeley Public Law* Research Paper No. 2801404. Available at SSRN: https://ssrn.com/abstract=2801404.

34 - Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique.

35 - CJUE, 6 oct. 2015, aff. C-362/14, *Maximilian Schrems vs Data Protection Commissioner* («Schrems») ; ECLI:EU:C:2015:650. V. Not. C. Castets-Renard, « Invalidation du *safe harbor* par la CJUE : tempête sur la protection des données personnelles aux États-Unis », *Dalloz* 2016, p. 88.

36 - C. Castets-Renard, « L'adoption du *Privacy Shield* sur le transfert de données personnelles », *D.* 2016, p. 1696 ; Fl. Benoît-Rohmer, Chronique Union européenne et droits fondamentaux – « L'adoption de mesures visant à renforcer la protection des données personnelles », *RTD eur.* 2017, p. 355.

37 - Décision de la Commission 2016/1250/UE du 12 Juillet 2016 concernant la Directive 95/46/CE du Parlement Européen et du Conseil sur l'adéquation de la protection apportée par l'accord UE-US Privacy Shield, JO L 207, 1.8.2016, p. 1.

38 - C. Castets-Renard, « Adoption du *Privacy Shield* : des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* 2016, p. 444. M. Schrems, « The Privacy Shield is a Soft Update of the Privacy Shield », 2, *Eur. Data Prot. L. Rev.* 148 (2016). Christopher Kuner, « Reality and Illusion in EU Data Transfer Regulation Post Schrems » (July 7, 2017). *18 German Law Journal 881* (2017). Available at SSRN: https://ssrn.com/abstract=2732346.

revue annuelle réalisée fin 2017 par la Commission européenne[39] et le G29[40] n'a pas véritablement permis de les dissiper[41]. Les affaires pendantes devant la Cour de justice concernant cet accord[42], ainsi que les clauses contractuelles types, autre instrument permettant les flux transfrontaliers de données, laissent d'ailleurs augurer de nouveaux remous[43]. Si on ajoute à cela l'insécurité politique générée par l'administration Trump[44] et le peu de considération pour les questions de *Privacy*, on peut penser que le fonds commun ainsi trouvé entre les États-Unis et l'Union européenne au travers de ce *Privacy Shield* semble fragile et risque d'être éphémère. D'autres pistes doivent alors être recherchées.

39 - *First annual review of the functioning of the EU–U.S. Privacy Shield*, 18 oct. 2017, COM(2017) 611 final. La revue annuelle a été faite par la Commissaire européenne pour la Justice, la consommation et l'égalité des genres, Věra Jourová, et le secrétaire au commerce Wilbur Ross. La délégation européenne contenait aussi huit représentants désignés par l'article 29, le conseil des autorités nationales de protection des États membres, ainsi que le Contrôleur européen à la protection des données. Du côté états-unien, des représentants du département du commerce, de la *Federal Trade Commission (FTC)*, du Département du Transport, du Département d'État, du Bureau du Directeur de l'Intelligence nationale (*Director of National Intelligence – DNI*) et le département de la Justice ont participé à la revue, ainsi que l'*Ombudsperson*, un membre du *Privacy and Civil Liberties Oversight Board (PCLOB)* et du Bureau de l'Inspecteur Général de la communauté du renseignement (*Inspector General of the Intelligence Community*).

40 - *EU-US Privacy Shield – First Annual Joint Review*, 28 Nov. 2017, WP 255.

41 - C. Castets-Renard, « Privacy Shield: toward a strong Personal Data Protection between the US and the EU? », *in Quel avenir pour la coopération transatlantique ?*, dir. R. Bismuth, *La Revue des juristes de Sc Po* n° 14, 2018, à paraître. Voir aussi S. Peyrou, « Transfert de données à caractère personnel UE-Etats Unis : nouvel épisode du feuilleton « Privacy Shield » (Réflexions à propos du rapport du Groupe de l'article 29 relatif au premier examen annuel conjoint du Privacy Shield, WP 255) », *site du GDR ELSJ* : http://www.gdr-elsj.eu/2018/01/01/informations-generales/transfert-de-donnees-a-caractere-personnel-ue-etats-unis-nouvel-episode-du-feuilleton-privacy-shield-reflexions-a-propos-du-rapport-du-groupe-de-larticle-29-re.

42 - Une première action entreprise par *Digital Rights Ireland* a été déclarée inadmissible (TPE, Ord. 22 nov. 2017, *Digital Rights Ireland v. Commission*, aff. T-670/16). Le tribunal de l'UE a considéré que les plaignants ne justifiaient pas d'un intérêt à agir. Une seconde action est portée par *La Quadrature du Net* sur laquelle la Cour de justice ne s'est pas encore prononcée (action portée le 25 oct. 2016, *La Quadrature du Net et autres v Commission*, aff. T-738/16). Le juge de l'UE pourrait décider dans cette affaire si le droit à un recours effectif et un tribunal impartial (Charte de l'UE, art. 47) est garanti ou non par le Privacy Shield.

43 - Dans une affaire opposant le commissaire irlandais à la protection des données à Facebook Ireland Ltd et, à nouveau, Maximilian Schrems, la Haute Cour Commerciale d'Irlande a décidé en Octobre 2017 de saisir la Cour de justice de l'UE pour une question préjudicielle portant sur la validité des clauses contractuelles contractuelle (n° 2016/4809P).

44 - C. Castets-Renard, « Privacy Shield: toward a strong Personal Data Protection between the US and the EU? », art. préc. ; A. Butler, « Whiter Privacy Shield in the Trump Era », *Eur. Data Prot. L. Rev.*, 111 (2017).

***Compliance* et *self-regulation* : assouplissement des outils normatifs dans le RGPD.** Si on s'attache, par ailleurs, à observer les outils normatifs mis en œuvre au sein du RGPD, on constate un certain assouplissement de la règlementation européenne, en comparaison de la directive de 1995. Le RGPD marque en effet un changement de culture, en consacrant désormais un système de contrôle *a posteriori* et non plus *a priori* par la suppression du système de déclaration préalable des traitements de données personnelles. Désormais, les responsables de traitement sont libres du choix des méthodes et instruments utilisés au sein de leurs organisations, sous réserve de documenter et d'être en capacité de prouver leur conformité au RGPD. Ainsi, les entreprises vont pouvoir déterminer leurs règles internes, afin de respecter concrètement les obligations du règlement, tenant par exemple à la protection de la vie privée dès la conception (*privacy by design*) (art. 25), aux études d'impact (*Privacy Impact Assesment*) (art. 33)[45], à la nomination d'un délégué à la protection des données (*data protection officer*) (*DPO*) ou encore aux règles d'entreprises contraignantes (*Binding Corporate Rules ou BCR*) (art. 46 et s.). Les entreprises doivent ainsi rendre compte (*accountability*) des choix faits[46]. Un tel système de *compliance*[47] est classique aux États-Unis, mais moins généralisé en Europe. En France, ce changement de méthode n'est pas propre à la protection des données personnelles et caractérise désormais la vie des entreprises[48], au point que d'aucuns évoquent un « monde nouveau »[49]. Aux États-Unis, cette conception caractérise

45 - Voir la méthode de cartographie des risques (étude d'impact) proposée par la CNIL : https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil.

46 - Winston Maxwell et Sarah Taïeb, « L'*accountability*, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT* 2016, p. 123.

47 - La Cercle de la Compliance la définit comme « L'ensemble des processus qui permettent d'assurer le respect des normes applicables à l'entreprise par l'ensemble de ses salariés et de ses dirigeants, mais aussi des valeurs et d'un esprit éthique insufflé par les dirigeants » : http://www.cercledelacompliance.com.

48 - Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite loi « Sapin II » et loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneurs d'ordre dite loi « vigilance ». Voir Géraldine Péronne et Emmanuel Daoud, Loi Sapin II, loi vigilance et RGPD : pour une approche décloisonnée de la *compliance*, Dalloz IP/IT 2017, p. 584.

49 - *La* compliance *: un monde nouveau ? Aspects d'une mutation du droit*, dir. A. Gaudemet, Colloques, Ed. Panthéon-Assas, 2016.

de nombreuses règlementations sur la *privacy* et laisse une large marge de manœuvre importante aux opérateurs dans la collecte et l'utilisation des informations personnelles. Ces derniers doivent autodéclarer leur conformité, comme l'illustre le système mis en œuvre par le S*afe harbor* et désormais par le *Privacy Shield*.

« **Droit souple** » ***versus*** « **droit dur** ». Naturellement, un tel système d'autorégulation (« droit souple ») ne peut être efficace et respecté que si des contrôles existent, associés à des sanctions, ce que le RGPD tend à faire en augmentant sensiblement les sanctions et les pouvoirs des autorités de contrôle. Le droit antérieurement mis en œuvre par la directive 95/46/CE, consacrant essentiellement des règles précises (« droit dur »), n'a pas fait la preuve de son efficacité. En France, par exemple, il est couramment admis que de nombreuses organisations publiques et privées ne sont pas conformes aux obligations posées par la loi 78-17 du 6 janvier 1978 dite informatique et libertés. Dès lors, sans doute faut-il dépasser le constat d'une simple opposition entre droit dur et droit souple et ne pas déduire une efficacité naturelle ou évidente du premier qui ne serait pas possible pour le second. L'effectivité n'est souvent pas aussi bonne qu'elle le devrait dans les deux cas, aussi doit-on poser plus globalement la question de savoir comment garantir une meilleure efficacité des règlementations sur la protection des données personnelles et de la vie privée. Le RGPD propose de nouvelles solutions et il faut accorder du temps pour en tirer des conclusions. En attendant, on peut d'ores et déjà constater que cette nouvelle façon de règlementer la protection des données personnelles est plus familière du droit américain, sans pour autant être identique. Ce constat se confirme à l'analyse de certaines règles précises du RGPD.

§2 : À la recherche d'un fonds commun dans le choix des règles applicables

Influences mutuelles. Les cultures et règlementations de la *privacy* et des données personnelles diffèrent, mais les négociations du *Privacy Shield* invitent les États-Unis à intégrer certaines exigences de l'approche européenne. L'inverse est également vrai. Le RGPD consacre de nombreuses nouvelles règles, parfois issues des droits des États membres qui ont pu être eux-mêmes précédemment inspirés par les lois américaines. Dans le cadre de ces quelques observations, l'objectif n'est pas de recenser l'intégralité des règles consacrées par

les 99 articles du règlement, ni même de savoir quelle part d'entre elles pourrait trouver leur origine en droit américain. Il s'agit simplement ici d'illustrer l'existence même d'une telle influence.

Notification des failles de sécurité dans le RGPD : exemple d'une convergence normative. Pour ce faire, l'exemple choisi ici est la règle de notification des failles de sécurité impactant les données personnelles, consacrée en droit allemand et espagnol, et précédemment dans plusieurs lois fédérales et étatiques des États-Unis. L'article 33 § 1 du RGPD prévoit désormais : « en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente ». La notification doit avoir lieu si possible 72 heures au plus tard après en avoir pris connaissance. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Cependant, la notification n'a pas lieu d'être si la violation en question n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. De même, le sous-traitant doit aussi notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Le paragraphe 3 précise par ailleurs les informations que doit contenir la notification et qui peuvent être communiquées de manière échelonnée (§ 4). Le responsable du traitement doit enfin documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier (§ 5). Outre la notification à l'autorité nationale de contrôle, le responsable de traitement doit aussi informer la personne concernée par une violation, susceptible d'engendrer un risque élevé pour les droits et libertés de ladite personne (art. 34). Des exceptions sont toutefois prévues, tenant au fait que le risque soit limité par la mise en œuvre de mesures de protection techniques et organisationnelles, telles que le chiffrement. La communication est aussi écartée si elle exige des efforts disproportionnés (§ 3).

Notification des failles de sécurité aux États-Unis. La Californie fut le premier État fédéré à consacrer une obligation de notification des failles de sécurité en 2002[50]. En février 2005, l'entreprise

50 - Notice of Security Breach law (Cal. Civil Code § 1798.29).

ChoicePoint qui collecte et compile des données personnelles et financières de millions de consommateurs a subi une faille de sécurité ayant entraîné la perte massive d'informations personnelles. En application de la loi californienne, l'entreprise a révélé cette faille aux résidents de l'État pour ensuite étendre l'information aux résidents des autres États affectés par l'incident. Depuis, presque tous les États fédérés ont adopté de telles obligations, à l'exception notable de l'Alabama et le Dakota du Sud.

Classiquement, ces législations étatiques prévoient des dispositions concernant le débiteur de la notification (par exemple les entreprises, les courtiers de données, les entités gouvernementales...). Elles définissent aussi le plus souvent la notion de « faille » (par exemple un accès ou une acquisition non autorisée de donnée) et précisent les informations personnelles à notifier (le numéro de sécurité sociale, le numéro de permis de conduire, la carte d'identité, les numéros de compte...), ainsi que d'éventuelles exceptions, telle l'hypothèse des informations cryptées comme dans le RGPD. Des dispositions de même nature se retrouvent dans certaines lois fédérales sectorielles comme le *Health Insurance Portability and Accountability Act (HIPAA)* (1996) dans le domaine de la santé ou le *Gramm-Leach-Bliley Act (GLBA)* concernant les services financiers.

Efficacité du dispositif. Si l'Union européenne consacre cette nouvelle règle de notification des failles de sécurité, bien connue aux États-Unis, c'est *a priori* qu'elle en attend une amélioration de la protection des individus (voir le considérant 85). Pourtant, force est de constater que les praticiens émettent beaucoup de doute sur son intérêt. Elle risque en effet d'être contreproductive en renseignant les auteurs de la faille. Son respect est d'ailleurs mis à mal sur le terrain. Aux États-Unis, de nombreuses failles de sécurité sont en effet révélées trop tardivement par les entreprises touchées ou par des tiers[51], si bien que les bénéfices que l'on pouvait en attendre ne se vérifient pas. Au demeurant, les failles de sécurité génèrent des dommages pour les droits des personnes qui ne sont pas faciles à prouver et se dévoilent souvent *a posteriori*,

51 - Voir par exemple récemment l'immense faille subie par l'entreprise de scoring Equifax : https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html.

sans qu'il soit alors aisé d'établir un lien entre la faille et l'utilisation frauduleuse des données survenant des années après. Les Cours fédérale et étatiques ont tendance à ne pas accorder de réparation d'un préjudice considéré comme simplement moral et hypothétique et ne répondant pas aux exigences du préjudice économique de la *Tort Law*[52]. La doctrine américaine spécialiste de la *privacy* critique cette approche minimaliste et cherche à faire reconnaître par les juridictions la réalité des dommages subis[53]. En fin de compte, les gains pour la protection des personnes concernées ne sont pas évidents. Il convient, là aussi, d'attendre pour savoir si les autorités nationales de contrôle des États membres et les juges européens parviendront à de meilleurs résultats. L'efficacité du RGPD sur de nombreux points dépendra amplement de ces deux catégories d'acteurs, mais aussi des parties prenantes qui sont sans doute les mieux placées pour élaborer concrètement un fonds commun entre l'Union européenne et les États-Unis.

§3 : À la recherche d'un fonds commun au travers des parties prenantes

Renforcement judiciaire de la *privacy* aux États-Unis. Les institutions, en particulier la Commission européenne et le Département américain du Commerce, jouent un rôle important dans le rapprochement des systèmes. Cependant, les efforts déployés pour adopter le *Privacy Shield* sont à l'évidence

52 - Dans l'affaire *Spokeo v. Robins*, jugée le 16 mai 2016, relatif à de fausses informations diffusées par le moteur de recherche *Spokeo* concernant la situation personnelle de Monsieur Robins en violation du *Fair Credit Information Act*, la Cour Suprême a décidé de renvoyer l'affaire devant la Cour d'appel du 9ème circuit pour qu'elle détermine si le préjudice moral potentiel allégué était suffisamment « concret et non hypothétique » pour constituer un « cas » ou une « controverse » (*case or controversery requirements*) au sens de l'article III, sec. 2, cl. 1 de la Constitution et donner le pouvoir de décider à la Cour Suprême. Monsieur Robins faisait valoir que les informations sur son statut marital, sa situation professionnelle et sa formation étaient fausses et gênées sa recherche d'emploi, sans qu'il soit en mesure de prouver la perte d'une recherche d'emploi en particulier. L'opinion de la Cour, délivrée par le juge Alito, précise qu'une violation d'une disposition législative peut ne créer aucun préjudice et donc ne pas devoir être réparée. Dans une décision rendue le 15 août 2017, la Cour d'appel du 9ème circuit a décidé que le dommage allégué par le plaignant était suffisamment « concret » pour satisfaire les exigences de la Cour Suprême, en violation d'une obligation prévue par la loi. Dès lors, un préjudice moral simplement potentiel, mais suffisamment concret a pu être réparé.

53 - Daniel J. Solove et Danielle K. Citron, "Risk and Anxiety: A Theory of Data Breach Harms », *GW Law Faculty Publication*, 2017.

insuffisants. Force est de rechercher ailleurs un fonds commun. En observant de plus près le droit fédéral et étatique états-unien, on constate que les juridictions jouent un rôle important dans le respect des règlementations et auto-engagements des entreprises (*self regulation*)[54]. Ainsi, des contentieux se sont développés sur le fondement de lois spécifiques sur la *privacy* , mais aussi sur la *tort law*. Également, les règlementations fédérales et étatiques visant les pratiques commerciales déloyales et déceptives ont permis aux *State Attorney General* (procureurs généraux des Etats) de faire sanctionner des atteintes à la *privacy* par les entreprises, ainsi que sur le fondement d'autres lois fédérales protégeant la *privacy* (*FCRA*[55], *COPPA* et *HIPAA*) pour lesquelles ils sont compétents.

Renforcement du pouvoir exécutif aux États-Unis : la FTC, régulateur de la *privacy*. Par ailleurs, la section 5 du *FTC Act* a permis de confier à la *Federal Trade Commission* le rôle de régulateur de la *privacy*[56]. La Commission est désormais l'interlocuteur privilégié des autorités nationales de protection des États membres. Elle a prononcé 39 actions d'atteinte au *Safe Harbor* contre les entreprises américaines et trois en violation du *Privacy Shield*[57] pour avoir faussement déclaré aux consommateurs participer à cet accord[58]. La *FTC* n'est cependant pas compétente pour faire respecter toutes les législations fédérales spéciales concernant la

54 - « Privacy Bridges : EU and US Privacy Experts in Search of Transatlantic Privacy Solutions », art. préc.

55 - Fair Credit Reporting Act (1970).

56 - Daniel J. Solove et Woodrow Hartzog, « The FTC and the New Common Law of Privacy » (August 15, 2013). *114 Columbia Law Review 583* (2014); *GWU Legal Studies* Research Paper No. 2013-120; *GWU Law School Public Law* Research Paper No. 2013-120. Available at SSRN: https://ssrn.com/abstract=2312913 or http://dx.doi.org/10.2139/ssrn.2312913 ; Chris Jay Hoofnagle, « The Federal Trade Commission's Inner Privacy Struggle », in *The Cambridge Handbook of Consumer Privacy* (Evan Selinger, Jules Polonetsky, & Omer Tene, eds) (Cambridge University Press 2017, Forthcoming).; *UC Berkeley Public Law* Research Paper No. 2901526. Available at SSRN: https://ssrn.com/abstract=2901526. Chris Jay Hoofnagle, *Federal Trade Commission: Privacy Law and Policy*, Cambridge University Press, 2016.

57 - *The FTC alleges that human resources software company Decusoft LLC, printing services company Tru Communication, Inc. (doing business as TCPrinting.net), and Md7, LLC, which manages real estate leases for wireless companies, violated the FTC Act by falsely claiming that they were certified to participate in the EU-US Privacy Shield.*

58 - *According to FTC Chairman Maureen K. Ohlhausen: « Companies that want to benefit from these agreements must keep their promises or we will hold them accountable ».*

Privacy. Elle bénéficie en revanche d'un large champ d'action en matière de concurrence, consommation et atteintes à la *privacy* qualifiables de pratiques déloyales et déceptives. En comparaison, les droits nationaux des membres de l'UE donnent souvent compétence à plusieurs régulateurs dans ces domaines, comme c'est le cas en France avec l'Autorité de la concurrence et la CNIL, ce qui peut limiter l'efficacité de l'action en certaines circonstances.

Au-delà des institutions : les outils pratiques et réseaux internationaux de professionnels. Le *Privacy Shield* et le RGPD constituent des textes utiles pour aider les institutions à se rapprocher, mais s'avèrent être également une base de discussion entre les praticiens dans leurs relations transatlantiques[59]. En effet, même si le *Privacy Shield* est fragile en lui-même et pourrait être à son tour invalidé, les négociations menées entre les deux blocs géographiques obligent à pousser la comparaison et la réflexion plus loin sur ce qui peut être acceptable pour chacun. Dès lors, du point de vue de la construction normative et de la recherche d'une convergence, les efforts ainsi déployés ne sont certainement pas vains. Cette base est particulièrement pertinente pour les acteurs de terrain, en particulier les entreprises et organismes non lucratifs. Au-delà des questionnements sur la solidité du *Privacy Shield*, force est bien pour les opérateurs de travailler ensemble et de trouver des solutions pour sécuriser ces échanges. Ces solutions résident naturellement dans les outils proposés par les institutions, comme les clauses contractuelles types de la Commission européenne, mais aussi les outils qu'elles élaborent elles-mêmes, tels les *BCR* (*Binding Corporate Rules*). Au demeurant, même à considérer le seul territoire américain, de nombreuses entreprises se sont dotées d'experts de la *privacy* (*Chief Privacy Officers* ou *CPOs*) qui tendent à imposer de bonnes pratiques de protection des données et à dépasser l'approche législative lacunaire du droit américain. D'aucuns évoquent même l'existence d'un « paradoxe » entre la *privacy* « dans les livres » et la *privacy* « sur le terrain » qui serait bien plus forte et convergente

59 - Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy*, *op. cit.,* spéc. p. 175.

qu'il y paraît[60]. Forts de cette réalité concrète, les professionnels américains sont naturellement conduits à expliciter leurs procédés à leurs partenaires européens, afin de gagner leur confiance. Les échanges transfrontaliers de données illustrent parfaitement le fait que la vie privée et l'utilisation des données personnelles sont une affaire de confiance entre toutes les parties prenantes[61]. Une analyse pragmatique invite à dépasser une approche manichéenne de mise en opposition des législations de l'Union européenne et des États-Unis.

En conclusion, on peut penser que le fragile fonds commun mis en œuvre par les institutions au travers du *Privacy Shield* risque d'avoir une durée de vie limitée. Il a cependant peut-être vocation à être remplacé par des outils pragmatiques et concrets des acteurs de terrain. Une démarche *bottom-up* peut trouver sa place dans le RGPD dont il faudra attendre sa réception à plus long terme pour en juger la réalité et l'efficacité.

60 - Kenneth A. Bamberger et Deirdre K. Mulligan, « Privacy on the Books and on the Ground » (November 18, 2011). *Stanford Law Review*, Vol. 63, January 2011; U*C Berkeley Public Law* Research Paper No. 1568385. Available at SSRN: https://ssrn.com/abstract=1568385.

61 - Ari Ezra Waldman, « Privacy as Trust: Sharing Personal Information in a Networked World » (March 1, 2014). *69 University of Miami Law Review 559* (2015). Available at SSRN: https://ssrn.com/abstract=2309632 or http://dx.doi.org/10.2139/ssrn.2309632 .

TOUS RESPONSABLES DE TRAITEMENT DE DONNÉES PERSONNELLES ?

Mélanie Clément-Fontaine
Maître de conférences HDR, DANTE, UVSQ, Université de Paris-Saclay

En ces premières semaines d'application du bloc européen de protection des données, en particulier du Règlement (UE) n° 2016/679 (RGDP)[1], et bientôt de la nouvelle loi informatique et liberté[2], la question consiste à savoir si nous ne serions pas tous potentiellement responsable de traitement. En effet qui, aujourd'hui, n'est pas susceptible de manipuler les données personnelles d'autrui ? Deux raisons principales, de nature conjoncturelle, justifient une telle interrogation. La première tient à la définition de données personnelles qui ne cesse de s'élargir en fait et, par voie de conséquence, en droit : la notion couvre toute information se rapportant à une personne physique identifiée ou identifiable et exclut les données anonymes ; pour autant, chacun, sans être expert en informatique, prend peu à peu conscience que la réidentification d'une personne est à la portée de ceux qui drainent les traces numériques que nous laissons de-ci de-là parfois aussi anodines que la manière particulière de frapper les touches d'un clavier d'ordinateur[3]. La seconde raison tient à la prolifération des outils de traitement des données qui, d'un côté se démocratisent et

1 - Ce bloc est constitué du Règlement général des données personnelles (RGDP) (Règl. (UE) n° 2016/679, 27 avr. 2016) et de la directive (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

2 - En cours de discussion au Parlement français. Projet de loi n° 490 du 13 décembre 2017 relatif à la protection des données personnelle.

3 - Il existe une technique biométrique de reconnaissance des personnes reposant sur le rythme de frappe propre à chacun appelée « frappologie ». Elle est appliquée par exemple au mot de passe qui devient ainsi beaucoup plus difficile à reproduire.

de l'autre irrigue l'économie actuelle[4]. Il est aujourd'hui commun de relever que celui qui détient à la fois la plus grande base de données et les outils pour les valoriser occupe une place prépondérante sur le marché[5].

Or, être responsable de traitement entraine des obligations importantes[6] dès lors que l'on tombe sous le coup du régime de protection de l'Union européenne dont le champ territorial a été élargi. Le RGDP s'étend à tout responsable de traitement, qu'il soit établi sur le territoire de l'Union ou pas, dès lors qu'il a recours à des moyens de traitement situés sur le territoire d'un État membre. Ainsi, il vise tout d'abord le responsable de traitement ou le sous-traitant qui dispose d'un établissement situé dans l'Union qui réalise un traitement de données à caractère personnel dans le cadre des activités de cet établissement et ce, peu importe que le traitement soit ou ne soit pas réalisé sur le territoire de l'Union[7]. Ensuite, la portée du RGDP s'étend au responsable de traitement et au sous-traitant qui, bien que n'étant pas établis dans l'Union, ont des activités de traitement liées à l'offre de biens ou de services gratuits ou payants aux personnes physiques qui se trouvent sur le territoire de l'Union[8].

4 - Règl. (UE) n° 2016/679, considérant 6 : L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publique ment et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

5 - Martine Behar-Touchais (dir.), *L'effectivité du droit face à la puissance des géants de l'Internet*, IRIS éd. 2015.

6 - Notons que le principe de responsabilité («*accountability*») introduit par le RGDP se substitue au système déclaratif Règl. (UE) n° 2016/679, art. 24.

7 - La notion d'établissement est définie dans le RGDP comme l'exercice effectif et réel d'une activité au moyen d'un dispositif stable, quelle que soit la forme juridique d'un tel dispositif. Il n'est donc pas nécessaire notamment que l'établissement soit doté de la personnalité juridique : Règl. (UE) n° 2016/679, consid. 22.

8 - Règl. (UE) n° 2016/679, consid 23.

Par-delà le contexte technique et social, mais aussi l'étendue territoriale du régime de protection dont s'est dotée l'Union européenne, la question se pose avec d'autant plus d'acuité que les critères de la définition de responsable de traitement sont accueillants tandis que l'exception des traitements personnelle ou domestique s'entend strictement.

§1 : Des critères accueillants

La notion de responsable de traitement a été définie, pour la première fois, par la directive du 25 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[9] comme «*le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement, détermine les finalités et les moyens du traitement de données à caractère personnel*»[10].

Par ailleurs, de jurisprudence constante, la notion de responsable traitement est entendue largement afin de garantir une meilleure protection des données à caractère personnel des personnes physiques et partant de la protection de la vie privée. L'une des plus célèbres illustrations de cette jurisprudence est l'arrêt Google Spain[11]. Sans qu'il soit nécessaire de rappeler en détail cette affaire amplement commentée[12], on soulignera simplement que la Cour a adopté une conception étendue de la notion de responsable de traitement tout d'abord en retenant une appréciation généreuse de la portée territoriale de la directive 95/46[13], ensuite en considérant que l'activité de moteur de recherche doit être qualifiée de traitement

9 - Directive 95/46/CE.

10 - Article 2 de la directive 95/46/CE.

11 - Arrêt du 13 mai 2014, *Google Spain et Google* : C-131/12, EU:C:2014:317.

12 - *RTD eur.* 2014. 283, édito J.-P. Jacqué, 879, étude B. Hardy, et 2016. 249, étude O. Tambou ; *D.* 2014. 1476, note V.-L. Benabou et J. Rochfeld, 1481, note N. Martial-Braz et J. Rochfeld, et 2371, obs. P. Tréfigny ; *AJDA* 2014, 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; *AJCT* 2014. 502, obs. O. Yambou ; Constitutions 2014. 218 chron. *D.* de Bellescize ; Dossier spécial *RLDI* 2014, n° 106. C. Castets-Renard, « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *Revue Lamy droit de l'immatériel*, 2014, n° 106.

13 - F. Jault-Seseke et C. Zolynski, «Le règlement 2016/679/UE relatif aux données personnelles. Aspects de droit international privé» *D.* 2016 p.1874.

de données[14] de sorte que, selon la CJUE, ce n'est pas l'utilisateur de moteur de recherche qui est responsable de traitement, mais celui qui met l'outil à disposition[15]. Enfin, la définition du responsable de traitement consacrée par le RGDP fait apparaître clairement les deux critères essentiels à savoir la capacité juridique et organisationnelle d'une part et l'autonomie à définir les finalités et les moyens du traitement d'autre part : «*est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre*».

Les critères ainsi posés permettent d'accueillir de nouvelles pratiques dans le giron de la protection des données à caractère personnel.

Premier critère : La capacité juridique et organisationnelle suppose que la personne (qui peut être physique ou morale, privée ou publique) agisse dans son propre intérêt, en son nom et pour son propre compte. De plus, les États membres ont la possibilité de désigner la personne dite responsable du traitement des données personnelles. Ainsi, selon le droit national français, la Caisse nationale d'assurance maladie (CNAMTS), qui est autorisée à procéder au traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1), est désignée par un texte réglementaire comme responsable de la création et la gestion de cette base vaccinale[16]. L'autorité de régulation de la protection des données personnelles (la CNIL) a pu en déduire

14 - Sur le fondement de l'article 2 b de la directive 95/46/CE, la CJUE décide que l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, en fin à les mettre à disposition des internautes selon un ordre de préférence donné doit être qualifié de « traitement de données à caractère personnel » lorsque ces informations contiennent des données personnelles.

15 - Voir l'application de ce raisonnement par les Cours de cassation belge (décision du 29 avril 2016, n ° C. 15 .0052 F) et française (Civ. 1, 12 mai 2016, n° 15-17.729) : notre commentaire groupé, *Auteur&Media* 2016/5-6, p. 453 et spéc. 456.

16 - Décret n° 2009-1273 du 22 octobre 2009.

que la CNAMTS est la seule responsable de traitement bien que plusieurs autres organismes interviennent dans la mise en œuvre de ce traitement. Cet exemple conduit à rappeler la distinction qui est faite entre responsable de traitement et sous-traitant. Contrairement au responsable de traitement, la mission du sous-traitant ne consiste pas à définir les finalités et les moyens de traitement, il agit pour le compte du responsable de traitement[17].

Second critère : l'autonomie à définir les finalités et les moyens du traitement permet davantage encore d'étendre la notion de responsable de traitement. Concrètement le responsable du traitement de données à caractère personnel est la personne qui décide pourquoi et comment seront traitées ces données. Comme l'indique le groupe de travail du G29, «*la notion de responsable du traitement est une notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle s'appuie donc sur une analyse factuelle plutôt que formelle*»[18]. L'apparente simplicité du critère recèle bien des interrogations. Les situations complexes se multiplient donnant lieu le plus souvent à des responsabilités conjointes. En effet, la mise en réseau des données favorise des traitements simultanés par plusieurs acteurs de manière horizontale de sorte que chacun est susceptible d'être qualifié de responsable de traitement en lieu et place de sous-traitant. Aussi, est-il précisé notamment à l'article 4 septièmement du RGDP que le responsable traitement «*est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement*». Partant, deux situations doivent être distinguées : selon la première situation, les responsables de traitement déterminent ensemble les finalités et les moyens du traitement et sont alors considérés conjointement responsables[19] de sorte que la victime peut demander réparation de la totalité de son préjudice à l'un d'entre eux à charge, pour ce dernier, de se tourner vers son cocontractant. Dans la seconde hypothèse, ils déterminent indépendamment les finalités et les moyens du traitement ; alors, l'étendue de leurs obligations sera proportionnelle à leur action

17 - Règl. (UE) n° 2016/679, art. 4.

18 - Avis 1/2010, p. 10.

19 - Règl. (UE) n° 2016/679, art. 26 § 1.

quand bien même le traitement porte sur les mêmes données. Le Groupe 29 résume la problématique en ces termes : *«lorsqu'il y a pluralité d'acteurs, ils peuvent entretenir une relation très proche (en partageant, par exemple, l'ensemble des finalités et des moyens d'une opération de traitement) ou, au contraire, plus distante (en ne partageant que les finalités ou les moyens, ou une partie de ceux-ci). Dès lors, un large éventail de typologies de la coresponsabilité doit être examiné, et leurs conséquences juridiques évaluées avec une certaine souplesse pour tenir compte de la complexité croissante de la réalité actuelle du traitement de données».*

Des affaires récentes,[20] soumises à la CJUE par la voie des questions préjudicielles, illustrent la complexité de la réalité actuelle du traitement des données personnelles qui peut tenir à la fois d'une pluralité des traitements simultanés et de l'apparition de nouvelles techniques de traitement comme les codes programmes « Facebook Insights » et « le module : j'aime » d'un réseau social. En effet, ces codes programmes permettent au réseau social qui les fournit de récupérer les données personnelles des personnes visitant le site ou la page sur lesquels les programmes sont installés ; de traiter ces données aux fins de procéder à la publicité ciblée ; et de fournir au gestionnaire du site ou de la page web des statistiques sur la fréquentation. Dans ces deux affaires[21], connues respectivement sous le nom de *Fashion ID* (C-40/17) et *Fan page* (C-210/16), la CJUE doit, pour la première fois, préciser si la personne qui insère dans son site ou sa page web le code programme a la qualité de responsable de traitement. La question est épineuse dans la mesure où le réseau social détermine à titre principal les objectifs et les modalités du traitement[22], tandis que le gestionnaire du site ou de la page web est à l'origine du processus en installant le programme informatique, mais n'en a pas la maitrise. Dans l'affaire C-210/16,

20 - Demande de décision préjudicielle présentée par l'*Oberlandesgericht* Düsseldorf (Allemagne) le 26 janvier 2017 — *Fashion ID GmbH & Co. KG contre Verbraucherzentrale NRW eV*, JO R 112 du 10 avril 2017, (2017/C 112/32) et CJUE, Concl. avocat général Yves Bot, 24 oct. 2017, aff. C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH, en présence de Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht*, pts 46 à 57 : *Comm. com. électr*. 2018, comm. 5, note Metallinos N.

21 - Préc.

22 - CNIL, Dél. n° 2017-006, 27 avril 2017, prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Irland.

une société allemande, spécialisée dans le domaine de l'éducation, avait créé une « page fan » (*Fanpage*) sur le réseau social Facebook de sorte qu'elle utilise l'outil appelé « Facebook Insights ». Cet outil est proposé par Facebook gratuitement, dans le cadre de conditions d'utilisation non modifiables aux administrateurs d'une « page fan ». Il permet à ces derniers d'obtenir des statistiques anonymes élaborées par Facebook à partir des données personnelles des personnes qui consultent la page et selon des critères qui peuvent être personnalisés par l'administrateur. Par ailleurs, Facebook utilise ces données personnelles afin de diffuser de la publicité ciblée. L'autorité régionale de protection des données de Scheswig-Holstein (l'ULD) avait, par décision du 3 novembre 2011, ordonné à l'administrateur de désactiver la page fan qu'il avait créée sur Facebook sous peine d'astreinte au motif que ni lui ni Facebook n'informaient les visiteurs de la page que ce dernier collectait leurs données à caractère personnel et qu'il les traitait. L'administrateur a alors introduit une réclamation contre cette décision dans laquelle il faisait valoir qu'il n'était ni responsable du traitement des données effectué par la société Facebook ni des cookies installés par elle. Par décision du 16 décembre 2011, l'UDL a rejeté cette réclamation considérant qu'en créant la page fan l'entreprise apportait également une contribution active et volontaire à la collecte de données à caractère personnel par Facebook, dont elle profitait grâce à des statistiques concernant les utilisateurs mis à disposition par ce réseau. L'entreprise a alors introduit un recours à l'encontre de cette décision devant le tribunal administratif allemand en faisant valoir notamment que l'ULD s'est retournée à tort contre elle et non directement contre Facebook. Le tribunal administratif, par un arrêt du 9 octobre 2013, lui donna raison en jugeant qu'elle n'était pas « organisme responsable » au sens de l'article 3 paragraphe 7 de la loi fédérale sur la protection des données et par conséquent annula la décision de l'ULD. La décision ayant été confirmée par le tribunal administratif supérieur allemand, l'ULD forma un recours en *Révision* devant la Cour administrative fédérale. Il est intéressant de s'arrêter un instant sur les motifs conduisant la Cour à ne pas qualifier la société administratrice de la page de responsable de traitement. La Cour considère que l'intimé ne détermine pas les finalités et les moyens de traitement de données personnel dans la mesure où, en prenant la décision de recourir à l'outil mis à disposition par Facebook, il n'a pas la possibilité d'influencer, de

guider, de modeler ou encore de contrôler la nature et l'étendue du traitement des données des utilisateurs de sa page fan par Facebook en raison de l'absence de négociation des conditions d'utilisation fixées unilatéralement par Facebook ni encore lui interdire de collecter et de traiter ces données. Par ailleurs, elle relève que le profit tiré de l'outil (l'obtention des statistiques de données anonymes) par l'administrateur n'est pas suffisant pour la qualifier de responsable de traitement. Partant de ce postulat, la Cour décida de sursoir à statuer pour demander, entre autres à la CJUE, si l'ULD était fondée à exercer ses pouvoirs d'intervention à l'encontre d'une personne n'ayant pas la qualité de traitement au sens de l'article 2, sous d), de la directive 95/46, mais qui pourrait malgré tout être tenue responsable en cas d'atteinte aux règles relatives à la protection des données à caractère personnel du fait de recourir à un réseau social tel que Facebook pour diffuser son offre d'informations. Or l'avocat général conteste le postulat de la Cour selon lequel l'administrateur n'est pas responsable de traitement et considère, au contraire, qu'il est responsable conjointement avec Facebook de la phase du traitement consistant dans la collecte de données à caractère personnel[23]. La raison principale avancée par l'avocat général tient au fait que l'administrateur exerce une influence déterminante sur le déclenchement du traitement des données à caractère personnel des personnes qui consultent sa page et inversement, il dispose du pouvoir de faire cesser ce traitement en fermant sa page fan. Par ailleurs, en ciblant un certain public il oriente les catégories des personnes dont les données seront collectées par Facebook. De plus, pour l'avocat général les responsables conjoints de traitement poursuivent des finalités étroitement liées : l'administrateur veut améliorer sa communication grâce aux statistiques d'audience et Facebook veut mieux cibler la publicité diffusée sur son réseau. Enfin, retenant une appréciation *in concreto* à partir des faits de l'espèce, l'avocat général rejette l'interprétation de la Cour tirée d'après lui exclusivement des clauses et des conditions du contrat conclu entre les protagonistes. Il rappelle à ce titre «*il n'est pas nécessaire pour être qualifié de responsable de traitement au sens de la directive 95/46 de disposer d'un pouvoir de contrôle sur tous les aspects du traitement. Affirmer le contraire, conduirait à limiter sérieusement la protection des*

23 - Affaire C-210/16, point 42.

données personnelles compte tenu de la complexité actuelle des traitements faisant intervenir plusieurs acteurs aux rôles complémentaires. Enfin, dans un souci de garantir la protection des personnes physiques, il importe de ne pas ouvrir une brèche qui consisterait à échapper aux obligations de responsable de traitement dès lors que l'on a recours aux services d'un tiers. Une interprétation contraire créerait un risque de contournement des règles relatives à la protection des données à caractère personnel»[24]. L'avocat général poursuit son analyse en ce référent à une autre affaire qui n'a pas encore été tranchée par la Cour (C-40-17). Dans cette dernière affaire dite Fashion ID, le gestionnaire d'un site web, la société Fashion ID a inséré dans son site ce que l'on appelle un «module social» (en l'occurrence le bouton «j'aime» de Facebook) d'un fournisseur externe (c'est-à-dire Facebook), qui entraîne une transmission de données à caractère personnel de l'ordinateur de l'utilisateur du site web au fournisseur externe. Une association de protection des consommateurs reproche à la société Fashion ID d'avoir ainsi permis à Facebook l'accès aux données à caractère personnel des utilisateurs de ce site, sans leur consentement et ce, en violation des obligations d'informations. La question posée à la CJUE consiste à déterminer si la Société Fashion ID est un responsable de traitement. Pour l'avocat général, les faits sont comparables à l'affaire *Fan page* (C-210/16) et conduisent à la même conclusion : l'administrateur d'une page ou l'exploitant d'un site web qui intègre le code d'un fournisseur de services de webtracking à son site web contribue à la transmission de données personnelles, l'installation de cookies et la collecte de données au profit du fournisseur de services de webtracking en sus du leur. Le gestionnaire d'un site web qui utilise ces modules sociaux est ainsi également un responsable de traitement au sens de la Directive 95/46 (et du RGPD).

Si l'on poursuit le raisonnement de l'avocat général, rien n'interdit de qualifier les utilisateurs d'un réseau social de responsables de traitement sauf à considérer que cette activité est strictement personnelle et domestique.

24 - Affaire C-210/16, Point 65.

§2 : L'exclusion des activités strictement personnelles ou domestiques

Selon le considérant 18 du RGDP, n'entrent pas dans le champ de protection les traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques. Le texte vise en particulier l'échange de correspondance et la tenue d'un carnet d'adresses, l'utilisation de réseaux sociaux et, enfin, les activités en ligne qui ont lieu dans le cadre de ces activités.

À titre liminaire, trois observations d'ordre général sur la portée de l'exception doivent être faites : tout d'abord, l'exception ne se borne pas aux seuls cas d'activités personnelles ou domestiques énumérés dans le texte. Par conséquent, le caractère non limitatif de la liste permet d'envisager d'autres activités susceptibles d'être personnelles ou domestiques ; ensuite, la liste ne lie pas le juge qui apprécie *in concreto* la situation afin de déterminer s'il s'agit réellement d'une activité personnelle ou domestique ; enfin, l'exception ne bénéficie pas aux responsables de traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

À ce stade, s'il demeure hasardeux de cartographier de manière abstraite ce qui relève effectivement d'une activité personnelle ou domestique et partant d'anticiper l'interprétation qu'en feront les juges, les exemples cités dans le considérant 18 du RGDP appellent une première série de réflexions.

Le premier exemple, relatif à l'échange de correspondance et la tenue d'un carnet d'adresses, est sans doute celui qui pose le moins de difficultés. L'exclusion du champ de la protection des données personnelles des carnets d'adresses personnels est déjà connue. En effet, elle est notamment consacrée à l'article 2 de la loi de 1978. Quant à la correspondance privée, elle a fait l'objet d'une importante jurisprudence tendant à tracer la frontière d'avec la correspondance professionnelle.

Le deuxième exemple, qui vise l'utilisation de réseaux sociaux, est sans doute davantage délicat à apprécier. Si l'on suit les conclusions

de l'avocat général dans l'affaire Fan page (C-210/16), celui qui a recours aux outils d'un réseau social permettant à ce dernier de traiter des données personnelles peut être qualifié conjointement de responsable de traitement. Certes, la solution préconisée par l'avocat général était guidée par le fait que l'affaire concernait clairement l'activité professionnelle d'une entreprise. A contrario, il est raisonnable d'en déduire que si l'usage du réseau social est réalisé par une personne physique et est strictement personnel alors il ne relève pas du champ de protection des données à caractère personnel. Mais entre l'usage professionnel et l'usage personnel bien des variantes sont possibles. L'expérience montre, en effet, que l'utilisation des réseaux sociaux est souvent à la fois personnelle et professionnelle. Par exemple, si l'on peut considérer que Linkedln est un réseau principalement professionnel, en revanche Facebook n'est ni un réseau à dominante professionnelle ni un réseau à dominante personnelle ou domestique : le même compte utilisateur est parfois utilisé indifféremment pour l'une ou l'autre de ces finalités. En ce cas, suivant une interprétation large du champ d'application de la protection des données personnelles retenue par les juges, l'activité professionnelle bien que marginale devrait conduire à soumettre l'usage du réseau social au RGDP. Une telle interprétation est renforcée par la formule consacrée selon laquelle seules les activités *strictement* personnelles ou domestiques sont concernées par la limitation.

Le troisième exemple vise les activités en ligne qui ont lieu dans le cadre de ces activités au rang desquelles il semble que l'on puisse retenir les sites personnels mentionnés à l'article 2 de la loi 1978. Ce dernier exemple renforce la thèse selon laquelle, les cas énoncés par le considérant 18 ne sont pas limitatifs et permettront l'adaptation du texte aux évolutions technique et sociale des outils numériques. Ainsi, un des problèmes actuels est de savoir si le *Cloud personnel* correspond à une activité personnelle ou domestique et s'il relève de l'exception prévue au considérant 18 du RGPD. En substance, le *Cloud personnel* est un serveur sécurisé de stockage des données d'une personne dont elle a l'exclusivité de l'accès. Les sociétés qui offrent de telles solutions aux individus espèrent de la sorte échapper aux obligations incombant à un responsable de traitement dans la mesure où elles n'ont ni accès aux données ainsi stockées ni le pouvoir d'en contrôler le traitement. Pour autant, ces sociétés

fournissent les moyens de traitement à défaut d'en concevoir les finalités. À ce titre, elles pourraient être qualifiées de responsables de traitement. Quant à l'utilisateur de *Cloud personnel*, rien ne s'oppose à ce qu'il endosse également la qualité de responsable dès lors que l'usage n'est pas strictement personnel ou domestique, et que les données qu'il traite sont les données personnelles de tiers. Cette solution technique destinée à permettre aux personnes de maitriser la confidentialité de leurs données personnelles pourrait finalement entrer dans le champ d'application de la protection des données à caractère personnel.

***

En conclusion, la raison de l'extension du nombre de personnes éligibles à la qualité de responsable de traitement ne nous semble pas résulter d'une dérive protectionniste du législateur ou encore du juge. Elle tient, en vérité, à la généralisation des traitements de données personnelles qui se banalisent. Le phénomène révèle la vulnérabilité de la protection de la vie privée au sein d'une société dans laquelle, inexorablement, les données identifiées ou identifiables sont égrainées. Inversement, la plasticité de la notion de responsable de traitement permet son adaptation aux nouvelles pratiques qui se complexifient. La CJUE a ainsi apporté deux éclairages déterminants : selon le premier, le RGDP s'applique aux traitements mixtes, c'est-à-dire dont la finalité est à la fois personnelle et professionnelle ; et selon le second, est responsable de traitement celui qui définit les finalités et/ou les moyens de traitement *même partiellement*.

La prochaine étape consistera à trancher le sort des traitements d'ensembles mixtes de données — à savoir personnelles et non personnelles — qui constituent une grande partie des données traitées. La réponse résultera de l'articulation retenue entre le futur Règlement relatif à la libre circulation des données[25] et le RGDP[26].

25 - Proposition de Règlement du parlement européen et du conseil concernant un cadre applicable à la libre circulation des données non personnelles dans l'Union européenne du 13 septembre 2017 COM (2017) 496 final.

26 - Voir sur ce point, par exemple, la proposition de résolution n° 80 (2017-2018) de M. Sutour déposée au Sénat le 9 novembre 2017, ainsi que la Résolution n° 24 (2017-2018), devenue résolution du Sénat le 5 décembre 2017.

En particulier, il s'agira de préciser quel texte s'appliquera lorsque les données d'un ensemble mixte sont inextricablement liées c'est-à-dire qu'elles ne peuvent être techniquement dissociées de sorte qu'une application distributive des régimes n'est pas envisageable. L'enjeu est de taille pour les entreprises qui souhaitent échapper à la qualification de responsable de traitement[27]. Il ne semble pas que l'on s'achemine vers une solution tranchée[28] malgré quelques voix en ce sens[29]. Le risque est de créer de nouvelles incertitudes quant à savoir qui est responsable de traitement.

Mai 2018

27 - Pour une solution favorable aux entreprises, voir l'amendement n° 5 relatif au considérant 10 du Projet d'avis du 30 janvier 2018, 2017/0228 (COD). PE<NoPE>613.537</NoPE><Version>v01-00 (rapporteur Zdzislaw Krasnodebski) selon lequel le RGDP s'applique « à moins que les données à caractère personnel ne figurent dans l'ensemble de données qu'à des fins administratives et ne soient pas des données à caractère sensibles ».

28 - Projet de rapport 2017/0228 (COD). PE-619.038v01-00 et Projet de rapport du 9 avril 2018 : 2017/0228 (COD). PE-619.414v02-00 (rapporteur Anna Maria Corazza Bildt) : « lorsque *des données à caractère non personnel et personnel d'un ensemble de données mixtes sont inextricablement liées, le présent règlement devrait s'appliquer à tout l'ensemble sans préjudice du règlement (UE) 2016/679* ».

29 - Voir les amendements 70 à 79. Par exemple l'amendement 79 présenté par Julia Reda au nom du groupe Verts/ALE visant à qualifier les ensembles de données « mixtes » de données personnelles en vue de l'application du RGDP. Pour une application du Règlement sur la libre circulation des données aux ensembles de données mixtes : amendements 80, 81. Pour la suppression du considérant 10 : amendement 69.

LE DROIT DES DONNÉES PERSONNELLES FACE À L'OPACITÉ DES ALGORITHMES PRÉDICTIFS : LES LIMITES DU PRINCIPE DE TRANSPARENCE

Jean-Marc Deltorn
Doctorant au laboratoire E.A. 4375, Centre d'études internationales de la propriété intellectuelle, Université de Strasbourg

Introduction

L'adoption du Règlement européen sur la protection des données personnelles[1] et, au niveau national, la promulgation de loi pour une République numérique[2], ont consacré l'importance d'un contrôle accru sur les procédés de traitement automatique mis en œuvre pour capter, manipuler et utiliser les données à caractère personnel. La protection de ces données bien particulières, droit fondamental inscrit aux articles 16 du Traité sur le fonctionnement de l'Union européenne et 8 de la Charte des droits fondamentaux de l'Union européenne, s'avère de fait nécessaire face à l'ubiquité, voire l'hégémonie, des intermédiations numériques. Dans ce nouvel espace technico-juridique, un principe de transparence, permettant aux individus d'être informés sur les traitements dont ils font l'objet a été inclus dans les dispositions du Règlement et de la loi pour une République numérique[3]. Or, l'émergence de nouvelles formes de procédés décisionnels automatisés vient en contrecarrer l'application. Des avancées algorithmiques récentes ont en effet conduit au développement de

1 - Règlement (UE) 2016/679, signé le 27 avril 2016 et publié le 4 mai au Journal officiel de l'Union européenne (ci-après « le Règlement ») .

2 - Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, publiée au Journal officiel le 8 octobre 2016.

3 - Selon les articles 13 §2(f) et 14 §2(g) du Règlement UE 2016/679, le responsable du traitement doit informer la personne de « l'existence d'une prise de décision automatisée, y compris un profilage, [et] des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée. » L'article 12 §1 précise en outre que cette information doit être communiquée « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ». Ce même principe est inscrit à l'article 4 la loi pour une République numérique, qui introduit l'article L.311-3-1 au livre III du Code des relations entre le public et l'administration. Cet article dispose en effet qu'« une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande. »

procédés reposant sur un apprentissage automatique de modèles prédictifs. À la différence des systèmes antérieurs dans lesquels les mécanismes de décision devaient être définis *a priori* (essentiellement sous forme de règles postulées par le concepteur), ces nouvelles approches permettent aux systèmes d'élaborer une représentation interne du processus décisionnel sur la seule base d'exemples. Dotés de capacités d'adaptation et de facultés prédictives inégalées, ces « algorithmes d'apprentissage » sont à présent le standard en matière de procédé décisionnel automatisé. Ils s'imposent aujourd'hui dans des domaines aussi variés que la reconnaissance de la parole et des images, en passant par l'analyse automatique du langage ou la robotique. Pourtant, malgré leur succès croissant, et en contrepoint de leur efficacité, ces objets techniques s'expriment dans un espace qui leur est propre, et qui n'a pas fonction à être humainement compréhensible. L'enchaînement déterministe permettant d'arriver à une prédiction échappe ainsi à toute interprétation. Ces modèles sont, ce faisant, la source d'une opacité à laquelle le principe de transparence doit se confronter.

Mais cette opacité technique, intrinsèque aux modèles statistiques, n'est pas seule à s'opposer à une application directe du principe de transparence. D'autres forces, juridiques, économiques, extérieures au traitement des données personnelles en tant que tel, contribuent à en limiter l'accès. Les modèles statistiques requièrent en effet pour leur développement des efforts importants, notamment dans la constitution d'un corpus de données d'entrainement dont dépend largement leur efficacité, mais aussi dans les choix spécifiques à leur architecture, ou encore les coûts liés aux infrastructures informatiques nécessaires à la phase d'apprentissage. Or, les modèles prédictifs, qui synthétisent en un produit final l'ensemble de ces investissements, sont largement résistants aux tentatives d'ingénierie inverse. Ils constituent ainsi des objets de propriété intellectuelle souvent protégés par le secret des affaires. Une forme de protection qui s'oppose à un accès à l'instrument même par lequel les décisions sont prises et constitue une seconde forme d'opacité. En l'absence de règle de prévalence entre les droits en concours, des tensions ne peuvent que survenir entre la prise en considération du droit à l'information des individus quant aux décisions prises sur la base de leurs données personnelles et le respect des droits de propriété intellectuelle et du secret des affaires.

Après avoir présenté les différents filtres techniques et les contraintes juridiques s'opposant à la transparence du traitement algorithmique des don nées personnelles (I), nous discuterons des articulations entre le droit d'accès à la logique sous-jacente aux modèles prédictifs et le respect du secret des affaires (II). Nous proposerons enfin quelques pistes pratiques pour adapter le principe de transparence à ce nouveau paysage technique et légal en y promouvant, en particulier, la notion de responsabilité (III).

Section I – Le traitement algorithmique des données personnelles : un nouvel enjeu juridique

§1 : Apprendre des données : les algorithmes prédictifs et les données personnelles[4]

A. L'émergence d'un nouvel objet technique

Cliquer sur un lien, bouger sa souris, entrer quelques mots-clés dans la barre d'un moteur de recherche, et nous voilà déjà tous producteurs de bribes de données, élémentaires sans doute, mais qui offrent pourtant un reflet de notre activité quotidienne. S'y ajoutent d'autres catégories d'informations, des « métadonnées », adresse IP, coordonnées GPS, et bien d'autres encore (police de caractères, carte son, taille écran, modèle de navigateur, etc...) qui viennent augmenter et enrichir le contenu descriptif de ce « double numérique » qui peu à peu émane de notre activité sur la toile ou au travers des divers objets connectés qui parsèment notre quotidien. Aussi abstraite et évanescente qu'elle puisse sembler, cette empreinte numérique ne disparaît pas, bien au contraire, elle est captée, gravée dans des mémoires et sert de base à une cohorte de calculs complexes.

L'exploitation systématique de la masse de données numériques produites par les utilisateurs est considérée aujourd'hui comme une opportunité en termes d'innovation économique et stratégique, une forme inédite de création de valeur. « [N]ouvel or noir de l'Internet

4 - Cette section reprend et développe certains passage d'une publication antérieure : J.-M. Deltorn, « La protection des données personnelles à l'épreuve des algorithmes prédictifs », *Revue des droits et libertés fondamentaux*, chron. n°12, 2017, p. 1.

et nouvelle monnaie du monde digital »,[5] ces données représentent la matière première à partir de laquelle il est possible d'analyser, de classer les activités, de suivre les comportements et de prédire les centres d'intérêt d'utilisateurs largement dépendants d'un réseau numérique de plus en plus dense et omniprésent. Les informations qui en sont extraites permettent ainsi de délivrer, en temps réel, des offres de plus en plus personnalisées,[6] d'augmenter l'efficacité des entreprises[7] et des services publics[8]. Des opérations si rapides et transparentes qu'elles échappent largement au filtre critique des utilisateurs, peu conscients de la valeur ajoutée de ces traces égrenées au fil de leur trajet numérique, ni de l'étendue de leur utilisation.

Soumises à des contraintes inédites de volume, de variété et de vitesse, ces méthodes ne reposent plus aujourd'hui sur la prescription de relations issues d'une observation attentive, de l'analyse d'experts dont l'expérience serait finalement capturée sous forme de règles pour être automatisée.[9] Elles sont le fait de familles d'algorithmes qui tirent des données elles-mêmes les modèles

5 - Meglena Kuneva, Commissaire Européen à la consommation, *Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling* (31 mar. 2009), citée dans *Personal data : the emergence of a new asset class*, World Economic Forum, jan. 2011, p. 5.

6 - J. Bobadilla, et al., « Recommender systems survey ». *Knowledge-Based Systems*, vol. 46, 2013, p. 109 ; V. Salonen, Ville et H. Karjaluoto, « Web personalization: The state of the art and future avenues for research and practice ». *Telematics and Informatics*, vol. 33, n° 4, 2016, p. 1088. Pour un panorama en chiffre du phénomène « Big data » : M. Chen, S. Mao et Y. Liu, « Big data: a survey ». *Mobile Networks and Application*s, vol. 19, n° 2, 2014, p. 171.

7 - En terme d'optimisation logistique en temps-réel, de contrôle qualité, du suivi de satisfaction des clients, et de marketing ciblé, etc. (R. Kitchin, «Big Data, new epistemologies and paradigm shifts». *Big Data & Society*, vol. 1, n° 1, 2014, p. 1).

8 - Par exemple, pour l'amélioration de la circulation urbaine ou la mesure des consommation d'énergie, mais aussi les services d'éducation à distance, le contrôle épidémiologique et l'optimisation des services de santé publique (G.-H. Kim, S. Trimi et J-H. Chung. «Big-data applications in the government sector». *Communications of the ACM*, vol. 57, n° 3, 2014, p. 78).

9 - Implémentées, par exemple, sous forme de « systèmes experts » reproduisant un raisonnement déductif à partir d'un ensemble de règles édictées par un ou plusieurs spécialistes d'un domaine technique particulier.

permettant de représenter l'objet étudié.[10] Capables de passer de la trace à l'information, en réduisant le recours à une intermédiation humaine supposée faillible et inapte à traiter les données de masse, ces algorithmes, dits « d'apprentissage automatique », sont à présent le principal instrument d'interprétation des données à grande échelle[11]. Leur développement récent, fulgurant, s'est fait sous

10 - En toute généralité, un « algorithme » consiste en un ensemble d'instructions permettant de résoudre un problème ou d'obtenir un résultat en un nombre fini d'étapes. Une définition aussi large recouvre une vaste gamme de procédés : la manière d'obtenir les racines d'une équation du second degré autant que la méthode de résolution d'un casse-tête ou encore la description d'une recette de cuisine rentrent ainsi dans le cadre de la définition (nous manions ainsi tous au quotidien sans le savoir, d'une manière ou d'une autre, à la manière d'un monsieur Jourdain moderne, la forme algorithmique). C'est cependant dans leur traduction en langage informatique qu'ils expriment toute leur puissance en tirant pleinement parti des capacités de calcul et de mémoire des ordinateurs. Les résultats quasi-instantanés d'une requête sur un moteur de recherche à partir du contenu de milliards de pages Internet, les suggestions publicitaires personnalisées d'une plateforme d'achat en ligne, la proposition d'un trajet optimal sur une application de navigation routière n'en sont que quelques exemples parmi les plus communs. Une catégorie particulière d'algorithmes a pour fonction de produire une représentation statistique de données qui lui sont fournies en entrée. Un exemple élémentaire est le procédé de calcul d'une moyenne et d'un écart-type (une mesure de la dispersion des données autour de la moyenne). Ces grandeurs produisent une caractérisation synthétique, approximative, du processus observé dont elles forment un « modèle ». L'algorithme permet donc dans ce cas d'obtenir, à partir de données mesurées, un modèle représentatif décrivant de manière idéalisée la distribution ayant généré ces observations. L'algorithme n'est alors qu'un intermédiaire nécessaire à la détermination du produit final, à savoir ici, le modèle statistique.

11 - Certaines classes d'algorithmes, dits « d'apprentissage » permettent de générer des modèles d'un type particulier, susceptibles d'être utilisés à leur tour pour répondre à des questions ou résoudre des problèmes. Selon la définition de T.M. Mitchell, « un programme d'ordinateur est susceptible d'apprendre de l'expérience si, compte tenu d'une catégorie de tâches et d'une mesure d'efficacité données, sa performance dans l'exécution desdites tâches s'accroît avec l'expérience. » (v. T.M. Mitchell, *The discipline of machine learning*, Carnegie Mellon University, School of Computer Science, Machine Learning Department, vol. 3, n° 06-108, 2006, p. 1. Notre traduction). Par exemple, à partir d'un ensemble d'images contenant un certain type d'objet, l'algorithme pourra déduire un modèle qui sera capable d'identifier si ce même objet est présent dans une nouvelle image (sans qu'il l'ait pourtant jamais vue). Les capacités des algorithmes et des calculateurs actuels permettent de répondre de manière satisfaisante à des problèmes jugés il y a peu insolubles : l'identification automatique de milliers d'objets dans des images, la reconnaissance de la parole, la traduction de textes entre plusieurs langues, ont ainsi connu un succès sans précédent. L'algorithme permet ainsi, par apprentissage et à partir de données dites « d'entraînement », de générer un modèle contenant une représentation de l'objet à identifier (objets visuels, sonores ou textuels) et de la question à retourner (« tel objet (ou tel mot) est-il présent dans les données ? » ou encore « comment traduire une phrase donnée ? »). Cette représentation « interne » au modèle sera le plus souvent constituée de paramètres, dont le nombre dépend, notamment, de la complexité du problème posé. Compte tenu de la complexité des problèmes qu'ils résolvent, l'expression des modèles afférents requiert des dizaines de millions, voire des milliards, de paramètres interdépendants. C'est dans cet espace de très grandes dimensions que s'expriment les modèles d'inférence. Ces techniques regroupent une large famille d'algorithmes reposant soit sur un apprentissage « supervisé » requérant une classification préalable des exemples d'entraînement, soit « non supervisé » dans le cas contraire. Pour un panorama, v. N. Jones, « The learning machines », *Nature*, vol. 505, 2014, p. 146 et Y. LeCun, Y. Bengio et G. Hinton, « Deep learning », *Nature*, vol. 521, 2015, p. 436).

l'impulsion conjointe de nouvelles approches algorithmiques,[12] de l'augmentation des capacités de calcul, notamment distribué et, en premier lieu, de l'accès à de vastes bases de données à partir desquelles ils sont susceptibles d'apprendre.[13] Les capacités de ces algorithmes permettent ainsi d'identifier des corrélations auparavant insoupçonnées, mais pourtant déjà statistiquement présentes dans les données qui lui sont proposées. Apprendre à reconnaître un piéton dans une image reviendra alors, non pas à définir manuellement un archétype du piéton en termes interprétables par la machine, mais à proposer à l'algorithme d'apprentissage des exemples d'images en lui indiquant à chaque instance si, oui ou non, elles contiennent bien un piéton. De ce croisement de données brutes, hétérogènes, individuellement « a-signifiantes »[14], l'algorithme compare, extrait des caractéristiques, déduit des règles de décision, et aboutit à une représentation interne de l'objet d'intérêt *sans qu'il ait jamais été nécessaire à l'opérateur d'en dicter les détails*. Lors de son utilisation ultérieure, soumis à des données inconnues, le modèle sera alors capable d'assigner une catégorie (p. ex. : « piéton ») ou une grandeur réelle (p. ex. : « la probabilité de présence d'un piéton ») aux données d'entrées et de fournir un résultat en accord avec les distributions statistiques apprises des exemples lors de l'apprentissage.

Le succès sans précédent de ces méthodes, dans les domaines les plus variés, de la vision par ordinateur à la reconnaissance de la parole ou

12 - Notamment dues aux progrès de « l'apprentissage profond » (v. Y. LeCun, Y. Bengio et G. Hinton, *Ibid.*).

13 - Pour une discussion sur les succès récents du « Big data », v. dans ce sens K. Kelly, The three breakthroughs that have finally unleashed AI on the world, Wired Online Edition, 27 October 2014. Le succès des méthodes d'apprentissage, qui reposent sur l'accès à des données d'entrainement réelles, est largement dépendant de la collecte et du partage en ligne de vastes bases de données (X.-W. Chen et X. Lin, « Big data deep learning: challenges and perspectives », *IEEE Access*, vol. 2, 2014, p. 514). Le choix d'une architecture adaptée - une nécessité pour réduire les temps de calcul - s'appuie sur les progrès des architectures GPU (« Graphical processing units ») et sur le développement récent d'une informatique « dématérialisée » (une analyse détaillée de l'influence des infrastructures distribuées sur le « Big analytics » est proposée par I.A.T. Hashem et al., « The rise of «big data» on cloud computing: Review and open research issues », *Information Systems*, vol. 47, 2015, p. 98).

14 - Le terme est emprunté à Antoinette Rouvroy (A. Rouvroy, *Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives*. T-PD-BUR(2015)09REV, Strasbourg, Conseil de l'Europe, janv. 2016), dont les travaux apportent un éclairage précieux sur l'articulation entre règles juridiques et objets numériques, en particulier en relation à la notion de « gouvernementalité algorithmique ».

des images[15], de l'analyse statistique du langage[16] à l'interprétation de données comportementales ou médicales[17], leur alloue un rôle central dès lors que des exemples sont disponibles en quantité suffisante pour leur permettre un apprentissage satisfaisant. L'accès à de vastes réserves de données a donc contribué à une profusion d'applications pratiques, encore favorisées par l'ouverture de plateformes *open-source* et de services distribués.[18] C'est donc tout naturellement que l'efficacité de ces algorithmes a été mise à profit pour interpréter les signaux bruts les plus élémentaires, qu'ils émanent de nos pérégrinations numériques sur l'Internet, ou qu'ils soient captés par les objets connectés. De fait, les algorithmes d'apprentissage automatique constituent à présent le fer de lance de l'analyse prédictive appliquée aux données de masse.

B. Les algorithmes d'apprentissage face aux droits fondamentaux

On ne s'émouvrait guère de ces développements techniques s'il ne s'agissait que de décisions sans conséquences. Or des prédictions aux effets juridiques majeurs sont aujourd'hui le fait d'un tel traitement algorithmique. Des traits de personnalité, des données sensibles au sens de l'article 8 de la loi n° 78-17 du 6 janvier 1978 (loi informatique et libertés) et de l'article 9 §1 du Règlement, sont ainsi obtenus sur des utilisateurs sans qu'ils ne manifestent à aucun moment la volonté d'en révéler la teneur. Outre les orientations politiques, religieuses et ethniques, les données de santé sont, dans

15 - L. Deng et L. Xiao, « Machine learning paradigms for speech recognition : an overview », *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 21, n° 5, 2013, p. 1060 ; H. Hodson, «Facebook as good as a human at recognising faces», *New Scientist*, n° 221.2961, 2014, p. 23.

16 - R. Collobert et J. Weston. « A unified architecture for natural language processing: Deep neural networks with multitask learning », *Proceedings of the 25th ACM international conference on Machine learning*, 2008, p. 160.

17 - D. Shen, G. Wu et H.-I. Suk., «Deep learning in medical image analysis», *Annual Review of Biomedical Engineering*, 2017, vol. 19, p. 221 ; Z. Peng, Q. Hu et J. Dang, « Multi-kernel SVM based depression recognition using social media data », *International Journal of Machine Learning and Cybernetics*, 2017, p. 1.

18 - Dont les services cognitifs d'IBM Watson, disponibles sur des interfaces programmatiques, la bibliothèque logicielle d'apprentissage automatique TensorFlow de Google, la mise en open source par Facebook du design de son serveur Big Sur pour l'utilisation de réseaux neuronaux profonds sur des GPU, les bibliothèques d'apprentissage profond du système de recommandation DSSTNE d'Amazon ou PaddlePaddle de Baidu, etc.

ce registre, particulièrement convoitées.[19] Là encore, l'apparente innocuité d'une utilisation usuelle des applications numériques et l'absence de prise de conscience du contenu dérivable de ces traces, en autorise une exploitation souvent subreptice, parfois abusive. L'historique de navigation, aisément accessible aux tiers lors de la visite de sites Internet, est ainsi particulièrement révélateur des préoccupations de santé d'un individu.[20] De même, les métadonnées, souvent écartées du régime des données à caractère personnel, seront autant d'indices qui participeront à établir un profil de santé de l'individu.[21] Aux États-Unis, la chaîne de magasins *Target*, inféra ainsi correctement, grâce à l'analyse automatique de ses achats, qu'une adolescente du Minnesota était enceinte : la conjonction de suppléments minéraux, d'huiles hydratantes, entre autres critères, avait suffi à faire entrer la cliente dans la catégorie des femmes enceintes. *Target* lui fit alors parvenir des publicités pour des produits pour nourrissons, à la surprise des parents de la jeune fille qui n'étaient pas encore au courant.[22] À ces données de navigation ou de consommation s'ajoutent de plus en plus de signaux reçus à partir d'objets connectés (p.ex. de mesure de l'activité physique) qui contribuent encore à la construction d'un profil de santé général. Le cabinet de consultants Deloitte reconnaît ainsi utiliser « des milliers de données issues de sources tierces non-traditionnelles, telles que l'historique des achats, pour prédire, avec une précision comparable

19 - H.K. Patil et R. Seshadri. « Big data security and privacy issues in healthcare», *in 2014 IEEE international congress on big data*, 2014, p. 762.

20 - T. Libert, «Privacy implications of health information seeking on the web», *Communications of the ACM*, vol. 58, n° 3, 2015, p. 68 ; T. Glenn et S. Monteith, «Privacy in the digital world : medical and health data outside of HIPAA protections », *Current psychiatry reports*, vol. 16, n° 11, 2014, p. 1.

21 - J. Mayer et P. Mutchler, « MetaPhone: the sensitivity of telephone metadata », *Web Policy*, 2014, [http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/].

22 - K. Hill, «How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did»*., Forbes, Inc*., 16 fév. 2012. Charles Duhigg (« Psst, You in Aisle 5 », *New-York Times*, 19 fév. 2012) décrit le procédé suivi par Target pour développer un modèle des futures grossesses. Une base de données d'entrainement a d'abord été constituée à partir de clientes enregistrées en ligne pour organiser la « fête prénatale » (« baby shower ») de leur futur enfant. Leurs achats ont ensuite été analysés pour former un modèle prédictif et établir un « score de grossesse », utilisé ultérieurement pour classer les clientes du magasin. Une stratégie de sélection particulièrement attrayante pour l'enseigne de grande distribution puisque, selon Duhigg : « *[w]hen consumers change their routines they are susceptible to forming new shopping habits. [...] As a Target statistician explained, if Target could identify pregnant consumers in their second trimester, "there's a good chance we could capture them for years."* ».

à celle d'un examen médical, le niveau de santé d'un candidat à une assurance vie »,[23] soulignant si nécessaire, la réalité du risque d'utilisation d'un substitut (virtuel) de notre état de santé réel.[24]

La quantification des comportements humains par l'intermédiaire d'outils de prédiction algorithmique pourrait donner l'illusion d'une métrique objective. Le fait que la décision émerge d'un objet mathématique, autant que la construction d'un modèle par un algorithme d'apprentissage indépendant d'une intervention humaine (dans la définition de sa représentation interne, tout du moins), participent tous deux à une impression de neutralité du processus de décision automatique. Là où une analyse statistique humaine serait, du simple fait de sa subjectivité, sujette à un regard critique, l'algorithme se voit paré d'une « rationalité algorithmique »[25] qui tend à accorder un caractère de certitude positive aux résultats qui en découlent. Or l'application pratique de ces procédés, loin d'une impartialité mécanique, reflète autant les choix des responsables du traitement (choix techniques, mais aussi stratégiques) que les contraintes imposées par les données dont elles dépendent.

Ni dénués d'arbitraire, ni exempts de malfaçons, ces procédés reflètent la nature des échantillons sur lesquels ils sont construits et les hypothèses sur leur distribution statistique. Ainsi, le déséquilibre numérique entre la distribution d'entrainement et les données réelles est aussi source de biais statistique. Il peut être dû à une insuffisance du nombre d'exemples disponibles pour l'une ou l'autre des catégories concernées (la représentation qui s'en déduit est alors dominée par un bruit statistique). Ce sera aussi le cas en présence d'un décalage quantitatif entre les échantillons représentatifs des différents profils. Si une classe d'individus est, en proportion, bien plus représentée lors de l'apprentissage du modèle que lors des tests ultérieurs, les règles apprises tendront à favoriser

23 - Notre traduction : « *thousands of non-traditional third-party data sources, such as consumer buying history, to predict a life insurance applicant's health status with an accuracy comparable to a medical exam* » (Robinson Civil rights, « Big data and our algorithmic future », *Soc. Just. & tech. 2014* [https://bigdata.fairness.io/predictive-policing]).

24 - V. aussi dans ce sens : N.P. Terry, « Protecting patient privacy in the age of big data », *UMKC Law Rev*., vol. 81, 2012, p. 385.

25 - A. Rouvroy et T. Berns, « Le nouveau pouvoir statistique », *Multitudes*, vol. 1, 2010, p. 88.

la distribution dominante dans l'ensemble d'entrainement.[26] Ce désavantage relatif d'une population par rapport à l'autre est ainsi source de discriminations dont le traitement des données personnelles n'est pas exempt. Ainsi le sexe de l'utilisateur (déduit de l'historique de navigation, des contacts, des préférences sur les réseaux sociaux) détermine la nature des publicités sélectionnées par Google : les hommes se voyant proposer davantage d'offres d'emplois à responsabilité, mieux rémunérés, que les femmes.[27] De fait, l'apprentissage automatique peut produire une représentation biaisée en terme social ou ethnique qui sera reflétée dans les décisions prises au moyen du modèle. Dans ce cas, le biais statistique n'est donc pas nécessairement le fait de choix conscients du responsable du traitement (consistant par exemple dans l'utilisation d'une base de données, de la sélection de caractéristiques pour représenter ces données ou de leur classification) mais résulte de l'acquisition d'échantillons d'entrainement non représentatifs de la distribution réelle. Ainsi, le simple fait d'entraîner un système d'apprentissage sur des données issues de l'Internet focalisera le modèle sur la population la plus représentée sur la toile, sans aucune considération d'équité.[28]

Alors même que les traces numériques laissées par les individus participent à l'attribution de scores de solvabilité,[29] à la classification

26 - « *[T]he classification "rules" [...] that predict the minority class tend to have a much higher error rate than those that predict the majority class. The second observation is that test examples belonging to the minority class are misclassified more often than test examples belonging to the majority class.* » (G.M. Weiss et F. Provost, «The effect of class distribution on classifier learning: an empirical study», *Technical Report ML-TR-44, Dept. of Computer Science*, Rutgers University, 2 août 2001, p. 1. V. en particulier section 2.2).

27 - A. Datta, M.C. Tschantz et A. Datta, « Automated experiments on ad privacy settings - A Tale of Opacity, Choice, and Discrimination », *in Proceedings on Privacy Enhancing Technologies,* 2015, vol. 1, p. 92. Il faut souligner ici que la responsabilité de la sélection de la publicité n'incombe pas nécessairement à Google seul : divers acteurs interviennent en effet entre l'accès au moteur de recherche par un individu donné et la présentation finale du message publicitaire. Un écosystème complexe de distribution de publicités en ligne qui rajoute à l'opacité du processus algorithmique de décision.

28 - N.B. Weidmann, et al., « Digital discrimination: Political bias in Internet service provision across ethnic groups », *Science*, vol. 353, n° 6304, 2016, p. 1151.

29 - Facebook est par exemple titulaire d'une famille de brevets (US9100400 « Authorization and authentication based on an individual's social network », Publié le 4 aout 2015 ; EP2296342, délivré le 20 juin 2012) permettant d'attribuer un tel score à un individu en fonction de son réseau social (c'est-à-dire en évaluant les scores de ses « amis », des « amis de ses amis », etc.).

des réfugiés,[30] ou à la décision de libération conditionnelle ou du risque de récidive,[31] les procédés de décision automatisés (en particulier lorsque leurs modèles dépendent d'échantillons réels) risquent de propager les biais statistiques déjà présents dans les données d'entrainement. De fait, « Le sondage des données et l'utilisation de classificateurs issus de procédés par induction peut conduire aux mêmes types de problèmes que ceux rencontrés par les décideurs humains, y compris être affectés de généralisations à caractère discriminatoire. Ces effets peuvent être particulièrement nuisibles dans la mesure où les méthodes d'analyse de données sont le plus souvent conçues comme fermement ancrées sur des bases statistiques et, pour cette raison, purement rationnelles et indépendantes de tout préjugé ».[32] En présentant les prédictions comme résultant d'un processus supposé indépendant de toute influence subjective, ils seront gratifiés d'une aura d'autorité, sans fondement réel mais qui contribuera à réifier les préjugés. Par ailleurs l'attribution automatique de labels reproduisant les biais présents dans le modèle pourra servir à entraîner de nouvelles générations d'algorithmes, participant ainsi au renforcement, voire à l'amplification du préjugé initial. Puisque de tels risques sont aujourd'hui bien réels, puisque « la dépendance irréfléchie à l'exploitation des données est susceptible de priver les membres de

30 - À partir de sa plateforme *i2 Enterprise Insight Analysis,* IBM a développé un outil de décision automatique qui pourrait, selon le groupe, « *help governments separate real refugees from imposters, untangle terrorist cells, or even predict bomb attacks* » (P. Tucker, « Refugee or Terrorist ? » *DefenseOne*, 2016, http://www.defenseone.com/technology/2016/01/). Bien sûr, IBM le souligne, il ne s'agit là que d'un « score », une aide à la décision (v. *IBM i2 Enterprise Insight Analysis for Defense Intelligence*, IBM Analytics - Solution brief, 2015, p. 1-7, http://www.ibm.com/analytics/us/en/industry/government/defense-intelligence/).

31 - R. Berk, « Balancing the Costs of Forecasting Errors in Parole Decisions », *Albany Law Review*, vol. 74, 2010, p. 1071 ; R. Berk, et al., « Forecasting murder within a population of probationers and parolees: a high stakes application of statistical learning », *Journal of the Royal Statistical Society* : Series A, vol. 172, n° 1, 2009, p. 191.

32 - Notre traduction : « *data mining and classifier induction can lead to similar problems as for human decision makers, including basing their decisions upon discriminatory generalizations. This can be particularly harmful since data mining methods are often seen as solidly based upon statistics and hence purely rational and without prejudice* » (T. Calders et I. Žliobait€, « Why unbiased computational processes can lead to discriminative decision procedures », *in Discrimination and Privacy in the Information Society*, Springer, 2013, p. 43).

groupes vulnérables d'une pleine participation à la société »[33], un contrôle accru des biais inhérents à la construction de modèles par apprentissage automatique et des décisions qui en résultent apparaît donc aujourd'hui comme une priorité.

§2 : Les recours juridiques en réponse au traitement algorithmique des données personnelles

A. Un accès (limité) à la logique des algorithmes

Le droit à la protection des données personnelles est actuellement assuré par un ensemble d'instruments juridiques. Au niveau national, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 pour transposer les dispositions de la directive 95/46/CE, forme aujourd'hui le principal cadre de protection des données à caractère personnel. La loi pour une République numérique, promulguée, le 7 octobre dernier, illustre de plusieurs mesures le principe du droit à la libre disposition de ses données personnelles (établissant, par exemple, la confidentialité des correspondances électroniques). Au niveau communautaire, le texte principal est à présent le règlement européen 2016/679 adopté le 27 avril 2016, après plus de quatre années de discussions. Il abrogera la directive 95/46/CE et entrera en application à compter du 25 mai 2018, date à partir de laquelle il sera d'application directe dans l'ensemble des États membres de l'Union européenne.[34]

Le droit à la protection des données à caractère personnel tel qu'établi par ces textes vise à garantir le respect des droits et des

33 - Notre traduction : « *unthinking reliance on data mining can deny members of vulnerable groups full participation in society* » (S. Barocas et A.D. Selbst, « Big data's disparate impact », *California Law Review*, 2016, vol. 104, p. 671).

34 - Pour une synthèse des changements introduits par le nouveau règlement, v. C. Castets-Renard, « Brève analyse du règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, juil. 2016, p. 334. D'autres textes communautaires concernent aussi la protection des données personnelles : notamment, La Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée par le Conseil de l'Europe le 28 janvier 1981, mais aussi la directive Vie privée et communications électroniques 2002/58/CE du 12 juillet 2002, modifiée par la directive 2006/24/CE du 15 mars 2006 sur la conservation des données.

libertés fondamentales.[35] La Convention 108 soulignait, il y a plus de 35 ans déjà, que « dans certaines conditions, l'exercice d'une complète liberté de traiter les informations risque de nuire à la jouissance d'autres droits fondamentaux (par exemple les droits à la vie privée, à la non-discrimination et à un procès équitable) ou à d'autres intérêts personnels légitimes (par exemple en matière d'emploi ou de crédit à la consommation). C'est pour maintenir un juste équilibre entre les différents droits et intérêts des personnes que la Convention impose certaines conditions ou restrictions au traitement d'informations. »[36] Le Règlement, au premier point de ses considérants, le souligne de même : « La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. » C'est donc à cette mesure qu'il faut envisager la protection des données personnelles : un droit fondamental dont les abus se manifesteront par des atteintes à la vie privée, des discriminations, des limites à la liberté d'expression.

Le Règlement souligne en son introduction la nécessité de permettre aux personnes physiques « d'avoir le contrôle des données à caractère personnel les concernant. » À cette fin, et pour permettre de maintenir la confiance dans l'économie numérique, « [l]a sécurité tant juridique que pratique devrait être renforcée pour les personnes physiques, les opérateurs économiques et les autorités publiques ». En particulier, les décisions fondées exclusivement sur un traitement automatisé, tel que le profilage, font l'objet de l'article 22 qui permet aux personnes concernées de s'opposer, dans certains cas, à un tel traitement dès lors qu'il s'accompagne d'effets juridiques l'affectant « de manière significative ». Or l'un des axes principaux sur lesquels repose la protection des individus face au traitement automatique de leurs données personnelles s'articule autour du principe de transparence. Il s'exprime en particulier dans le Règlement au travers de ses articles 13 §2(f), 14 §2(g) et 15 §1(h), qui disposent que le responsable du traitement doit informer la personne de

35 - L'article 8 §1 de la Charte des droits fondamentaux de l'Union européenne, comme l'article 16 §1 du traité sur le fonctionnement de l'Union européenne, disposent ainsi que « [t]oute personne a droit à la protection des données à caractère personnel la concernant. »

36 - Point 25, du Rapport explicatif à la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janv. 1981.

« l'existence d'une prise de décision automatisée, y compris un profilage, [et] des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée. »[37] Ces informations sont en effet considérées nécessaires pour garantir « un traitement équitable et transparent » (art. 13 §2, 14 §2). L'article 12 §1 précise en outre que cette information doit être communiquée « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ». Ce même principe est inscrit à l'article 4 de la loi pour une République numérique, qui introduit l'article L.311-3-1 au livre III du Code des relations entre le public et l'administration. Cet article dispose en effet qu'« une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande. »

Cette possibilité d'accès à la « logique sous-jacente » au traitement dans le cadre du Règlement, si elle n'est pas strictement nouvelle,[38] participe certainement d'une volonté de la part du législateur d'accroître la transparence des systèmes de traitement algorithmique et prévenir ce faisant les nombreux abus dont ils sont déjà la manifestation. Pourtant l'interprétation de ce nouveau droit a récemment fait débat. Si Bryce Goodman et Seth Flaxman y ont vu l'avènement d'un

37 - C'est-à-dire dans le contexte de l'article 22, relatif au traitement automatisé.

38 - V. article 12(a) de la Directive 95/46/CE, qui accorde l'accès aux informations à toute personne concernée le droit d'obtenir du responsable du traitement : « la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1 » (l'article 15 de la Directive correspondant à l'article 22 du Règlement). L'article 39(5) de la loi Informatique et libertés n° 78-17 du 6 janvier 1978 dispose quant à lui que toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir « Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé ». La nouveauté dans la formulation du Règlement est l'introduction d'une précision sur la nature des informations fournies : celles-ci devront à présent être, aux termes des articles 13 §2(f), 14 §2(g) et 15 §1(h), des « informations *utiles* » (nous soulignons). Les dispositions de l'article 12 du Règlement précisant le caractère « concis, transparent, compréhensible » de ces informations étaient absentes de la Directive 95/46/CE et ne trouvent pas non plus d'équivalent dans la loi n° 78-17 du 6 janvier 1978.

véritable « droit d'explication »[39] permettant de révéler la face cachée des processus de traitement automatique des données personnelles, une analyse détaillée a fait en revanche émerger une interprétation plus restrictive. Sandra Wachter, Brent Mittelstadt et Luciano Floridi soulignent ainsi , avec justesse, que le règlement ne mentionne de manière explicite l'accès à une « explication » que dans le considérant 71 (considérants dont la fonction n'est, rappelons-le, que de contribuer à une juste interprétation des dispositions essentielles de l'acte, sans revêtir de caractère contraignant). Il précise, en lien avec l'article 22 relatif au droit d'opposition à la prise de décision automatisée,[40] qu'un tel traitement devrait en effet être assorti de « garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, *d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation* et de contester la décision. » (Nous soulignons). L'accès au droit à une « explication » ne ferait donc pas partie (de manière légalement contraignante) des dispositions du droit d'opposition, mais ne relèverait, selon ces mêmes auteurs, que d'un droit d'information *ex ante*.[41] Plus précisément, il s'agirait d'un devoir de notification des responsables du traitement *au moment où les données personnelles sont collectées*, dans le cas de l'article 13 §2(f), ou *préalablement au traitement,* dans le cas de l'article 14 §2(g). Sous ces conditions, le supposé « droit d'explication » ne saurait relever d'une description des processus exacts mis en œuvre pour aboutir à une décision particulière concernant un individu (puisque, en tout état de cause, ces décisions n'ont pas encore été réalisées, la notification précédant le traitement effectif des données personnelles). L'information devant être fournie par le responsable du traitement ne pourrait

39 - B. Goodman et S. Flaxman, « European Union Regulation on Algorithmic Decision Making and a Right to Explanation », *ICML Workshop on human interpretability in machine learning*, New-York, USA, 2016 (disponible sur [https://arxiv.org/abs/1606.08813]) ; B. Petkova et F. Boehm, « Profiling and the Essence of the Right to Data Protection », *Cambridge Handbook of Consumer Privacy*, Eds.: J. Polonetsky, O. Tene & E. Selinger, à paraître, 2018.

40 - L'article 22 §1 dispose en effet que « 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. »

41 - S. Wachter, B. Mittelstadt et L. Floridi, « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », *International Data Privacy Law*, vol. 2, n° 7, 2017, p. 76.

en effet alors consister qu'en une explication « générique » du processus mis en œuvre dans le traitement, un principe général de fonctionnement.

Bien que cette interprétation soit convaincante dans le contexte de la collecte des données (article 13) ou de leur traitement ultérieur (article 14, lorsque les données n'ont pas été collectées directement auprès de la personne concernée ou l'ont été pour un autre objet), il semble néanmoins que le Règlement autorise une interprétation plus large et permette, dans certaines occurrences au moins, de justifier un accès aux détails du mécanisme de décision ultérieurement au traitement. En particulier, l'article 15, qui concerne « le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données » semble le justifier. Ce « droit d'accès » s'applique en effet également une fois le traitement automatisé effectué et comprend, en sus d'un accès aux données personnelles ayant servi de base au traitement, une information relative à « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée. » Ainsi, même si l'article 22 du Règlement ne contient, en tant que tel, aucune mesure normative relative au droit d'explication,[42] l'application de l'article 15 offre bien un canal d'accès à la logique du traitement dans les conditions d'application de l'article 22 § 1, c'est-à-dire lorsqu'une décision est prise sur la base d'un traitement exclusivement automatisé et produisant des effets juridiques significatifs pour la personne concernée. Ce n'est donc pas seulement dans une configuration *ex ante* que le droit d'accès à la logique du système aura fonction à s'appliquer.[43] En outre, dans cette configuration, il serait envisageable, au moins en principe,

42 - Sandra Wachter, Brent Mittelstadt et Luciano Floridi ont en effet montré que la référence à un « droit d'explication », présent dans les versions initiales de l'article 22, avait été « reléguée » hors de la partie normative de l'acte, dans les considérants, dès 2014 (*Ibid.*, pages 9 à 11).

43 - Les dispositions de l'article 22 § 3 du Règlement donnent ainsi à la personne le droit « d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision ».

que l'information transmise ne se cantonne pas à une description générale du procédé de décision automatique, aux fonctionnalités du système donc, mais (puisque, dans ce cas, une décision spécifique a bien été prise) qu'il soit possible de revendiquer un accès aux circonstances particulières ayant conduit à cette décision. Nous reviendrons plus en détail sur ce point dans la section suivante.

B. Les conditions d'application du droit d'accès à la logique des algorithmes

Si un accès à une explication de la logique sous-jacente au traitement semble donc bien envisageable, qu'elle soit *ex ante* ou *ex post*, certaines interrogations subsistaient quant aux conditions d'application de l'article 22. Ainsi, la formulation étroite donnée à la condition préalable de « décision fondée *exclusivement* sur un traitement automatisé » (Article 22 §1, nous soulignons) pouvait laisser penser qu'une quelconque intervention humaine dans la chaîne de traitement interdirait l'application de l'article. Tout du moins, la formulation méritait précision.[44] Le groupe de travail de l'article 29 (qui rassemble, à l'échelle européenne, les représentants de chaque autorité indépendante de protection des données nationales.) vient de s'exprimer sur ce point au travers d'un jeu de recommandations, référence en matière d'interprétation du Règlement.[45] Le document précise ainsi que le champ d'application de l'article peut s'étendre aux cas où une activité humaine s'ajoute à un processus de décision automatique : « Le responsable du traitement ne peut éviter les dispositions de l'Article 22 en fabricant une participation humaine. Par exemple, si des profils générés automatiquement sont régulièrement appliqués à des individus sans aucune influence sur les résultats, les décisions devront être considérées comme provenant d'un traitement automatisé. Pour

44 - L'*Information Commissioner's Office* (ICO), l'autorité anglaise de contrôle en matière de traitement des données à caractère personnel, notait ainsi dans une publication récente que « *the interpretation of the word "solely" [...] requires further consideration* » et qu'il était « *debatable [...] whether "automated processing" means purely automated, or whether human involvement at any stage takes the processing out of the definition* ». (Information Commissioner Office, *Feedback request – profiling and automated decision-making*, v1.0, 6 avr. 2017, [https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf]).

45 - Article 29 Working Party Recommendation, 3 oct. 2017 (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083).

qu'une intervention humaine puisse être prise en compte il faut que l'influence sur la décision soit significative et ne se résume pas à un geste symbolique. »[46] Le caractère « exclusivement » automatisé du traitement semble donc devoir être interprété dans le sens d'un processus « essentiellement » automatisé, laissant dès lors la possibilité d'invoquer le droit même en présence d'une médiation humaine. Mais si cette interprétation est sans doute nécessaire pour éviter de rendre le droit inopérant dans la pratique, elle introduit néanmoins une marge d'interprétation quant au sens à attribuer à l'apport, substantiel ou pas, des interventions humaines en sus du traitement algorithmique.

Ces mêmes recommandations sont venues éclairer la nature des « effets juridiques » sur les personnes concernées par une décision automatisée et des effets « l'affectant de manière significative de façon similaire ». Concernant le premier effet, le groupe de travail précise : « La notion d'effet juridique suggère une activité de traitement ayant un impact sur les droits d'un individu, tel que la liberté d'association, le vote lors d'une élection ou la possibilité d'intenter une action en justice. Un effet juridique peut aussi avoir une incidence sur le statut juridique d'une personne ou sur ses droits en vertu d'un contrat. Par exemple, les décisions automatisées impliquant qu'un individu se voit accordé ou refusé le droit à un avantage social accordé par la loi, tel que l'allocation familiale ou logement ; qu'il se voit refuser l'entrée sur le territoire, qu'il soit soumis à des mesures de sécurité accrues ou à une surveillance de la part des autorités compétentes ; qu'un individu soit déconnecté automatiquement de son service de téléphonie mobile pour rupture de contrat, seront considérées comme ayant un effet juridique. »[47] Pour le second effet, il s'agira, « Pour qu'un traitement de données puisse affecter un individu de manière significative, les effets du traitement ne doivent pas être seulement triviaux et doivent être suffisamment importants pour justifier l'attention. En d'autres termes, la décision résultante doit avoir le potentiel d'influencer significativement les circonstances, le comportement ou les choix de l'individu concerné. Dans sa forme

46 - *Ibid.* Section II.A. (Notre traduction). Concernant la question du profilage, le document precise, dans le même sens, que : « *Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition* ». (Section II.A).

47 - *Supra*, not. n° 43, section II.B (Notre traduction).

la plus extrême, la décision peut conduire à l'exclusion ou à la discrimination des individus. »[48] Référence est faite dans ce contexte au considérant 71 du Règlement qui fournit quelques exemples pouvant entrer dans cette catégorie, tels que : « le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine. », mais le document aborde également le problème de l'utilisation du profilage dans le cadre du marketing ciblé. Bien que le plus souvent la publicité ciblée ne produise pas d'effets significatifs sur les individus, la situation contraire sera aussi envisageable, dépendant du degré d'intrusion du profilage, de la manière dont la publicité est présentée et de la vulnérabilité des personnes concernées.[49]

Ces précisions apportées, il reste que l'article 22 §2 du Règlement introduit un nombre d'exceptions qui pourront en pratique limiter significativement le droit de ne pas faire l'objet d'une décision automatisée. Ce sera le cas lorsque « la décision est nécessaire à l'exécution d'un contrat entre la personne concernée et un responsable du traitement», mais aussi lorsque la décision « 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 » et, enfin, lorsque la décision « est fondée sur le consentement explicite de la personne concernée » (notion de « consentement explicite » dont on connaît pourtant les limites pratiques de mise en œuvre face à la complexité des procédés de décision[50]).

48 - *Ibid.* (Notre traduction).

49 - En particulier dans ce contexte, il est noté que : « *[p]rocessing that might have little impact on individuals generally may in fact have a significant effect on certain groups of society, such as minority groups or vulnerable adults. For example, someone in financial difficulties who is regularly shown adverts for on-line gambling may sign up for these offers and potentially incur further debt.* » (*Ibid.*, section II.B). D'autres exemples sont fournis dans un autre document publié par le groupe de l'article 29 : *Guidelines for identifying a controller or processor's lead supervisory authority,* 5 Avr. 2017 (http ://ec.europa.eu/newsroom/document.cfm?doc id=44102).

50 - D. Le Métayer et C. Lazaro, « Le consentement au traitement des données personnelles: une perspective comparative sur l'autonomie du sujet », *La Revue Juridique Themis*, vol. 48, n° 3, 2014, p. 32 ; C. Paul et C. Féral-Schuhl, *Rapport d'information sur le droit et les libertés à l'âge du numérique*, Documents d'information de l'Assemblée nationale, oct. 2015, p. 136.

Section II – Le principe de transparence à l'épreuve des modèles prédictifs

§1 : L'opacité des modèles prédictifs : interpréter l'ininterprétable ?

A. La « logique sous-jacente » aux procédés algorithmiques, une notion en construction

Les dispositions des articles 13 §2(f), 14 §2(g) et 15 §1(h) imposent au responsable du traitement d'informer l'individu dont les données personnelles sont utilisées, lorsqu'un processus de traitement automatisé est susceptible de produire sur lui des effets juridiques (ou de l'affecter de manière significative, de façon similaire à des effets juridiques). Cette information consiste d'une part à signaler « l'existence d'une prise de décision automatisée » et, d'autre part, de présenter « des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».

Si le fait de rendre compte d'un traitement automatisé ne suscitera aucune difficulté particulière, le sens à donner à la notion d'« information utile » sur un traitement automatisé autorise, en revanche une grande latitude d'interprétation. Le considérant 60 indique que « le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités. Le responsable du traitement devrait fournir à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, *compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées* » (nous soulignons). Bilyana Petkova et Franziska Boehm ont ainsi considéré que l'article 13 §2(f) pouvait être interprété comme accordant à un individu le droit de recevoir une explication sur la logique ayant conduit *à une décision*[51]. Une première interprétation a pu en effet voir dans cette règle un droit d'accès *à un processus associé à un traitement spécifique* : la « logique sous-jacente » à une « prise de décision automatisée », en lien avec des données personnelles particulières, donc. C'est cette

51 - B. Petkova et F. Boehm, *supra*, not. n° 38.

même interprétation qui a pu associer la formulation des articles 13, 14 et 15 à la possibilité d'un supposé « droit d'explication ».[52] Or, nous l'avons vu, cette interprétation ne peut se concilier avec les dispositions des articles 13 et 14, dont la fonction est d'informer les individus, de manière préalable au traitement, d'une éventuelle décision basée sur des données personnelles, afin, notamment, qu'il soit possible à chacun d'accorder son consentement (condition de la licéité du traitement, au sens de l'article 6 §1(c) du Règlement).[53] Et puisque cette information précède le traitement en propre, dès qu'une décision sera susceptible d'avoir une conséquence juridique significative *pour un individu quelconque*, l'information quant à la logique sous-jacente devra nécessairement être communiquée, mais il ne pourra s'agir que d'une description générique du modèle décisionnel.

Les dispositions de l'article 15 §1(h) pourraient en revanche permettre de requérir une information sur le mécanisme logique ayant conduit à une décision particulière. Le droit d'accès inscrit à l'article 15 n'a pas en effet vocation à s'exercer uniquement *ex ante*, comme dans le cas du droit d'information cité précédemment, mais également *ex post*, après que les données ont passé le filtre du processus automatisé. Dans ce cas, il serait légitime que l'individu ayant été l'objet d'une décision particulière puisse revendiquer une explication sur les raisons spécifiques à cette décision. Les recommandations du groupe de travail ne vont cependant pas dans ce sens. Elles indiquent que l'« [a]rticle 15(1)(h) permet aux personnes concernées d'obtenir les informations relatives à un traitement automatisé, y compris le profilage, selon les dispositions des articles 13(2)(f) and 14(2) (g)... La personne responsable du traitement devrait avoir déjà fourni ces informations à la personne concernée par application de l'article 13. »[54] Ou encore que : « L'article 15 implique une forme plus générale de contrôle que le droit à l'explication d'une décision particulière. Néanmoins, à

52 - B. Goodman et S. Flaxman, 2016, *supra* not. n° 38.

53 - La notion de « consentement explicite » énoncée à l'article 22 §2(c) diffère du consentement « simple », en tant que prérequis à la licétité du traitement, tel qu'inscrit dans les dispositions de l'article 6 §1(a). Les spécificités d'un tel « consentement explicite » ne sont pas explicitées plus avant dans le Règlement. Les recommandations du groupe de travail de l'article 29 indiquent en ce sens que : « *explicit consent is not defined in the GDPR but suggests that the consent must be specifically confirmed by an express statement rather than some other affirmative action*. », v. *supra*, not. n° 43.

54 - *Supra*, not. n° 43, section III.D.2. (Notre traduction).

travers l'exercice de ce droit, la personne concernée peut prendre connaissance d'une décision prise à son endroit, y compris celle basée sur le profilage. »[55] C'est donc, dans cette interprétation au moins, seulement à une information générale, non spécifique aux caractéristiques d'un individu donné, que les dispositions de l'article 15 §1(h), tout comme celles des articles 13 §2(f), 14 §2(g) , pourront donner accès.

Dans ce cas, la nature de l'information proposée sera donc pratiquement limitée à une présentation du cadre général de fonctionnement du processus automatisé, à commencer par la nature des données d'entrée utilisées et les catégories de projection de ces données (à l'issue du traitement) sur lesquelles la décision sera fondée. Entre ces « entrées » et ces « sorties », le processus algorithmique lui-même ne pourra être décrit que de manière générique (sauf dans les cas les plus simples, où une relation univoque entre données personnelles, catégories de projection, et décision finale peut être retracée), sans lien spécifique aux données de la personne concernée. Dans le cas d'une demande de crédit, par exemple, dans laquelle le responsable du traitement détermine un score afin d'accorder ou pas la demande, les informations à fournir, toujours selon le groupe de travail de l'article 29, devront au minimum inclure les caractéristiques considérées pour déterminer le score et valider la décision (à savoir, dans ce cas, les données fournies par l'utilisateur et toute autre information s'y rapportant : historique de crédit, informations publiques relatives à l'insolvabilité de la personne concernée), sans aucune mention à la « logique » du processus, c'est-à-dire aux décisions ayant permis de déduire de ces données d'entrée un score effectif. Il s'agirait donc là d'une version bien appauvrie de la notion de « logique sous-jacente » au traitement automatisé. L'interprétation définitive du sens à donner à la notion de « logique sous-jacente » reste de toute évidence encore à clarifier, mais si le principe de transparence qui sous-tend ces prérogatives (au moins « en ce qui concerne les fonctions et le traitement des données à caractère personnel et [en ce qu'il permette] à la personne concernée de contrôler le traitement des données »[56]) ne se réduise

55 - *Supra*, not. n° 43, section IV.D.2. (Notre traduction).

56 - Considérant 78, Règlement (UE) 2016/679.

pas à un prétexte de transparence,[57] cette logique ne saurait se restreindre aux seules données à la source du traitement. De fait, selon les dires mêmes du groupe de l'article 29, le responsable du traitement devrait fournir *les raisons* ayant conduit à une décision : « Le responsable du traitement devrait trouver une manière simple de fournir à la personne concernée par le traitement les raisons sous-jacentes à la décision, ou les critères utilisés pour y parvenir, sans nécessairement recourir à une explication complexe de l'algorithme utilisé ni en dévoilant l'algorithme dans sa totalité »[58].

Si le Règlement méritera clarification, les dispositions de l'article 4 la loi pour une République numérique sont quant à elles explicites : « une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande. » Les « règles » du processus algorithmiques devront dans ce cas être explicitées par le responsable du traitement. L'article R. 311-3-1-1 inscrit à présent au code des relations entre le public et l'administration, apporte encore des précisions utiles sur la nature des informations à fournir. Elles devront ainsi inclure : « 1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ; 2° Les données traitées et leurs sources ; 3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ; 4° Les opérations effectuées par le traitement. » Dans le même sens, au Royaume-Uni, les dernières modifications à la « *Data protection bill* » (qui viendra remplacer le « *Data protection act* », en ligne avec le Règlement (UE) 2016/679) ont proposé l'inclusion d'une clause relative au droit à l'information dans le contexte du profilage algorithmique lorsqu'il est le fait d'une autorité publique. Cette nouvelle clause spécifie que l'information devra comprendre non seulement les données sources, mais aussi les *pondérations*

57 - Ou une « illusion de transparence » selon l'expression de David Heald (D.A. Heald, *Transparency as an Instrumental Value, in : Transparency : The key to a better governance ?* sous la dir. de C. Hood et D.A. Heald, Oxford University Press, 2006).

58 - *Supra*, not. n° 44, section IV.D.2. (Notre traduction).

dont dépend la détermination du profil.[59] Il faudra donc bien, dans ces diverses interprétations, traduire de manière compréhensible certaines des caractéristiques essentielles du processus algorithmique menant des données personnelles à la décision.

En France, la difficulté d'un accès à la logique sous-jacente aux décisions prises par un processus automatisé a été récemment soulignée par l'affaire APB (« Admission Post-Bac »). Le système, de pré-inscription dans l'enseignement supérieur et d'affectation des futurs étudiants dans les diverses formations, repose en effet sur un procédé algorithmique (de type arbre de décision) à partir du domicile du candidat, de sa situation de famille et de l'ordre de préférence des vœux qu'il a formulés. Face à l'absence de transparence de la méthode d'affectation, l'association « Droits des lycéens » avait initié en 2016 une demande d'accès au code source, à laquelle la Cada (« Commission d'accès aux documents administratifs ») avait donné un avis favorable.[60] Le ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche a alors donné un accès, partiel, au code source (la logique du procédé était dans ce cas directement inscrite en langage informatique, l'accès au code était donc essentiel). Le code n'avait été communiqué cependant que dans un format papier, sans commentaires et ne concernait qu'un des algorithmes concernés.[61] La mission Etalab d'avril 2017 a alors proposé de « publier, sans attendre une nouvelle demande de communication, le code source de la dernière version d'APB et les données non-réidentifiantes

59 - https://services.parliament.uk/bills/2017-19/dataprotection.html. En revanche, la nouvelle loi allemande sur la protection des données personnelles, le *Bundesdatenschutzgesetz*, adoptée par le parlement fédéral allemand le 27 avril 2017, qui est venue adapter la législation allemande aux dispositions du Règlement (UE) 2016/679 n'a pas ajouté de précision quant aux informations à fournir en cas de traitement algorithmique des données.Ò

60 - CADA, avis n° 20161989 du 23 juin 2016.

61 - S. Graveleau, « APB : les questions que soulève le code source », *Le Monde*, 25 oct. 2016 (relayant la frustration de la communauté des développeurs alors engagée à décrypter le dispositif : « Comment interpréter un code informatique sans la documentation technique détaillant les « variables » utilisées ? Sans le cahier des charges qui va avec et qui explique le schéma des bases de données utilisées par l'algorithme en question ? »).

associées. »[62] Dans le même temps, la CNIL a décidé d'engager un contrôle du dispositif pour en évaluer la conformité. Constatant plusieurs manquements aux dispositions de la loi informatique et libertés, la présidente de la CNIL a mis en demeure, le 30 août 2017, le ministère de se mettre en conformité avec la loi dans un délai de trois mois.[63] La décision souligne ainsi un manquement au droit d'accès et au droit à l'information : « aucune information relative à l'utilisation d'un algorithme et au fonctionnement de celui-ci pour procéder au classement et à l'affectation des personnes au sein des établissements de l'enseignement supérieur (notamment la méthode ayant permis de développer l'algorithme, les contraintes ou les besoins définis par l'administration, le taux d'erreur de l'algorithme ou encore le score obtenu par le candidat, les seuils de *scoring* et leur signification) n'est fournie aux candidats. » Elle note également l'absence d'intervention humaine pour l'affectation des candidats dans les filières non sélectives : « une décision produisant des effets juridiques à l'égard des candidats est prise sur le seul fondement du traitement APB », contrairement aux dispositions de l'article 10 de la loi informatique et libertés. Le dévoilement du code a donc été ici un prérequis pour évaluer sa conformité et permettre de remédier, finalement, à ses défauts.

B. Un accès à la logique en bute face aux modèles prédictifs

L'application de ce droit d'accès à la logique du traitement automatisé sera pourtant mise en difficulté par l'utilisation de procédés statistiques de décision, dont les réseaux de neurones profonds sont aujourd'hui le principal moteur. Le développement de ces nouveaux intermédiaires algorithmiques, dont il était difficilement envisageable de prévoir la prévalence actuelle lorsque les premières versions du Règlement ont été conçues, impose un exercice d'interprétation supplémentaire. Un effort illusoire peut-être. Le recours aux algorithmes d'apprentissage est en effet préconisé là même où l'on ne peut formuler de règle précise décrivant le

62 - Recommandation n°1, *Rapport de la mission Etalab sur les conditions d'ouverture du système Admission Post-Bac*, Avril 2017. ([http://www.ladocumentationfrancaise.fr/rapports-publics/174000345/index.shtml]).

63 - CNIL, décision n° MED-2017-053 du 30 août 2017.

phénomène que l'on souhaite prédire ou représenter.[64] C'est au procédé lui-même de formuler, par induction, une représentation interne, un modèle. Or, ce langage intérieur, propre à la machine, n'a pas fonction à être humainement interprétable. Comment, alors, concilier l'opacité intrinsèque de ces opérateurs algorithmiques avec l'exigence légale de transparence des décisions issues de processus automatisés au sens du Règlement ou de la Loi pour une République numérique ? Comment extraire « des informations utiles sur la logique sous-jacente » et permettre que cette information soit fournie de manière concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples » (pour reprendre la formulation de l'article 12 §1 du Règlement) ?

Les décisions issues d'un traitement automatisé émergent d'une architecture composée d'un ensemble d'entités : algorithmes, codes informatiques, bases de données, modèles prédictifs. Chacun de ces éléments participe à l'élaboration d'un produit final (à savoir une classe, une catégorie, un score ou un profil associé à un individu donné), chacun s'exprime dans un langage spécifique (il s'agira par exemple de règles formelles ou d'expressions mathématiques pour l'algorithme, d'un langage informatique particulier pour le code, de listes ou de tableaux pour les bases de données). Lorsque le règlement propose d'expliciter une logique sous-jacente au procédé de traitement, lequel de ces éléments, lequel de ces langages faudra-t-il invoquer ? Il semble évident que le simple dévoilement, *tel quel*, d'un programme informatique, d'une structure algorithmique abstraite, des giga-octets de données d'un répertoire ne rempliront aucune des conditions de l'article 12 §1 du Règlement.[65] Quelles règles issues de cet assemblage hybride devront alors être proposées par le responsable du traitement sous forme « concise » et « compréhensible » ?

64 - « *Machine learning is applied to the sorts of problems for which encoding an explicit logic of decision-making functions very poorly* » (Jenna Burrell, « How the machine 'thinks': understanding opacity in machine learning algorithms », *Big Data and Society*, Jan.-Jun. 2016, p. 1). Dans le même sens : « *the whole reason we turn to machine learning rather than handcrafted decision rules is that for many problems, simple, easily understood decision theory is insufficient.* » (Z.C. Lipton, «The Mythos of Model Interpretability», arXiv preprint n° 1606.03490, 2016).

65 - À moins de supposer le public capable d'interpréter sans effort excessif l'un ou l'autre de ces objets, c'est à dire à considérer chacun comme un informaticien ou un mathématicien en puissance.

Retraçons les fonctions de ces différents éléments dans le cas des modèles prédictifs, en particulier dans le contexte de l'apprentissage automatique. L'algorithme est d'abord constitué d'un ensemble de règles qui décrivent la manière dont il est possible, sur la base d'exemples, au travers d'une phase d'entrainement, d'approximer la solution à un problème donné (ce pourra être, par exemple, un problème de classification : prédire la solvabilité des personnes demandant un crédit, les centres d'intérêt d'un internaute afin de lui proposer une publicité adaptée). À partir de données réelles, par confrontation systématique entre les prédictions issues du modèle prédictif et les catégories attendues,[66] et par correction des paramètres constitutifs d'un « modèle », l'algorithme d'apprentissage permet de construire, une fois l'entrainement achevé, une représentation interne du problème et de sa solution. Cet algorithme, initialement exprimé sous forme de règles formelles, pour pouvoir être appliqué en pratique à des données d'utilisateurs (qu'elles soient recueillies « en ligne » ou stockées dans des bases de données) requiert d'être traduit dans un langage informatique. Mais ces objets (algorithme, code, base de données) ne sont que les préalables nécessaires à la formation de l'opérateur de décision final : le modèle. C'est en effet lui qui recueille et condense en un objet unique l'expérience captée à partir des données d'entrainement. C'est lui qui contient la « logique » prédictive qui, appliquée à de nouvelles données permettra d'obtenir une prédiction (si un crédit doit être accordé ou pas à un nouveau demandeur, le type de publicité qui sera présentée sur la page Internet). Ce modèle final déduit de manière empirique directement à partir des corrélations présentes dans le corpus de données, peut s'exprimer sous maintes formes : arbres de décisions, forêts aléatoires, graphes Bayésiens, machines à supports vecteurs, ou encore l'une des multiples instances des architectures neuronales (le choix de l'une ou l'autre de ces structures étant déterminé par les contraintes du problème posé, par des considérations d'efficacité, la nature des données, etc.). Quelle que soit son expression, et bien

66 - Ces « catégories » (encore dénommées « classes » ou « labels ») assignent une interprétation aux données fournies à l'algorithme. Dans le cadre d'un apprentissage « supervisé », ces catégories et leurs valeurs sont préalablement définies par des humains et attribuées à des exemples utilisés pour entrainer le modèle. L'algorithme construit alors un modèle en apprenant à assigner les bonnes catégories aux données d'entrées tout en maintenant une capacité de généralisation maximale. D'autres approches, dites « non supervisées » laissent la machine découvrir d'elle-même ces catégories à partir du contenu des données d'entraînement.

qu'il remplisse son objectif en terme d'efficacité de prédiction, la mécanique de classification ou de profilage qu'il met en jeu ne sera dans aucun cas l'expression d'un opérateur humain. Ni la personne ayant conçu l'algorithme, ni l'informaticien l'ayant traduit en code informatique, ni le responsable des bases de données ou de la phase d'apprentissage ne sont à même de prédire les caractéristiques précises du modèle qui en est déduit.[67] Ce sera pourtant le lieu de la décision. Le modèle prédictif agit en effet comme un opérateur, une fonction de transformation d'un espace d'entrée formé par les données (une adresse IP, un historique de navigation, un mot clef, etc.) ou par des grandeurs caractéristiques dérivées, et produisant en sortie une prédiction. Ainsi, puisque les décisions sont effectivement le produit direct des modèles prédictifs, c'est bien la « logique sous-jacente » à ces objets qu'il s'agirait, en principe au moins, de dévoiler.

En principe seulement, car alors que les manifestations de ce modèle nous sont directement accessibles, puisque la machine est conçue pour émettre une prédiction interprétable (un profil individuel, une probabilité d'appartenance à une catégorie), dès que la dimension du problème à résoudre s'élève (le nombre de paramètres décrivant le profil, la complexité de la topologie utilisée pour représenter le modèle), l'enchaînement déterministe permettant d'arriver à une prédiction échappera, lui, à toute traduction.[68] Dans le cas des réseaux de neurones artificiels, les données en entrées seront ainsi séquentiellement pondérées, croisées, transformées. À chaque couche de l'architecture, ce brassage non-linéaire produira de nouvelles grandeurs qui subiront à leur tour, à la couche suivante,

67 - Sans nier pour autant la nécessaire intervention de l'homme dans la chaîne d'apprentissage : selon les cas, il choisit l'origine des données d'entrainement, propose les exemples et les labels associés et définit la « fonction d'utilité », l'objectif à satisfaire, mais il n'en est pas moins absent de la formulation du modèle appris par l'algorithme. Alors que le processus algorithmique d'apprentissage - aussi complexe soit-il - peut être compris (c'est-à-dire que sa logique peut s'expliquer, le choix des paramètres peut être justifié, les corpus de données utilisés pour la formation peuvent être analysés), son produit, le modèle lui-même, reste inaccessible à une interprétation directe. Sous une apparence « d'objectivité algorithmique » (soutenue par une efficacité quantifiée, telle que mesurée, par exemple, par un score de confiance ou un taux d'erreur sur un ensemble d'apprentissage), la décision émerge directement de la machinerie interne au modèle, ininterprétable le plus souvent, et ne reflète qu'indirectement le processus algorithmique qui a servi à construire le modèle.

68 - Sauf dans certaines architectures (par exemples le arbres de décision) et sauf à sacrifier l'efficacité du modèle (en limitant les caractéristiques d'entrée, en réduisant le nombre de paramètres et la dimension de l'espace de représentation).

un nouveau mélange. Alors même que la richesse prédictive des modèles est le fruit de ce mécanisme, déterministe, de croisement, la variété combinatoire qu'il exprime ne pourra se réduire à une interprétation « concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ». La fonction de l'algorithme d'apprentissage est en effet en premier lieu de minimiser une erreur de prédiction et de produire un modèle susceptible de généralisation à de nouveaux cas, non pas de fournir une représentation sous une forme humainement intelligible,[69] puisqu'en effet, Leo Breiman le souligne : « l'objectif n'est pas d'être interprétable mais de produire des informations précises ».[70]

À cette opacité du modèle s'ajoute la difficulté d'interpréter le résultat, non pas en tant que tel, mais en relation avec les données d'entrée. Les procédés de décision automatique sont en effet des systèmes de détection de *corrélations* entre paramètres, ce ne sont pas des moyens d'expliciter les éventuelles relations *causales* entre variables d'entrée et de sortie, entre données personnelles et décisions.[71] Pourrait-on alors imaginer transcrire ces modèles en une structure plus simple ? Bien qu'il existe en effet des procédures de conversion,[72] elles restent cependant largement approximatives.

69 - À quelques exceptions près, cependant. Par exemple, les « arbres de décisions » permettent de suivre pas à pas, dans une structure hiérarchique, les variables identifiées comme étant les plus à même de catégoriser les données d'entrainement. Des méthodes de guidage de l'entrainement (S. Tan, K.C. Sim et M. Gales, « Improving the interpretability of deep neural networks with stimulated learning », *IEEE Workshop on Automatic Speech Recognition and Understanding* (ASRU), 13 dec. 2015, p. 617-623), d'analyse *a posteriori* (M.T. Ribeiro, S. Singh et C. Guestrin, Why Should I Trust You?: Explaining the Predictions of Any Classifier. KDD 2016, San Francisco, arXiv preprint n° 1602.04938, 16 fev. 2016) ou de « visualisation » des modèles sont aussi parfois utilisées (par exemple dans le cas de l'apprentissage profond : J. Yosinsky et al., «Understanding Neural Networks Through Deep Visualization», *Deep Learning Workshop, 31st International Conference on Machine Learning (ICML)*, Lille, France, 2015, p. 1-12).

70 - Notre traduction : « *the goal is not interpretability, but accurate information* » (L. Breiman, « Statistical modeling, the two cultures », *Statistical science*, vol. 16, n° 3, p. 199).

71 - « *Machine optimizations based on training data do not naturally accord with human semantic explanations. The workings of machine learning algorithms can escape full understanding and interpretation by humans, even for those with specialized training, even for computer scientists.* » (J. Burrell, *supra,* not. n° 61). Une discussion, plus approfondie, sur les limites d'interpretabilité des modèles statistiques est proposée dans G. Shmueli, « To explain or to predict ? », *Statistical science,* vol. 25, n° 3, 2010, p. 289 et dans Lipton, *Supra*, not. n° 63.

72 - J.J. Thiagarajan et al., «TreeView: Peeking into Deep Neural Networks Via Feature-Space Partitioning », arXiv preprint n° 1611.07429, 2016.

Pour reprendre l'expression de Jenna Burrel, elles « conduisent à une compréhension au mieux incomplète et, au pire, à un faux sentiment de sécurité ».[73]

Ainsi, l'intermédiation d'un filtre opaque dans la séquence de traitement des données personnelles entrave la traçabilité des décisions : s'il est autorisé à fonctionner sans contrainte, le modèle statistique pourrait donc servir « d'écran » entre ses concepteurs et les individus sur lesquels il opère. Que faire alors face à ce constat ? Si de tels systèmes sont réfractaires à toute interprétation, faudrait-il en interdire l'utilisation lorsqu'ils sont à même de conduire à des décisions juridiques « significatives » ? Si aucune interprétation des décisions prises ne peut être obtenue, faudrait-il en déduire, avec Mireille Hildebrandt, que « les réseaux de neurones et autres formes de profilage par induction ne peuvent être utilisés dans la mesure où ils rendent inapplicable la condition d'accès à une information interprétable. »[74] Ce n'est pas l'avis du groupe de travail de l'article 29, qui, reconnaissant d'une part la place croissante des procédés d'apprentissage statistique dans les usages quotidiens et, d'autre part, le fait que leur complexité pourra s'opposer à leur compréhension,[75] propose en revanche une information « à deux niveaux ». Le groupe recommande en effet de rendre compte en priorité des catégories

73 - Notre traduction : « *explanations that bring forward a human-manageable list of key criteria (i.e. the 10 most heavily weighted/spammy words present in an email or a single sentence description) provide an understanding that is at best incomplete and at worst false reassurance.* » (J. Burrel, *Supra*, not. n° 63).

74 - Notre traduction: « *neural networks and other forms of bottom-up profiling cannot be used insofar as they render the provision of meaningful information impossible.* » (Mireille Hildebrandt, *Smart technologies and the end(s) of Law*, Edward Elgar Publishing, 2016, p. 198-199). Ceci est d'autant plus pertinent qu'il a été démontré que les modèles neuronaux pouvaient être manipulés (pour aboutir à des résultats arbitraires) en modifiant leur entrée d'une manière imperceptible pour les observateurs humains (see A. Nguyen, J. Yosinski et J. Clune, « Deep neural networks are easily fooled: High confidence predictions for unrecognizable images », *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015, p. 427 ; C. Szegedy, et al., « Intriguing properties of neural networks », arXiv preprint n° 1312.6199, 2013). Des perturbations mineures sur les données d'entrée peuvent induire une classification incorrecte et, par conséquent, conduire à des décisions tout aussi peu fiables. Si tel est le cas, comment un résultat obtenu par un tel modèle peut-il vraiment être fiable? Quand un processus automatisé est-il suffisamment sûr pour être appliqué aux personnes concernées, notamment lorsque le procédé de traitement est susceptible de produire des « effets juridiques la concernant ou l'affectant de manière significative de façon similaire » (Considérant 71 et Article 22 §1 du Règlement).

75 - Article 29 Working Party Recommendations, *Supra* not. n° 43, section III.D.1.

(par exemple, les types de profils) utilisées lors du traitement et de la raison pour laquelle ces catégories sont considérées utiles à la prise de décision. Les détails sur le fonctionnement mathématique de l'algorithme seraient alors réservés aux seuls experts, si nécessaire, afin qu'ils puissent éventuellement évaluer le fonctionnement du processus prédictif.[76] Une approche pragmatique sans nul doute, mais qui n'offre qu'une solution partielle. En effet, si la décision est le produit du modèle issu d'un apprentissage statistique (un réseau de neurones profonds, par exemple), elle échappera autant à l'expert qu'au profane. Aux mieux, les experts ne pourront valider que le processus d'élaboration de ce modèle (à partir non seulement de sa construction algorithmique, mais aussi des données ayant servi à son entrainement, des contraintes et des choix stratégiques auxquels il a été soumis), sans atteindre à la « logique sous-jacente » du processus de décision lui-même. L'accès à cette information reste néanmoins crucial pour comprendre le contexte dans lequel l'outil décisionnel a été construit et pourra certainement renseigner sur les intentions des responsables du traitement autant que sur leur diligence à suivre les bonnes pratiques, en terme de respect de la vie privée notamment.

§2 : Le secret des modèles prédictifs, source d'opacité

A. Les modèles prédictifs et le recours au secret

Les dispositions des articles 13 §2(f), 14 §2(g) et 15 §1(h) du Règlement, même à n'y voir qu'un accès à une information générique (non spécifique à un individu donné), s'accommodent donc bien difficilement de ces nouveaux outils de décision. L'opacité technique, intrinsèque aux modèles statistiques, n'est pourtant pas seule à s'opposer à une application directe du principe de transparence. D'autres forces contribuent en effet à limiter l'accès aux procédés de traitement automatique. Des algorithmes de classement des moteurs de recherche, jusqu'aux procédés de recommandation

76 - « *Information about the categories of data that have been or will be used in the profiling or decision making process and why these are considered pertinent will generally be more relevant than providing a complex mathematical explanation about how algorithms or machine-learning work, although the latter should also be provided if this is necessary to allow experts to further verify how the decision–making process works.* » (*Ibid.*, Annex 1).

des plateformes de vente en ligne, de l'algorithme de classement pageRank de Google[77], aux systèmes de tarification « intelligents » de Uber[78], l'ubiquité du traitement algorithmique des données semble s'accompagner presque systématiquement d'un recours au secret. Mais comment alors, s'interrogent Danièle Citron et Frank Pasquale, « remettre en question le processus d'évaluation et [ses] résultats [si] l'algorithme est un secret d'affaire jalousement gardé »[79] ? Comment le « droit d'information » sur les processus de décision automatisés peut-il alors s'articuler avec le respect du secret des affaires ?

Les modèles statistiques construits à partir de données personnelles sont le produit d'investissements substantiels, à la fois en terme financier et de recherche et développement. En assurer la protection est donc d'un intérêt crucial, autant sur le plan économique que stratégique, pour les entreprises qui en sont à l'origine. De fait, les modèles prédictifs sont le résultat de processus algorithmiques complexes, ayant requis la collecte et l'analyse – souvent laborieuse – de grandes quantités de données. Les détenteurs de ces modèles pourraient ainsi justifier d'une quasi-propriété sur ces objets mais également sur les constructions qui en sont dérivées (y compris les profils individuels et les décisions qui en sont issues). Or, ces objets particuliers se prêtent mal à une protection par le droit d'auteur ou le droit des brevets. En revanche, puisqu'ils constituent, par construction même, de véritables « boites noires », l'impossibilité d'en interpréter le contenu est considérée garante de leur inaccessibilité. Ainsi, la protection des modèles d'inférence est aujourd'hui largement assurée par le secret.[80] En tant qu'objets de propriété intellectuelle, de nombreuses juridictions en limitent de ce fait l'accès, y compris dans le contexte d'un « droit à

77 - « *Nobody outside of Google knows the exact details of its search algorithms and, despite the best efforts of the search engine optimization crowd, nobody has been able to fully figure them out.* » (V. Lindberg, *Intellectual property and open source*, O'Reilly, 2008, p. 130).

78 - F. Marty, «Algorithmes de prix, intelligence artificielle et équilibres collusifs», *Sciences Po OFCE working paper n° 2017-14*, 2017 ; N. Diakopoulos, «Accountability in algorithmic decision making », *Communications of the ACM*, vol. 59, n° 2, 2016, p. 56.

79 - « *No one can challenge the process of scoring and the results because the algorithms are zealously guarded trade secrets* » (D.K., Citron et F. Pasquale, « The scored society: due process for automated predictions », *Wash. Law Rev.*, vol. 89, n° 1, 2014, p. 1).

80 - D.L. Wenskay, «Intellectual property protection for neural networks», *Neural networks*, vol. 3, n° 2, 1990, p. 229.

l'information » des personnes sujettes à un traitement automatisé.[81] L'article 39 §5 de la loi informatique et libertés dispose ainsi que « les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle ». L'article 8(5) du *UK data protection act 1998* dispose dans le même sens que « la mise à disposition [du requérant] de la logique sous-jacente au processus de décision automatisé n'est pas requise si cette information constitue un secret des affaires »[82] (notre traduction). Le Règlement (UE) 679/16 stipule de même dans ses considérants que le droit d'accès à la logique du traitement « ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel ».[83] En Allemagne, la section 29 du *Bundesdatenschutzgesetz*, dont les dispositions ont été adoptées par le Parlement fédéral allemand le 27 avril 2017 détaille les droits des sujets face aux obligations de protection des secrets. Il y est précisé que « [l]e droit d'accès conformément à l'article 15 du règlement (UE) 2016/679 ne s'applique pas dans la mesure où l'accès divulgue des informations qui, par la loi ou par leur nature, doivent être tenues secrètes, notamment en raison des intérêts supérieurs légitimes d'un tiers. »[84] Or, malgré ces restrictions explicite à la divulgation des objets de propriété intellectuelle, le Règlement précise cependant que « ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée ».[85] Quelles caractéristiques des modèles statistiques et des procédés algorithmiques doivent alors être dévoilées et quelles autres justifient d'un maintien dans le secret ? Comment articuler la prise en considération du droit à l'information des individus sur les procédés de traitement de leurs données personnelles et les

81 - V. dans ce sens : Considérant 39 et Art.5(1)(a) du Règlement.

82 - « *Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in any decision-taking if, and to the extent that, the information constitutes a trade secret.* » (Data Protection Act 1998, section 8 §5).

83 - Considérant 63 du Règlement.

84 - Notre traduction : « *Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.* » (Bundesdatenschutzgesetz, §29(1)).

85 - Considérant 63 du Règlement.

droits de propriété intellectuelle et du secret des affaires ? Giovanni Commandè n'hésite pas à voir dans cette confrontation l'émergence d'un nouveau « choc juridique » entre droit fondamental des individus au respect de leur vie privée et les intérêts des entreprises qui collectent les données et en tirent profit.[86]

Cette confrontation a d'ailleurs fait récemment l'objet d'une décision de la Cour suprême fédérale allemande (*Bundesgerichtshof*) du 28 janvier 2014, qui a rejeté une demande d'information relative à un procédé algorithmique d'attribution de crédits financiers, au motif que ces derniers étaient protégés par le secret d'affaires.[87] La Cour affichait ce faisant sa volonté de protéger la valeur commerciale du procédé de traitement automatique au détriment du droit d'accès à la logique d'attribution des crédits.

Un autre exemple de conflit entre un accès aux données personnelles, cette fois, et le secret des affaires est à l'origine de l'affaire qui a opposé Max Schrems à Facebook et a conduit à l'invalidation du dispositif « safe harbour » (qui autorisait le transfert de données de l'Europe vers les Etats-Unis.).[88] La demande faite par M. Schrems en juillet 2011 d'accéder à la totalité des données que Facebook détenait sur lui avait été refusée.[89] Se référant au Code irlandais de protection des données, la plateforme avait opposé l'exception au droit d'accès au motif que ces données constituaient un secret des affaires : « *Section 4(12) of the Acts carves out an exception to subject access requests where the disclosures in response would adversely affect trade secrets or intellectual property. We have not provided any information to you which is a trade secret or intellectual property of*

86 - « *A modern clash of rights seems to emerge in the classifying society—between, on the one hand, the right of individuals to control their own data, and, on the other, the interest of business in continuously harnessing that data as an asset. The latter are increasingly protected by IP or quasi IP as trade secrets* » (G. Commandè, « Regulating Algorithms' Regulation? First Ethico-Legal Principles, Problems, and Opportunities of Algorithms », *Transparent Data Mining for Big and Small Data*, sous la dir. de T. Cerquitelli, D. Quercia et F. Pasquale, Spinger, 2017, p. 186).

87 - Bundesgerichtshof, 28 janv. 2014, cas n° VI ZR 156/13. V. en particulier le point 29.

88 - CJUE, arrêt du 6 octobre 2015 (C-362/14).

89 - Dans un entretien avec le magazine ZDNET, Max Schrems notait ainsi que « *his Likes, his facial recognition data, and the data generated by the Like button was not in the package he received.* » (Europe versus Facebook: The law protects program logic, not data, ZDNET, 13 oct. 2011, [http://www.zdnet.com/article/europe-versus-facebook-the-law-protects-program-logic-not-data/]).

Facebook Ireland Limited or its licensors. »[90]

Plus récemment, des affaires aux États-Unis ont conduit à des jugements contradictoires, décidant dans certains cas de faire prévaloir le secret des affaires et d'accorder, dans d'autres, un accès aux traitements algorithmiques des données personnelles. Dans une première affaire, le requérant, M. Loomis, avait été condamné en 2013 après avoir plaidé coupable pour conduite d'une voiture volée et délit de fuite[91]. Le juge de première instance avait utilisé, pour déterminer la peine, un outil de profilage (« COMPAS », pour « *Correctional Offender Management Profiling for Alternative Sanctions* », logiciel développé par Northpointe Inc.), permettant d'évaluer automatiquement le risque de récidive[92], risque estimé particulièrement élevé dans le cas de M. Loomis. Le juge suivit les recommandations de COMPAS et M. Loomis fut condamné en conséquence à 6 ans d'emprisonnement. M. Loomis interjeta appel contre ce jugement, la décision ayant été basée, en partie au moins, sur un algorithme protégé par le secret des affaires : ni lui ni le juge n'avaient eu les moyens d'examiner la formule utilisée pour déterminer la probabilité de récidive.[93] La Cour suprême du Wisconsin confirma cependant la décision. Le respect de la propriété intellectuelle de Northpointe Inc. requérait de ne pas dévoiler l'algorithme et que bien que secret, le calcul du score obtenu par le procédé automatique n'avait été qu'un élément de la décision du juge. Cependant, dans une opinion concordante jointe à la décision, Shirley S. Abrahamson, l'un des juges de la Cour suprême reconnait

90 - Lettre de Facebook Ireland Ltd à Max Scherms datée du 20 septembre 2011 : [http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf].

91 - Précisément : « *attempting to flee a traffic officer and operating a motor vehicle without the owner's consent.* » (Loomis 881 N.W.2d 749, Wis. 2016, point 754).

92 - T. Brennan et al., « Evaluating the Predictive Validity of the COMPAS Risk and Needs Assessment System», *36 Crim. Just. & Behav.*, vol.21, 2009. L'utilisation de tels procédés est une pratique de plus en plus fréquente aux Etats-Unis. V. en ce sens : P.M. Casey et al., «Nat'l Ctr. for State Courts, Using Offender Risk and Needs Assessment Information at Sentencing:», *Guidance for Courts from a National Working Group*, vol. 1, 2011, p. 1 ; R. Wexler, « Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System », *Stanford Law Review*, vol. 70, 2018, à paraître.

93 - « *Northpointe, Inc., the developer of COMPAS, considers COMPAS a proprietary instrument and a trade secret. Accordingly, it does not disclose how the risk scores are determined or how the factors are weighed. Loomis asserts that because COMPAS does not disclose this information, he has been denied information which the circuit court considered at sentencing.* » (Eric L. Loomis v. Wisconsin, cour suprême du Wisconsin. 881 N.W.2d 749 Wis. 2016, point 761).

que « le manque de compréhension de COMPAS était un problème important » et que le refus de la Cour d'évaluer le fonctionnement de COMPAS avait été une erreur.[94] En effet, comment justifier de la décision si elle repose (même partiellement) sur un score algorithmique dont on ne peut vérifier le bien-fondé ?

Dans une seconde affaire, l'American Civil Liberties Union (ACLU) avait initialement exigé des explications sur la baisse soudaine du montant des aides fédérales reçues par environ 4000 personnes affectées d'handicaps. À la suite de cette demande elle s'était vue opposer une fin de non-recevoir au motif que la méthode prédictive utilisée pour déterminer les aides était l'objet d'une protection au titre du secret des affaires. Face à ce refus, un recours collectif (« class action ») a été initié par l'ACLU contre le programme d'assurance Medicaid de l'état d'Idaho. La Cour fédérale de l'état d'Idaho a dans ce cas finalement donné raison à l'ACLU, imposant de rendre publique la méthode de calcul des aides. Une analyse du procédé de décision, tant par les experts mandatés par l'ACLU que par la Cour, a pu ainsi montrer que le modèle prédictif reposait sur des données erronées (le programme utilisait notamment un historique incomplet et entaché d'erreurs pour prédire les besoins à venir des individus). Cette procédure devrait se conclure par le développement d'une nouvelle méthode, transparente cette fois, de calcul des aides.[95]

B. Entre secret des affaires et droit d'accès aux modèles, quelle articulation ?

Ces quelques cas récents illustrent les difficultés pratiques à faire valoir les droits des personnes face à un traitement prédictif. Ils soulignent aussi l'absence de relation d'ordre clairement établie entre droit des personnes au contrôle de leurs données et le secret. En Europe, l'absence d'une définition claire du secret des affaires et de sa protection participait de cette ambiguïté. L'adoption de la directive communautaire (UE) 2016/943 du 8 juin 2016 vient remédier, en partie au moins, à cette lacune. Tout en proposant une

94 - *Ibid.* point 774.

95 - K.W. v. Armstrong, class action, aff. 1:12-cv-00022-BLW (28 mars 2016). L'ensemble des documents relatifs à la procédure sont disponibles au lien suivant : [https://www.acluidaho.org/en/cases/kw-v-armstrong].

harmonisation de la protection du secret des affaires, le texte inclut également des références à la directive 95/46/CE, notamment quant aux droits d'accès aux données à caractère personnel soumises à un traitement. Parallèlement, le Règlement mentionne explicitement que le droit d'accès « ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle ». [96] Il est donc légitime de se demander si ces textes apportent un nouvel éclairage sur l'articulation entre droit des personnes et secret des affaires et permettent de dépasser l'aporie.

La directive communautaire (UE) 2016/943 du 8 juin 2016 relative à la « protection des secrets d'affaires contre l'obtention, l'utilisation et la divulgation illicites »[97] (ci-après, « la Directive »), dont la transposition en droit national devra être effectuée avant le 9 juin 2018, vise à protéger les entreprises contre l'espionnage économique et industriel. En demandant aux Etats membres d'harmoniser leurs législations en y inscrivant des « mesures, procédures et réparations » afin « d'empêcher l'obtention, l'utilisation ou la divulgation illicites d'un secret d'affaires ou d'obtenir réparation pour un tel fait »[98], elle permet aux victimes de demander réparation devant les tribunaux en cas de vol d'informations confidentielles telles que les innovations technologiques. Selon la Directive, le secret d'affaires est défini comme l'ensemble des informations confidentielles dont la divulgation cause un préjudice à leur détenteur légitime. L'utilisation du qualificatif générique d'« information » n'impose aucune restriction sur la nature de l'objet à protéger : données numériques, structures de données, et autres artefacts technologiques, y compris les algorithmes d'apprentissage et les modèles prédictifs qui en sont déduits, entreront donc dans le champ de protection de la directive. Le respect des droits fondamentaux est explicitement mentionné dans la directive. Elle « observe les principes reconnus notamment par la Charte, en particulier le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel.»[99] Les considérants indiquent par ailleurs que la Directive

96 - Règlement (UE) 2016/679, Considérant 63.

97 - JOUE L157, 15 juin 2016 ([http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32016L0943]).

98 - *Ibid.* art. 4 § 1.

99 - Directive (UE) 2016/943, Considérant 34.

« ne devrait pas avoir d'incidence sur les droits et obligations fixés par la directive 95/46/CE, notamment le droit de la personne concernée d'accéder aux données à caractère personnel la concernant qui font l'objet d'un traitement. »[100]

D'autre part, le Règlement, dans ses considérants, souligne que, bien que « toute personne concernée devrait avoir le droit de connaître et de se faire communiquer, en particulier, les finalités du traitement des données à caractère personnel, [...], la logique qui sous-tend leur éventuel traitement automatisé et les conséquences que ce traitement pourrait avoir, au moins en cas de profilage », pourtant ce droit « ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. » Le même considérant poursuit cependant en précisant que « ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée. » [101] L'article article 23 §1(i) du Règlement dispose par ailleurs que les obligations auxquelles doit se soumettre le responsable du traitement , y compris le droit d'accès à la logique sous-tendant le traitement des données, peuvent être limitées, « lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir [...] la protection de la personne concernée ou des droits et libertés d'autrui. » (y compris les droits de propriété intellectuelle sur les procédés de traitement automatisés).

Les deux textes se renvoient donc dos-à-dos en s'accordant sur le respect mutuel de leurs principes directeurs. D'une part, l'application de la Directive devrait respecter le droit des personnes au contrôle des données personnelles. D'autre part, le Règlement ne doit pas contrevenir au secret des affaires. Que déduire de ce croisement de références dans le contexte du droit d'accès à la logique du traitement des données ?

Bien que la Directive spécifie que la protection du secret ne devrait pas s'opposer au « droit de la personne concernée d'accéder aux

100 - *Ibid.* Considérant 35.

101 - Règlement (UE) 2016/679, Considérant 63.

données à caractère personnel la concernant qui font l'objet d'un traitement et le droit d'obtenir la rectification, l'effacement ou le verrouillage de ces données lorsqu'elles sont incomplètes ou inexactes »[102], aucune mention n'est faite du droit d'accès à la logique du traitement, pourtant déjà présent à l'article 12(a) de la directive 95/96 CE aux côtés du droit d'accès aux données (art. 12(a)) et du droit de rectification (art. 12(b)). Ceci est d'autant plus notable que cette « logique sous-jacente » est ici, comme on l'a vu, l'objet même de la protection par le secret des affaires. En effet, si l'effacement, la rectification des données elles-mêmes ne semble poser de véritable problème au regard du secret (sauf à considérer que lesdites données fassent partie du secret d'affaire, comme semblait l'avancer Facebook dans sa communication à Max Schrems[103]), en revanche l'accès aux principes de fonctionnement même du traitement remettra en question la protection par le secret. En effet, à la différence des autres droits de propriété intellectuelle, le titulaire d'un secret d'affaire ne détient pas de droit exclusif sur les informations qui y sont liées et la protection du secret prend fin dès qu'il est divulgué. Ainsi, bien que le secret puisse « apporter quelque sécurité à celui qui veut s'en entourer, [il] ne confère aucun pouvoir juridique de se réserver *erga omnes* l'information en cause ».[104] On comprend donc la réticence à inclure dans Directive une quelconque prévalence du droit d'accès à la logique du traitement.

Le Règlement laisse également ouverte la question du droit d'accès à la logique face au secret des affaires. Comment comprendre la nécessité de respecter à la fois le secret des affaires et le fait de ne « pas refuser toute communication d'informations à la personne concernée »[105] ? Les recommandations du groupe de travail de l'article 29 adressent directement cette question : « Le considérant 63 accorde une certaine protection au responsable du traitement préoccupé par la révélation éventuelle de secrets d'affaires ou d'objets de propriété intellectuelle, situation particulièrement

102 - Directive (UE) 2016/943, Considérant 35.

103 - *Supra*, not. n° 87.

104 - J. Huet, « Le reverse engineering, ou ingénierie inverse, et l'accès aux interfaces dans la protection des logiciels en Europe : questions de droit d'auteur et de droit de la concurrence », *Recueil Dalloz*, 1990, p. 99.

105 - Règlement (UE) 2016/679, Considérant 63.

pertinente dans le contexte du profilage. Il énonce que le droit d'accès « ne devrait pas porter atteinte aux droits ou libertés d'autrui » Cependant, c'est seulement dans des circonstances exceptionnelles que ces droits devraient prévaloir sur le droit d'accès des individus ; les responsables du traitement ne devraient pas trouver là une excuse pour refuser de fournir toute information aux personnes concernées. Ces droits devraient être considérés de manière contextuelle et pondérés au regard du droit d'accès des individus à l'information ».[106] (nous soulignons). Face à une possible systématisation du recours au secret qui justifierait un déni d'accès à la logique du traitement, la position du groupe de travail souligne, judicieusement, la nécessité d'opposer des garde-fous, ou tout du moins de rechercher un équilibre. Il reste cependant que les recommandations n'apporte pas davantage de précisions quant à la nature des informations à fournir. En l'absence de critère de priorité explicite, il semble donc que la responsabilité doive incomber au juge du fond de se livrer, au cas par cas, à une appréciation concrète et objective pour circonscrire l'accès à l'information et concilier au mieux les deux principes.

Dans ce contexte, le recours à des experts, spécialistes de l'algorithmique, semble une condition préalable en cas de litige pour assurer l'examen des procédés de décision automatique et permettre d'analyser les circonstances dans lesquelles une décision (spécifique) a pu être obtenue, ou si les conditions légales de protection des données personnelles et de finalité du traitement ont été suivies.[107] L'article 9 de la Directive concerne la protection du caractère confidentiel des secrets d'affaires au cours des procédures judiciaires. Il y est précisé que « [l]es États membres veillent à ce que les parties, leurs avocats ou autres représentants, le personnel judiciaire, les témoins, les experts et toute autre personne participant à une procédure judiciaire relative à l'obtention, l'utilisation ou la divulgation illicite d'un secret d'affaires, ou ayant accès à des documents faisant partie d'une telle procédure, ne soient pas autorisés à utiliser ou divulguer un secret d'affaires » (art. 9 §1). Les autorités doivent ainsi « prendre les mesures particulières nécessaires pour protéger le caractère

106 - *Supra* not. n° 43, section IV.D.2 (Notre traduction).

107 - Dans ce sens : A. Tutt, « An FDA for Algorithms », *Administrative Law Review*, vol. 67, 2016, p. 1.

confidentiel de tout secret d'affaires » (art. 9 §2). Dans ce cadre, dans la mesure où des experts assermentés sont susceptibles de saisir la nature de tels objets techniques et les conditions de leur évaluation dans le maintien des règles de confidentialité, il ne semble aucunement justifiable d'interdire tout accès aux algorithmes sans dénier au juge la possibilité de décider de la licéité de leur usage. Un rapport récent du Conseil de l'Europe invite à cette fin les responsables du traitement à fournir, dans le cadre d'une « analyse d'impact » du traitement (art. 35 du Règlement) à « communiquer toute information confidentielle éventuelle dans une annexe séparée du rapport d'évaluation, laquelle ne doit pas être rendue publique, mais pourrait être consultée par les autorités de contrôle ».[108] Il reste cependant que la nature des modèles statistiques qui prévalent à ce jour (au premier rang desquels les réseaux de neurones profonds) ne permettra pas, dans la vaste majorité des situations, d'accéder à une logique interprétable. Comme nous l'avons vu précédemment, la construction d'une décision particulière se forme dans un espace paramétrique qui échappe à une transcription intelligible. L'analyse des programmes informatiques dans lesquels sont exprimés les algorithmes de constructions de ces modèles, s'ils sont eux accessibles au regard critique des experts, n'apportera dans ce cas qu'une information secondaire, ne permettant au mieux de s'assurer que les codes de bonnes pratiques ont été suivis mais sans apporter un éclairage direct sur le processus de traitement des données exprimé dans le modèle statistique lui-même.

La volonté de transparence annoncée dans le Règlement européen, au moins dans sa dimension explicative, se heurte donc à plusieurs obstacles : d'une part, l'opacité intrinsèque des nouvelles générations d'algorithmes prédictifs basés sur un apprentissage statistique, irréductibles à toute interprétation. D'autre part la protection par le secret des affaires de ces mêmes objets techniques rend, au mieux, incertain l'accès à leur logique et pourrait offrir un moyen de contourner les obligations d'information et d'accès. Faut-il alors sonner le glas du principe de transparence ? Ou est-ce là l'occasion de revenir à la fonction de ce principe et aux moyens pratiques d'en délinéer les modalités d'application ?

108 - Rapport du Conseil de l'Europe, *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, T-PD(2017)01, 23 jan. 2017, p. 1.

Section III – Au delà du principe de transparence, vers un principe de responsabilité

§1 : Face à la volatilité des développements techniques, le recours au droit souple

Confrontée aux conséquences négatives attribuables aux procédés d'apprentissage statistique, notamment en termes de discriminations,[109] une partie de la communauté scientifique a pris conscience de la nécessité de développer des outils techniques afin d'en prévenir les biais.[110] Cet engagement s'est notamment manifesté par des tentatives d'interprétation dans un langage humainement compréhensible de ces « boites noires » que constituent les dernières générations de processus algorithmiques.[111] Malgré des avancées importantes, ce champ de recherche n'en est qu'à ses balbutiements et les procédés de traduction qu'il propose n'offrent aujourd'hui que des options d'interprétation bien approximatives. Devant la complexité de ces modèles, dont les réseaux de neurones profonds sont l'exemple emblématique, le principe de transparence algorithmique se réduit donc comme peau de chagrin. Qu'en reste-t-il ? Une notion d'explication « générique » (puisque, nous l'avons

109 - On a ainsi vu surgir des algorithmes qualifiés de « racistes », non seulement dans la cas de l'outil COMPAS déjà évoqué ci-avant dans l'affaire Loomis (v. J. Larson et al., « How We Analyzed the COMPAS Recidivism Algorithm », *ProPublica*, 23 Mai 2016, [https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm]) mais aussi au travers de « tchatbots » relayant et amplifiant les biais présents dans les données utilisées pour son entrainement (M. Garcia, « Racist in the Machine The Disturbing Implications of Algorithmic Bias », *World Policy Journal*, vol. 33, n° 4, 2016, p. 111).

110 - C. Sandvig et al., «Auditing algorithms: Research methods for detecting discrimination on Internet platforms, Data and discrimination: converting critical concerns into productive inquiry », *in 64th Annual Meeting of the International Communication Association*, Seattle, WA, USA, 22 mai 2014 ; S. Hajian, F. Bonchi et C. Castillo, « Algorithmic bias: from discrimination discovery to fairness-aware data mining » *in : Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, p. 2125-2126.

111 - Il pourra s'agir d'une approximation des modèles dans des structures décisionnelles intelligibles (tels que des arbres de décision, ou encore certains modèles graphiques) soit de l'identification de cas emblématiques permettant de proposer un schéma explicatif du fonctionnement des processus décisionnels au travers d'exemples caractéristiques. A. Datta, S. Sen et Y. Zick, « Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems », *2016 I.E. Symposium on Security and Privacy,* 2016, p. 598 ; M. T. Ribeiro, S. Singh et C. Guestrin, « Model-Agnostic Interpretability of Machine Learning », arXiv preprint n° 1606.05386, 2016.

vu, il ne s'agit pas de rendre compte du comportement du modèle prédictif dans des cas particuliers), « sans nécessairement toujours rechercher une explication complexe de l'algorithme utilisé ou un dévoilement de l'algorithme dans son entièreté »[112], nous rappelle le groupe de travail de l'article 29 (et en effet, comment imposer à chacun de comprendre les derniers développements de l'apprentissage profond, les dernières subtilités des algorithmes d'optimisation ?). Mais bien qu'il soit certainement toujours possible de décrire dans ses grandes lignes un système algorithmique, si le principe de transparence mis en avant dans le Règlement se borne en pratique à une telle dimension « descriptive », « approximative », le risque sera alors grand qu'il ne se réduise qu'à un faux semblant, une illusion de transparence dénuée de tout effet juridique. Pire encore, s'il suffit d'invoquer le secret des affaires pour le maintenir dans l'ombre, il pourrait bien servir de paravent, d'écran algorithmique, derrière lequel maintenir l'opacité de ses utilisations et avec, la responsabilité de ses opérateurs.

On ne saurait pour autant abandonner *en bloc* tout principe de transparence. Cependant, les limites imposées par l'intermédiation de filtres décisionnels opaques imposent d'en délinéer à nouveau, dans ce contexte particulier, les contours. Plutôt qu'un renoncement à un principe essentiel de bonne gouvernance, c'est donc là une opportunité d'en préciser non seulement le périmètre d'application mais également les moyens de sa mise en œuvre effective. Car si le principe peut être conçu comme une limite asymptotique (nécessairement médiée, filtrée, sujette à interprétation, soumise à contraintes), c'est par ailleurs une notion composite faite, Jean-François Kerléo le rappelle, d'une « multiplicité des buts réunis au sein d'un même usage (contrôle, probité, légitimation, etc.) ».[113] Cette multi-dimensionnalité du principe de transparence lui accorde la flexibilité nécessaire qui permet, par un ajustement de ses articulations internes (et, en quelque sorte, de la pondération relative de ses différentes composantes), de l'adapter à de nouveaux objets. Et, en effet, si la mécanique de décision inscrite au sein du modèle d'inférence échappe en tant que telle à l'interprétation, d'autres étapes significatives du

112 - Notre traduction. *Supra* note n° 43.

113 - J.-F. Kerléo, « La transparence de la vie publique en droit, Sens-Dessous », n° 20, 2017, p. 15.

traitement automatique des données personnelles restent quant à elles directement accessibles et promptes à en éclairer le processus décisionnel (au premier rang desquelles, la finalité du traitement et les modalités pratiques de sa mise en œuvre). Le principe de transparence, ineffectif à rendre compte des raisons d'une décision particulière issue d'un modèle statistique, ininterprétable, est ainsi applicable à d'autres composantes de la chaîne de décision. Au delà, et plus généralement, il doit rester un principe directeur de l'ensemble de la procédure. De fait, si une fonction du principe de transparence vise à « la transmission d'un certain nombre d'informations objectives destinées à aider le citoyen dans son choix »,[114] dans une interprétation plus large il désigne « une logique de fonctionnement à laquelle les organisations devraient idéalement toujours se plier. D'un point de vue descriptif, la transparence recouvre ainsi la traçabilité interne du fonctionnement des organisations ».[115] Il faut donc dépasser la seule dimension explicative de la notion de transparence – qui n'en constitue qu'une seule de ses dimensions – et revenir à la fonction de ce principe consistant à promouvoir et engager la responsabilité de l'ensemble des acteurs du traitement des données personnelles. Il est aussi nécessaire, à cette même fin, d'identifier les moyens pratiques de son exercice.

Dans ce contexte, force est de constater que la rapidité d'évolution et la volatilité du paysage technologique, en particulier dans le domaine du traitement algorithmique de l'information, sont telles qu'un cadre législatif, soit trop limitatif (sur le plan technique), soit trop rigide (dans son inaptitude à s'adapter à ces nouveaux intermédiaires techniques), s'expose à une obsolescence rapide. Sans revêtir les caractères obligatoires et contraignants du droit positif, les « *soft laws* » (droits « souples ») offrent en revanche un ensemble d'instruments normatifs, qui permettent d'encadrer les pratiques et les comportements tout en conservant un degré de flexibilité qui lui permet de s'adapter et de suivre les derniers développements techniques. Le Règlement laisse une place importante à de tels outils qui s'inscrivent directement dans le cadre d'une mise en œuvre du principe de responsabilité.

114 - J. Pitseys, « Le concept de gouvernance », *Revue interdisciplinaire d'études juridiques*, vol. 65, n° 2, 2010, p. 207.

115 - *Ibid.*

Parmi ces instruments, le Règlement encourage ainsi la mise en place de codes de conduite. L'initiative est laissée aux « associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants » d'élaborer, de modifier ou de proroger (après avis positif de l'autorité de contrôle) de tels codes « aux fins de préciser les modalités d'application du présent règlement » (Article 40 §1 ; voir également le considérants 77 et 98). L'article 40 §2 énumère un ensemble, non exhaustif, de principes auxquels pourraient s'appliquer de tels codes de conduite, y compris « le traitement loyal et transparent » des données (art. 40 §2(a)). Ces codes, outre leur fonction de définition qui leur permettra de servir de guide lors de la phase de développement des procédés automatiques, pourra servir plus tard, dans une phase de suivi, « au contrôle obligatoire du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer » (art. 40 §4). Parmi ses recommandations de « bonnes pratiques », le groupe de travail de l'article 29, suggère ainsi dans le contexte de l'article 22, la mise en place de procédures d'évaluation (dans le sens de procédures d'audit) afin de « tester les algorithmes utilisés et développés par apprentissage automatique, pour démontrer qu'ils se comportent bien comme escompté et ne conduisent pas à des résultats discriminatoires, erronés ou injustifiés».[116] Le groupe propose de considérer les « codes de conduite pour l'évaluation des procédés impliquant un apprentissage automatique ».[117]

Autre balise proposée par le Règlement, le développement de procédures d'analyse d'impact : « 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 » (art. 35 §1). Dans un tel cas, le responsable du traitement a pour obligation d'effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Cette précaution est en particulier requise dans le cas d'un traitement automatisé au sens de l'article 22. Dans le cas des procédés d'apprentissage statistique, la mise en œuvre de telles analyses nécessitera la validation du corpus

116 - *Ibid.* Annexe 1. (notre traduction).

117 - *Ibid.*

d'entrainement sur lequel se base le modèle d'inférence. C'est en effet là que les biais statistiques déjà présents dans les échantillons utilisés lors de l'apprentissage, seront transférés dans les profils prédits par le modèle et conduiront à une éventuelle propagation des discriminations. Ces approches peuvent être menées en amont de l'apprentissage, dans une phase de prétraitement des données pour y détecter la présence de biais statistiques[118], mais aussi lors de l'apprentissage, pour identifier l'émergence de discriminations.[119] Elles peuvent enfin s'appliquer dans une phase de validation post-traitement pour évaluer le modèle une fois son entrainement achevé.[120] Ces procédures, s'avèrent en particulier nécessaires lorsque des analyses statistiques ont pour vocation de déduire des traits personnels (composantes qui, bien qu'elles puissent donner lieu à des estimations d'ensemble, restent, au plan des prédictions individuelles, éminemment arbitraires) et devraient s'intégrer dans le cahier des charges des responsables du traitement des données avant la mise en ligne de toute application.

Des associations professionnelles telles que *l'Institute of Electrical and Electronics Engineers* (IEEE) ont récemment approuvé plusieurs projets de normes répondant à ces impératifs. Parmi elles, notamment, la norme IEEE P7003™ relative aux « methodologies and processes to help certify the elimination of negative bias in the creation of algorithms » se propose de donner priorité aux principes de responsabilité (« *accountability* ») pour, en particulier, « réduire l'impact des discriminations et encourager la neutralité et l'équité pour les technologies futures ».[121] Selon son directeur, Ansgar Koene, il s'agit avec une telle norme de fournir un cadre dans lequel il sera possible de démontrer « que les algorithmes sont développés et utilisés sans générer aucun biais négatif pour les individus ou groupes d'individus », en particulier en ce qui concerne les données sensibles

118 - F. Kamiran, et T. Calders, «Data preprocessing techniques for classification without discrimination», *Knowledge and Information Systems*, vol. 33, n° 1, 2012, p. 1. Voir aussi, dans le même sens : M. Feldman et al., « Certifying and removing disparate impact », *KDD*, 2015, p. 259.

119 - R. Zemel et al., «Learning fair representations », *ICML*, 2013, p. 325 ; M.B. Zafar et al., « Fairness Constraints: A Mechanism for Fair Classification », *2nd Workshop on Fairness, Accountability, and Transparency in Machine Learning*, 2015.

120 - S. Hajian, et al., « Discrimination-and privacy-aware patterns », *Data Mining and Knowledge Discovery*, vol. 29, n° 6, 2015, p. 1733.

121 - (Notre traduction) [http://standards.ieee.org/news/2017/ieee_p7003.html].

telles que l'origine ethnique, le genre, les orientations sexuelles.[122] Dans le même sens, le conseil de *l'Association for Computing Machinery* (ACM) a publié en janvier 2017 une déclaration sur l'« Algorithmic Transparency and Accountability » incluant sept grands principes que les créateurs d'algorithmes devraient suivre afin de tenir compte et d'éviter les effets discriminatoires pouvant être dus à l'utilisation de procédés de traitement automatique des données.[123] En France, la mise en place d'une « plateforme scientifique collaborative destinée à favoriser, d'une part le développement d'outils logiciels et de méthodes de tests d'algorithmes « responsables et transparents », et d'autre part la promotion de leur utilisation » fait partie des recommandations du rapport « Modalités de régulation des algorithmes de traitement des contenus » publié en décembre 2016 par le Conseil Général de l'Economie.[124] L'INRIA s'est proposée pour mener le développement d'une telle plateforme (« TransAlgo »), avec pour fonction de contribuer à développer « une culture et un savoir-faire pour une production, une analyse algorithmique et une valorisation des données responsables et éthiques. TransAlgo aidera aussi à diffuser les bonnes pratiques auprès des services de l'Etat, des industriels et des citoyens. »[125]

Ces premières approches pourront ainsi servir de fondement à la mise en forme de certifications, autre mécanisme de droit souple appuyé par le Règlement. L'article 42 § 1 dispose en ce sens que « [l]es États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. » Des organismes de certification se sont d'ores et déjà engagés dans la définition de normes pour certains des aspects relatifs à la protection des données personnelles tels que définis à l'article 25 § 1 du

122 - *Ibid.* (Notre traduction).

123 - [http://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf].

124 - Rapport de I. Pavel et J. Seris, *Modalités de régulation des algorithmes de traitement des contenus, Conseil général de l'économie, de l'industrie, de l'énergie et des technologies,* 13 mai 2016.

125 - [https://www.economie.gouv.fr/files/files/PDF/Inria_Plateforme_TransAlgo2016-12vf.pdf].

Règlement. Les dispositions de l'article 25 imposent au responsable du traitement l'implémentation du principe de « protection des données par défaut » (« *privacy by design* »), à savoir l'application de « mesures techniques et organisationnelles appropriées, telles que la pseudonymisation », afin de protéger les données personnelles. Or la mise en application pratique de ces mesures est laissée à la libre décision du responsable du traitement.[126] En l'absence de recommandations claires sur les modalités d'implémentation des principes de « protection des données par défaut », le risque est grand (et avéré, d'ailleurs, au vu des nombreux incidents concernant les atteintes à la vie privée des individus, dont Google, Facebook, AOL, Twitter, Microsoft, etc. ont été l'objet[127]) que leur mise en œuvre ne remplisse qu'imparfaitement les conditions de l'article 25 §1. Un ensemble de normes techniques relatives à la protection des données personnelles proposées par l'organisation internationale de normalisation ISO, notamment un « cadre privé » (ISO/IEC 29100) et un code de bonnes pratiques (ISO/IEC 27018) pourraient néanmoins servir de guide en la matière. En particulier, la norme ISO/IEC AWI 20889, en cours de développement, aura vocation à proposer un jeu de techniques d'anonymisation éprouvées, dans la lignée de celles prévues par les dispositions de l'article 25 du Règlement.[128]

126 - Alors même qu'un fondement clair au concept de « privacy by design » fait défaut : des scientifiques et informaticiens européens ont d'ailleurs noté le recours fréquent à des définitions récursives : « *privacy by design means applying privacy by design* » qui ne permettent pas de déterminer « *neither what exactly this 'privacy matter' is, nor how it can be translated into design*.» (S. Gürses, C. Troncoso et C. Diaz, « Engineering privacy by design », *Computers, Privacy & Data Protection*, vol. 14, n° 3, 2011, p. 1). Pour des exemples d'applications de ce principe : R.J. Bayardo et R. Agrawal, « Data privacy through optimal k-anonymization », *21st International conference on data engineering (ICDE'05)*, 2005, p. 217 ; M. Mun, et al., « Personal data vaults: a locus of control for personal data streams », *Proceedings of the 6th International ACM Conference*, 2010, p. 17.

127 - I. S. Rubinstein et N. Good, « Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents », *Berkeley Tech. Law Journal*, vol. 28, n° 2, 2013, p. 1333.

128 - Les techniques d'anonymisation ou de « dé-identification » des données consistent à empêcher (autant que possible) leur lien avec un individu donné. Les normes ISO/IEC AWI 20889 (« Privacy enhancing data de-identification techniques », 29 sept. 2015), ISO/IEC 29100 (« Cadre privé », 5 dec. 2011), ISO/IEC 27018 (« Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII », 29 juil. 2014) sont disponibles sur le site http://iso.org/.

§2 : Quelques considérations pratiques de mise en œuvre du principe de responsabilité algorithmique

La référence au principe de responsabilité est mentionnée explicitement dans le Règlement. L'article 5 §2 dispose en ce sens que « [l]e responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (*responsabilité*). » Nous soulignons : il est notable en effet que dans la version anglaise du texte, « responsabilité » corresponde à « *accountability* », notion à géométrie variable,[129] sans équivalent strict en français mais qui sous-tend à la fois l'exigence d'un respect de certaines règles, et la possibilité d'une sanction pour manque de respect de ces règles. Il s'agit au fond de l'expression d'une capacité à pouvoir « rendre des comptes ». Les nouvelles mesures introduites par le Règlement, telles que l'obligation d'une protection des données personnelles (art. 25), mais aussi de certification (art. 42) et d'analyse d'impact (art. 35), évoquées précédemment, sont autant d'expressions de ce principe. Clef de voûte du principe de « responsabilité/*accountability* », la nécessité d'une « démonstration » du respect des règles s'articule en pratique autour d'une notion essentielle, celle de traçabilité des processus. La mise en œuvre de cette notion repose sur un effort systématique, précis, d'enregistrement et d'archivage de l'ensemble des étapes du traitement automatisé sur lesquelles se fondent les décisions.

Les nouvelles dispositions du Règlement vont partiellement dans ce sens, en imposant au responsable du traitement de maintenir un registre des opérations menées sur les données personnelles (v. article 30). Ces dispositions paraissent d'abord dirigées vers une responsabilisation accrue des acteurs et une meilleure traçabilité des données et de leur utilisation (le registre devant en effet contenir les informations relatives à la finalité du traitement, mais aussi aux destinataires des données ainsi qu'au transfert vers des pays tiers). Or, il serait judicieux et prudent d'ajouter un archivage des modèles eux-mêmes ainsi que des données ayant permis leur construction. Conserver une archive du corpus d'entraînement, des

129 - Pour Richard Mulgan, c'est « un terme général pour qualifier tout mécanisme qui oblige une institution à rendre des comptes au public auquel elle s'adresse. » (Notre traduction) R. Mulgan, *Holding Power to Account: Accountability in Modern Democracies*, Palgrave Macmillan UK, 2003, p. 19).

caractéristiques utilisées pour décrire ces données, des paramètres d'entraînement du système, contribuerait ainsi largement à la possibilité d'un audit et à l'analyse *a posteriori* du processus de traitement. Encourager les efforts d'interprétation des modèles pourrait servir autant les intérêts des utilisateurs que ceux des concepteurs de tels systèmes.[130] Il est à regretter que la nécessité de conservation d'une telle archive soit cependant limitée aux entreprises de plus de 250 employés, « sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données [sensibles] » (art. 30 §5). La pratique mériterait en effet d'être étendue, ou systématisée, simplement pour se prémunir des cas où l'impact du traitement aurait été sous-évalué en phase de développement.

La question se pose toutefois des moyens d'archivage qui permettront d'assurer un audit effectif. Une approche basée sur les technologies de registres distribués (« *distributed ledger technologies* ») dont font partie les techniques de type « *blockchain* », pourrait permettre d'encoder de manière irréversible (évitant ainsi toute fraude) et vérifiable (lors d'une phase d'audit par exemple), l'ensemble des opérations de sélection des données, de leur prétraitement mais aussi des choix (paramètres, architectures, fonctions d'utilité) ayant déterminé l'entrainement d'un modèle prédictif particulier. Sans nécessairement chercher à expliquer les décisions du modèle final, un tel « instantané » de l'état du système à chaque étape de la phase d'apprentissage pourrait permettre d'en reproduire la construction et d'enquêter sur son fonctionnement en cas d'audit ou de litige. Bien que la force probante des *blockchains* reste cependant encore à définir,[131] elle pourrait se rapprocher, sous certaines conditions, des caractéristiques de la signature électronique et permettre ce faisant

130 - Dans ce sens : « *Understanding why machine learning models behave the way they do empowers both system designers and end-users in many ways: in model selection, feature engineering, in order to trust and act upon the predictions, and in more intuitive user interfaces.* » (M.T. Ribeiro, S. Singh et C. Guestrin, « Model-Agnostic Interpretability of Machine Learning », arXiv preprint n° 1606.05386, 2016).

131 - C. Zolinsky, « Fintech - Blockchain et smart contracts : premiers regards sur une technologie disruptive », *Revue de Droit bancaire et financier,* n° 1, dossier 4, n° 21, jan. 2017 ; D. Legeais, *JuriClasseur Commercial Fasc. 534 : BLOCKCHAIN,* Date du fascicule : 7 Mars 2017. Date de la dernière mise à jour : 7 Mars 2017.

l'établissement d'actes authentiques.[132] Il serait ainsi envisageable de développer un système apparenté aux cahiers de laboratoire dans lesquels les chercheurs inscrivent les étapes d'un processus expérimental,[133] ou, aux Etats-Unis, des « cahiers d'invention ».[134] Le registre contiendrait ainsi, dans un format sécurisé, l'ensemble des séquences nécessaires à la reproduction du modèle. Des prototypes ont d'ailleurs déjà été élaborés dans ce but, soit dans un contexte général de l'enregistrement d'un processus de laboratoire,[135] soit dans les conditions plus spécifiques à l'apprentissage machine.[136]

Outre l'archivage, prérequis à la démonstration du suivi des règles ou des codes de conduite, le principe d'« *accountability* » doit s'accompagner de mécanismes de contrôle et de vérification. L'article 41 du Règlement concerne ainsi le suivi des codes de conduite approuvés et dispose que « le contrôle du respect du code de conduite en vertu de l'article 40 peut être effectué par un organisme qui dispose d'un niveau d'expertise approprié au regard de l'objet du code et qui est agréé à cette fin par l'autorité de contrôle compétente. » Il est de la responsabilité de ce même organisme d'établir des procédures qui lui permettront « d'apprécier si les responsables du traitement et les sous-traitants concernés satisfont aux conditions pour appliquer le code, de contrôler le respect de ses dispositions et d'examiner

132 - La signature électronique consiste « en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. » (C. civ. 1304 §2). L'article 1316-1 dispose en outre que « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

133 - A. Amiard et al., « Le cahier de laboratoire électronique (CLE) », *STP Pharma Pratiques*, vol. 21, n° 6, 2011, p. 475.

134 - Registre nécessaire dans le contexte de l'attribution de l'invention au « premier à inventer » (« *first to invent* »), dans lequel la date de protection correspond à la date de conception (système utilisé aux Etats-Unis pour les demandes déposées avant le 16 mars 2013. Le système actuel est à présent, comme en Europe, celui du « premier déposant »). C. J. Garascia, « Evidence of Conception in US Patent Interference Practice: Proving Who is the First and True Inventor », *U. Det. Mercy L. Rev.*, 73, p.717, 1995 ; J.T. Nickla et M.B. Boehm, « Proper laboratory notebook practices: protecting your intellectual property », *Journal of neuroimmune pharmacology*, vol. 6, n° 1, 2011, p. 4.

135 - J. Moehrke, « Blockchain and Smart-Contracts applied to Evidence Notebook, » *Healthcare exchange standards*, 29 Août 2016, [https://healthcaresecprivacy.blogspot.nl/2016/08/blockchain-and-smart-contracts-applied.html].

136 - M. Galtier, Mathieu et C. Marini, « Morpheo: Traceable Machine Learning on Hidden data », arXiv preprint n° 1704.05017, 2017.

périodiquement son fonctionnement » (art. 41 §2(b)). Par ailleurs, l'article 58 §1(f) accorde aux autorités de contrôle le pouvoir de « mener des enquêtes sous la forme d'audits sur la protection des données ». Face à la complexité des systèmes de décision automatisés, le développement de corps d'experts spécialisés dans les domaines de l'algorithmique[137] semble une condition préalable pour réaliser les fonctions de suivi et d'audit inscrites dans le Règlement.

Conclusion et perspectives

Le principe de transparence, valeur fondamentale de gouvernance des démocraties modernes,—tient une place centrale dans le Règlement et dans la loi pour une République numérique.[138] Notion plurielle, elle y exprime autant la nécessité d'informer les personnes concernées des finalités du traitement que de donner accès à la logique des décisions prises à leur endroit, en particulier lorsqu'elles sont le fait de processus automatisés. Or, cette seconde dimension, explicative, achoppe face au développement récent d'outils de traitement de l'information reposant sur des méthodes statistiques dites « d'apprentissage ». Les caractéristiques techniques de ces approches – qui forment aujourd'hui le principe actif d'une économie de l'information et des données personnelles en pleine croissance – obligent, de fait, à remettre en question l'effectivité de ce principe. Ces nouveaux procédés, en reposant sur un apprentissage automatique, ne nécessitent plus en effet l'expression *ab initio* par un opérateur humain des règles de décision qu'ils mettent en œuvre. Ces règles, induites lors de la phase d'apprentissage, sont directement produites par l'algorithme. Elles sont exprimées au sein d'un modèle d'inférence, dans un espace de représentation abstrait qui lui est propre, qui ne se prête pas à une transcription *a posteriori* en un langage simple, humainement interprétable. Les données y sont ainsi décomposées, croisées, pondérées, transformées

137 - En ce sens, v. le rapport de I. Pavel et J. Seris, *Supra* note n° 123 (Recommandation 1, p. 41).

138 - L'article 5 §1(a) du Règlement dispose ainsi que « Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ». L'article 12 traite par ailleurs de la « transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée ». Enfin, le considérant 39 en détaille les différents aspects. V. aussi les articles 49 et 50 de la loi pour une République numérique.

pour conduire *in fine*, après d'innombrables modifications, à une prescription : l'appartenance à un profil individuel ou de groupe, un score ou une catégorie. Des décisions sont alors prises sur des personnes – qu'il s'agisse, par exemple, de décider d'un crédit ou du droit à une allocation, d'une libération conditionnelle ou de la durée d'une peine – sur la base des modèles ainsi élaborés sans que l'on puisse en révéler de manière claire et intelligible les raisons précises de leur émergence. L'application de tels procédés statistiques réduit ainsi à son strict minimum l'application du droit d'accès à la logique sous-jacente aux traitements automatisés qu'ils mettent en œuvre. Au delà de l'impossibilité à interpréter les décisions particulières obtenues au moyen de tels modèles algorithmiques, l'intermédiation d'objets techniques dans la chaîne de traitement des données personnelles est susceptible d'ajouter d'autres freins à la transparence des décisions qui en sont issues. Ces mêmes algorithmes et modèles d'inférence sont en effet le plus souvent l'objet d'une protection au titre de la propriété intellectuelle. Le recours au secret des affaires offre alors un moyen supplémentaire de s'opposer à un accès direct pour les personnes concernées à la « mécanique interne » de ces modèles, alors même qu'elle est le lieu de la décision.

Les limites imposées au principe de transparence par ces nouveaux objets, soit de part leur nature algorithmique, soit du fait de leur protection par le secret des affaires, ne devraient pourtant pas justifier d'en abandonner les fondements. Or, Guy Carcassonne le souligne justement, puisque « la transparence n'est pas une fin en soi », mais « simplement un moyen, comme d'autres et parmi d'autres, d'atteindre les finalités supérieures que porte en elle l'idée démocratique »,[139] il faut, pour en permettre l'expression, dans un contexte technique et juridique en pleine évolution, revenir à la fonction de ce principe. Ainsi, face à l'inintelligibilité intrinsèque des modèles, plutôt que la vaine recherche d'une explication précise des décisions spécifiques, c'est le caractère de responsabilité (dans le sens anglais d'« *accountability* ») du principe qu'il faudra invoquer. Le Règlement s'y réfère directement et offre certains mécanismes, notamment de droit « souple », qui permettraient sa mise en œuvre pratique. Des possibilités techniques d'évaluation des biais inhérents

139 - G. Carcassonne, « Le trouble de la transparence », *Pouvoirs*, vol. 97, 2001, p. 19.

aux procédés d'apprentissage, mais également des outils d'archivage (en particulier des données et des paramètres utilisés lors de la phase d'entraînement) pourraient ainsi aider à son application et contribuer à assurer, *en amont*, lors du développement des modèles, le respect des bonnes pratiques, et offrir *en aval*, lors de leur application, des possibilités de contrôle et d'audit. Cette approche, délibérément pragmatique, aurait pour mérite d'imposer un cadre de construction des procédés de traitement automatique permettant, faute d'un accès à une logique explicite des décisions, l'analyse des conditions mise en œuvre de leur traitement. L'accès à l'information que sous-tend le principe de transparence devra enfin être mis en balance avec les éventuels droits de propriété intellectuelle qui y sont attachés. L'articulation entre l'accès à la logique des outils de décision et le secret des affaires pourra ainsi s'opérer dans le cadre de l'article 9 de la Directive sur le secret. En cas de litige le juge aura alors la possibilité de justifier d'un accès aux informations requises pour qu'il puisse fonder sa décision en connaissance de cause, à savoir dans ce cas aux caractéristiques essentielles du processus de décision (ou, tout au moins, aux archives de déploiement des algorithmes) dans le respect des règles de confidentialité. Jean-Michel Belorgey évoquait ailleurs ce nécessaire équilibre entre transparence et secret, précisant que les deux notions « loin de s'opposer de façon irréconciliable, doivent faire l'objet d'un dosage et d'une articulation. [...] Il revient donc aux politiques et aux juristes de suivre avec attention l'évolution des techniques, de faire preuve à la fois de détermination et d'inventivité ».[140] Gageons qu'il faudra voir en l'émergence de ces objets techniques complexes que sont les algorithmes d'apprentissage et les modèles d'inférence dans le champs du traitement des données personnelles, au delà de la source de nouveaux conflits, l'opportunité d'une telle détermination, d'une telle inventivité.

140 - J.-M. Belorgey, « L'état entre transparence et secret », *Pouvoirs*, vol. 97, 2001, p. 25.

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL APPLIQUÉ AUX ÉTATS TIERS : UNE APPRÉCIATION DE SON CARACTÈRE EXTRATERRITORIAL

Élodie Weil
Doctorante en droit public à l'Université de Cergy-Pontoise
Déléguée à la protection des données au Centre interdépartemental de gestion de la Grande Couronne d'Ile-de-France

La guerre des mots est déclarée par les GAFA à l'égard des autorités européennes de protection des données à caractère personnel. Alors que les secondes cherchent à garantir aux personnes physiques la protection de leurs données à caractère personnel, les premiers ont recours aux termes « extraterritorial » ou encore « mondial », pour qualifier la réglementation européenne[1]. L'actualité illustre le climat tendu entre les autorités de protection des données personnelles et les sociétés, responsables du traitement des données des Européens[2] : il suffit pour s'en convaincre d'observer les réactions

1 - J. Darmanin, « La CNIL rejette le recours de Google contre "un droit à l'oubli mondial" », *Le Figaro*, publié le 21 septembre 2015, disponible sur http://www.lefigaro.fr/secteur/high-tech/2015/09/21/32001-20150921ARTFIG00216-la-cnil-rejette-le-recours-de-google-contre-un-droit-a-l-oubli-mondial.php [consulté en dernier lieu le 22 février 2018] ; Tambou O., « Droit au déréférencement : condamnation symbolique de Google par la CNIL », *Dalloz Actualité*, publié le 13 avril 2016, disponible sur https://www.dalloz-actualite.fr/chronique/droit-au-dereferencement-condamnation-symbolique-de-google-par-cnil#.Wk5IP3kiGUk [consulté en dernier lieu le 22 février 2018].

2 - En plus des sanctions prononcées à l'encontre de Google (voir note précédente), voir les décisions dirigées contre Facebook : O. Tambou, « La CNIL donne une leçon de droit européen à notre ami américain Facebook », *Dalloz Actualité*, publié le 23 février 2016, disponible sur https://www.dalloz-actualite.fr/chronique/cnil-donne-une-lecon-de-droit-europeen-notre-ami-americain-facebook#.Wk5I5nkiGUk [consulté en dernier lieu le 22 février 2018] ; E. Weil, « La CNIL sanctionne Facebook pour de nombreux manquements à la législation française de protection des données à caractère personnel », *Eloveillesurlesdp.fr*, publié le 20 mai 2017, disponible sur http://eloveillesurlesdp.fr/?p=253 [consulté en dernier lieu le 22 février 2018] ; CNIL, Formation restreinte, Délibération prononçant une sanction pécuniaire à l'encontre des sociétés Facebook INC. et Facebook Ireland, n° SAN-2017-006 du 27 avril 2007, disponible sur https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000034728338 [consulté en dernier lieu le 22 février 2018] ; CNIL, Formation restreinte, Délibération prononçant une sanction pécuniaire à l'encontre de la société Google Inc., n° 2016-054 du 10 mars 2016, disponible sur https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032291946 [consulté en dernier lieu le 22 février 2018].

de ces sociétés lorsqu'elles font l'objet de sanctions prononcées par les autorités de protection des données. Google, par exemple, a largement souligné la portée extraterritoriale des sanctions prononcées à son encontre[3]. En 2017, la Cour de Justice de l'Union européenne (ci-après CJUE) a été saisie par le Conseil d'État de plusieurs questions préjudicielles dont l'une portait sur le champ d'application territorial du droit au déréférencement[4]. Le Conseil d'État interrogeait la juridiction européenne pour savoir si le droit au déréférencement devait s'étendre à tous les noms de domaine du moteur de recherche américain. En attendant la réponse de la Cour, l'avocat général dans cette affaire a proposé récemment une approche nuancée du champ d'application territorial applicable au déréférencement[5]. Sans exclure systématiquement un déréférencement global, il suggère que le champ d'application territorial de ce droit fondamental soit mis en balance avec le droit à l'accès à l'information et la liberté d'expression afin d'éviter des atteintes excessives à ces autres droits et surtout d'avertir tout risque de réactions d'autres États qui limiteraient par effet de réciprocité l'accès aux informations des ressortissants européens[6]. Le champ d'application territorial du droit au déréférencement et de manière générale de la réglementation européenne fait donc l'objet de nombreuses inquiétudes.

L'appréhension des situations sur Internet par une approche territoriale semble au premier abord malaisée. Bien que le monde numérique soit difficile à saisir par une règle juridique, tant il donne l'image de s'être affranchi du cadre territorial, il n'est pas déconnecté

3 - J. Lausson, « Google continue de s'opposer à un droit à l'oubli mondial », *Numérama*, publié le 16 novembre 2017, disponible sur https://www.numerama.com/politique/306941-google-continue-de-sopposer-a-un-droit-a-loubli-mondial.html [consulté en dernier lieu le 22 février 2018].

4 - Conseil d'État, 10ème et 9ème Chambres réunies, 19 juillet 2017, n° 399922. Voir également Conseil d'État, 10ème Chambre, 24 février 2017, n° 391000, 393769, 399999, 401258.

5 - Voir les conclusions de l'avocat général M. Szpunar, présentées le 10 janvier 2019 dans la demande de décision préjudicielle formée par le Conseil d'État à l'égard de la CJUE, *Google LLC c. CNIL*, C-507/17, §§58-63.

6 - *Ibid.*

du territoire des États[7]. Dès lors, l'exercice de compétences étatiques dans le monde virtuel et dans le monde réel n'est pas éloigné[8]. Ainsi, pour la Cour de Justice, dans l'affaire *Bodil Lindqvist*, les règles européennes n'ont pas vocation à s'appliquer à tous les États sans qu'un critère de rattachement suffisant le justifie[9].

L'Union européenne a retenu une approche territoriale de sa juridiction en matière de protection des données à caractère personnel, et a au surplus eu recours à des critères de plus en plus extensifs conduisant l'Union à affirmer sa compétence au-delà de ses frontières : ainsi l'article 4 de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoyait que seule la présence d'un établissement ou d'un moyen sur le territoire d'un État membre peut justifier l'application d'une loi

7 - J. L. Goldsmith, « Against Cyberanarchy », *The University of Chicago Law Review,* vol. 65, n° 4, 1998, pp. 1199-1250 ; A. K. Woods, « Against Data Exceptionalism », *Stanford Law Review*, vol. 68, n° 4, p. 734.

8 - *Contra* : D. G. Post, « Against "against Cyberanarchy" », *Berkeley Technology Law Journal*, vol. 17, n°4, 2002, pp. 1365-1388 ; D. J. B. Svantesson, « Against "against Data Exceptionalism" », *Masaryk University Journal of Law and Technology*, vol. 10, n° 2, 2016, pp. 200-211.

9 - CJCE, Décision préjudicielle du 6 novembre 2003, *Bodil Lindqvist*, C-101/01, *Rec.*, I, 2003, p. 12992. Les autorités judiciaires suédoises ont soumis des questions à la Cour dans le cadre d'une procédure pénale poursuivie contre Mme *Lindqvist* laquelle était accusée d'avoir enfreint la législation suédoise en publiant sur son site Internet, accessible partout dans le monde, des données à caractère personnel. Le *Göta hovrätt* a décidé de surseoir à statuer et de soumettre à la Cour la question de savoir si l'insertion de données à caractère personnel à l'aide d'un ordinateur par une personne, présente sur le territoire d'un État membre, sur un site stocké sur un serveur de ce même État membre, de sorte que les données deviennent accessibles partout dans le monde, États tiers compris, constitue un transfert de données vers des pays tiers au sens de l'article 25 de la directive 95/46/CE. La Cour a rappelé que le régime institué par l'article 25 est un régime d'exception. Or, si l'article 25 devait interpréter en ce sens qu'il existe un transfert vers un pays tiers chaque fois que des données à caractère personnel sont chargées sur une page Internet, ce transfert serait nécessairement un transfert vers tous les pays où il y aurait un accès à Internet. Le régime d'exception deviendrait alors un régime d'application générale. En effet, selon la Cour, le régime de l'article 25 de la Directive ne s'applique pas de manière indifférenciée à tous les États ayant les moyens techniques suffisants pour accéder à ces données (§ 69). Dès lors, la Cour répond par la négative à la question posée par la juridiction suédoise.

nationale correspondant à la transposition de la directive[10]. Dès lors, certaines entreprises étrangères ne disposant pas d'établissement sur le territoire d'un État membre pouvaient mener des activités contraires à la réglementation européenne. C'est la raison pour laquelle les autorités européennes ont cherché à étendre le champ d'application territorial des règles contenues dans la directive. En effet, le Groupe de Travail Article 29 (ci-après G29) a retenu une interprétation large de ce qu'il fallait entendre par « moyens » et a reconnu que dans certains cas, « la collecte de données à caractère personnel effectuée via les ordinateurs des utilisateurs, comme par exemple dans le cas des cookies [...] entraînent l'application [...] du droit de l'UE en matière de protection des données »[11]. Le second critère de rattachement à l'application de la directive – l'établissement situé sur le territoire d'un des États membres – a également fait l'objet d'une lecture extensive par le G29, mais aussi par la Cour de Justice de l'Union européenne, dans l'affaire *Weltimmo s. r. o.*[12]. À cet égard, la Cour de justice a tout d'abord précisé que le lieu d'enregistrement du responsable de traitement n'est pas déterminant pour établir

10 - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOCE*, n° L281, p. 31, Article 4 : « 1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque :
a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ; [...]
c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés. [...] ».

11 - Groupe de travail « Article 29 » sur l'application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE, Document de travail du 30 mai 2002, 5035/01/FR/Final, WP 56, p. 9 et p. 24. Le G29 reconnaît toutefois que l'utilisation de ce critère peut avoir des conséquences non satisfaisantes lorsqu'elle aboutit à l'application des règles européennes à des situations où le lien avec l'UE est ténu.

12 - CJUE, 3ème Ch., Arrêt du 1er octobre 2015, *Weltimmo s. r. o.*, C-230/14. En l'espèce, il n'était pas question de déterminer l'application du droit européen, mais d'identifier la loi nationale applicable. En effet, la société en cause avait son siège sur le territoire de l'Union européenne. La question n'était pas tant celle de l'applicabilité de la directive, qui ne faisait aucun doute, que celle de la résolution du conflit de lois nationales (les deux droits internes concurrents étant ceux de deux États membres) et de la détermination de la juridiction compétente. Pour autant, les critères dégagés peuvent également permettre la détermination du champ *ratione loci* de la directive lorsque le responsable de traitement n'est pas immatriculé sur le territoire de l'Union.

si le responsable a un établissement sur le territoire de l'Union[13]. La Cour a ensuite adopté une interprétation souple de la notion d'établissement au sens de l'article 4 de la directive. Pour elle, c'est la réunion de plusieurs critères qui permet l'applicabilité de la directive. Il suffit que le responsable du traitement des données « exerce, au moyen d'une *installation stable sur le territoire de cet État membre*, une *activité effective et réelle*, même minime, *dans le cadre de laquelle* ce traitement est effectué »[14].

S'agissant de la première exigence, la Cour a rappelé que « le traitement de données à caractère personnel en question soit effectué non pas «par» l'établissement concerné lui-même, mais uniquement «dans le cadre des activités» de celui-ci »[15]. Pour qualifier l'activité (dans le cadre de laquelle le traitement des données a lieu) d' « effective et réelle » et la rattacher au territoire d'un État membre, la juridiction d'un État membre peut tenir compte du fait que celle-ci est principalement, voire entièrement, tournée vers ledit État membre[16]. La seconde exigence, l' « installation stable sur le territoire », est vérifiée lorsqu'est situé sur le territoire un représentant qui participe, même de manière minime, à l'activité dans le cadre de laquelle le traitement est effectué[17].

Reste que la notion d'établissement est entendue très largement, de sorte que la réglementation européenne soit applicable à une multinationale dont le siège serait établi hors de l'Union européenne,

13 - CJUE, 3ème Ch., Arrêt du 1er octobre 2015, *Weltimmo s. r. o.*, C-230/14, § 28 : « [s]'agissant, en premier lieu, de la notion d'«établissement», il convient de rappeler que le considérant 19 de la directive 95/46 énonce que l'établissement sur le territoire d'un État membre suppose [...] que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante (arrêt Google Spain et Google, C-131/12, EU:C:2014:317, point 48) ».

14 - *Ibid.*, § 41. (nous soulignons).

15 - CJUE, Gde. Ch., Arrêt du 13 mai 2014, *Google Spain et Google*, C-131/12, § 52.

16 - CJUE, 3ème Ch., *Weltimmo s. r. o.*, préc., § 41. En l'espèce, il s'agissait d'une activité d'annonces immobilières payante au-delà d'un mois de publication, concernant des biens immobiliers de cet État, entièrement rédigé dans la langue de cet État.

17 - *Ibid.* Ainsi la Cour a considéré que le fait que le responsable qui dispose « d'un représentant dans ledit État membre, [...] chargé de recouvrer les créances résultant de [l']activité [en question] ainsi que de le représenter dans des procédures administrative et judiciaire relatives au traitement des données concernées », est suffisant pour considérer que la condition de l'installation stable sur le territoire est remplie.

mais dont les activités seraient tournées vers les personnes situées sur le territoire de l'UE dans le cadre desquelles un traitement des données serait effectué et qui dispose d'une installation stable sur ce territoire, participant, même de manière minime, à cette activité.

C'est précisément cette même logique qui gouverne l'identification du champ d'application territorial du règlement général sur la protection des données : la destination de l'activité exercée par le responsable de traitement est déterminante pour l'applicabilité du règlement européen. En effet, bien que le règlement européen abandonne les critères retenus par la directive en faveur de nouveaux rattachements, les deux textes semblent suivre un mode d'établissement de la juridiction similaire. Selon l'article 3 du règlement,

« 2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitements sont liées :

a) à *l'offre de biens ou de services* à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

b) au *suivi du comportement de ces personnes*, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union »[18].

L'interprétation de la CJUE, dans l'affaire *Weltimmo*, des critères de rattachement de la directive s'apparente à une transition avec l'arrivée du règlement[19]. Toutefois, la portée du règlement dépasse celle de la directive : le règlement européen, n'exigeant pas la présence d'un établissement sur le territoire de l'Union, peut désormais régir des situations qui sortaient du champ d'application

18 - 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 95/46/CE (règlement général sur la protection des données), *JOUE*, n° L119, p. 1, Article 3.

19 - On peut noter toutefois que paradoxalement, alors que le critère de la destination de l'activité a justifié l'élargissement de l'applicabilité de la directive, il va être celui qui va encadrer le champ d'application du règlement et limiter son extension.

territorial de la directive. La présence physique sur le territoire de l'Union n'est ici plus nécessaire. C'est désormais la seule destination de l'activité exercée par le responsable de traitement qui commande l'application du règlement, caractérisant l'extraterritorialité de la réglementation européenne.

L'Union européenne justifie le choix d'une telle extension extraterritoriale : élevée au rang de norme fondamentale[20], la protection des données personnelles fait l'objet de protections inégales dans le monde. Pour pallier les carences des législations étrangères, et « afin de garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit »[21], les auteurs du Règlement européen ont entendu étendre les principes promus dans la réglementation européenne aux États tiers. La portée large de la réglementation européenne permet ainsi d'éviter que des responsables de traitement situés sur le territoire d'États tiers ne puissent se cacher derrière le critère de l'établissement pour exercer des activités illégales de traitement de données.

L'élargissement du champ d'application de la réglementation européenne en matière de protection des données a fait l'objet d'une levée de boucliers par la doctrine étrangère[22]. Certains questionnent l'existence d'un lien territorial effectif entre la situation litigieuse et l'Union européenne et reprochent que « such an expansive approach to jurisdiction and applicable law would bring about precisely the "general application" that the ECJ [in the *Bodil Lindqvist* Case] tried to prevent »[23].

---

20 - M. Taylor, « The EU's Human Right Obligations in Relation to its Data Protection Laws with Extraterritorial Effet », *International Data Privacy Law*, vol. 5, n° 4, 2015, pp. 247-248.

21 - Règlement (UE) 2016/679, préc., Considérant 23.

22 - O. Tene, C. Wolf, « Overextended : Jurisdiction and Applicable Law under the EU General Data Protection Regulation », Future of Privacy Forum, janvier 2013, disponible sur https://fpf.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf [consulté en dernier lieu le 22 février 2018] ; voir également les inquiétudes soulevées par la doctrine russe : A. Petrova, « The Double Burden : Russia and the GDPR », *Lexology*, publié le 25 juillet 2017, disponible sur https://www.lexology.com/library/detail.aspx?g=dc52e55f-e299-4588-96ea-257a17316f63 [consulté en dernier lieu le 22 février 2018].

23 - O. Tene, C. Wolf,., *ibid.*, p. 3.

La question de l'extraterritorialité n'est pas propre au domaine de la protection des données[24]. Les activités sur Internet sont particulièrement affectées par des réglementations extraterritoriales[25]. Toutefois, elle pose la question de la sécurité juridique à l'égard des entreprises étrangères. Parce que ces dernières sont visées par la réglementation européenne, elles devront à la fois respecter la réglementation européenne, mais également la réglementation de leur État de nationalité[26].

Pour ces raisons, la licéité et l'efficacité de la réglementation européenne méritent d'être examinées au regard du droit international. L'exercice requiert que les critères retenus par la réglementation européenne sur lesquels repose l'extraterritorialité de cette norme soient appréciés à l'aune des règles du droit international public (I) avant d'examiner en second lieu l'efficacité de cette réglementation sur le territoire des États tiers (II).

§1 : La licéité de l'extraterritorialité

L'extraterritorialité est une « [s]ituation dans laquelle les compétences d'un État (législatives, exécutives ou juridictionnelles) régissent des rapports de droit situés en dehors du territoire dudit

24 - Voir par exemple, P. Jacob, « Quand les nuages ne s'arrêtent pas aux frontières. Remarques sur l'application du droit dans l'espace numérique à la lumière du Cloud Act », *Cahiers de droit de l'entreprise*, n° 4, juillet 2018, dossier 28 ; R. Bismuth, « Pour une appréhension nuancée de l'extraterritorialité du droit américain – Quelques réflexions autour des procédures et sanctions visant Alstom et BNP Paribas », *AFDI*, vol. LXI, 2015, pp. 785-807.

25 - Voir par exemple les différentes jurisprudences de juges nationaux au sujet d'ordonnances qui produisent des effets allant au-delà des frontières de leur propre État : TGI, Paris, *APC c. Auchan Telecom*, ordonnance de référé du 28 novembre 2013, disponible sur https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-28-novembre-2013/ [consulté en dernier lieu le 20 septembre 2018] ; TGI, Paris, *Mosley c. Google*, jugement du 6 novembre 2013, disponible sur https://www.youscribe.com/BookReader/Index/2335642/?documentId=2313066 [consulté en dernier lieu le 20 septembre 2018] ; High Court of Ireland, *McKeogh c. Doe*, jugement du 22 janvier 2012, n° 2012254P, 2012 [*IEHC*] 95.

26 - A. Petrova A., *op. cit.* La question n'intéresse pas que les destinataires de la réglementation, mais également ceux que la réglementation protège. Ainsi, les ressortissants européens peuvent se trouver en situation dans laquelle ils souhaitent avoir accès aux données collectées par une société étrangère sans savoir quelle loi est applicable. Voir dans ce sens, A. S. De Sousa Gonçalves, « The Extraterritorial Application of the EU Directive on Data Protection », *SYBIL*, vol. 19, 2015, pp. 195209, en particulier p. 196.

État »[27]. Il s'agit de l'exercice d'un « pouvoir juridique conféré ou reconnu par le droit international »[28]. Dès lors, l'exercice de la compétence extraterritoriale doit trouver sa source dans l'ordre juridique international[29]. En tant que tel, ainsi que l'a consacré la Cour permanente de justice internationale dans la célèbre affaire du *Lotus*[30], l'exercice d'une compétence normative extraterritoriale n'est pas interdit[31]. Si la lecture de cette affaire a créé des divisions au sein de la doctrine[32], il semble que tous s'accordent sur le fait que la compétence extraterritoriale n'est conforme au droit international que pour autant qu'elle est justifiée par un rattachement « raisonnable »[33] à un des critères de compétences des États reconnus par le droit international général, ou alors sous réserve de l'absence d'opposition de la part des États concernés. Le droit international admet plusieurs rattachements pour l'exercice de la compétence étatique normative : la compétence territoriale et la compétence personnelle. Toutefois l'Union européenne fonde sa juridiction en matière de protection des données à caractère personnel

27 - J. Salmon(dir.), *Dictionnaire de droit international public*, Bruylant, Bruxelles, 2001, p. 491.

28 - *Ibid.*, p. 210.

29 - J. Bourguignon, *La compétence personnelle passive*, Mémoire de recherche sous la direction de Gérard Cahin, Paris II, 2010, disponible sur https://docassas.u-paris2.fr/nuxeo/site/esupversions/e31f020c-9b14-46a5-83cb-b869636cf66c [consulté en dernier lieu le 22 février 2018], p. 2.

30 - CPJI, *Lotus*, Arrêt du 7 septembre 1927, Série A, n° 13, p. 19.

31 - Dans cette affaire, un navire français, le Lotus, avait abordé un navire turc, lequel sombre juste après l'intervention du navire français avec huit Turcs présents à bord. L'officier aux commandes du Lotus et le capitaine du navire turc ont tous les deux été arrêtés à Constantinople et fait l'objet de poursuites pénales en vertu de la législation turque. Contestant la compétence des juridictions turques, la France a saisi la Cour permanente de Justice internationale afin qu'elle statue sur la question de savoir si la Turquie pouvait exercer sa compétence conformément aux règles du droit international.

32 - Sur ce point, et pour une analyse détaillée de l'affaire voir M. Cosnard, « Les lois Helms Burton et d'Amato-Kennedy, interdiction de commercer avec et d'investir dans certains pays », *AFDI*, vol. 42, 1996, pp. 37-38.

33 - L'application extraterritoriale, quand bien même fondée sur un critère de rattachement admis, peut mener à des conflits de compétences. Dès lors, l'admissibilité de la compétence extraterritoriale doit au surplus se justifier au regard du principe de bonne foi : il s'agit d'éviter des conflits de compétences en justifiant d'un rattachement raisonnable de la situation avec l'État. Voir en ce sens, CIJ, *Barcelona Traction, Light and Power Company*, Arrêt du 5 février 1970, *CIJ Rec.* 1970, opinion individuelle du juge Fitzmaurice, p. 105. Voir également B. Stern, « Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit », *AFDI*, vol. 32, 1986, pp. 45-46.

principalement sur une facette contestée de ces rattachements : la conception extensive du principe de territorialité objective (A). Il semble néanmoins que ce rattachement n'ait pas fait l'objet de vives réactions étatiques (B).

A. L'extraterritorialité de la réglementation européenne fondée sur une conception extensive du rattachement territorial

Le principe de territorialité est un principe largement reconnu comme moyen d'établissement de la juridiction d'un État. Conformément à ce principe, un État peut exercer à la fois ses compétences normative et coercitive aux situations se déroulant sur son territoire[34]. De fait, les situations entièrement territoriales ne posent aucune difficulté quant à l'opportunité et la licéité de l'application de la réglementation européenne. Le fondement territorial inclut à la fois un principe de territorialité subjective, « donnant compétence à l'État sur les actes ayant reçu un commencement d'exécution sur son territoire »[35], et un principe de territorialité objective « donnant compétence à l'État sur des actes commis à l'étranger, mais dont un des éléments constitutifs, qui peut être l'effet de l'acte, s'est produit sur le territoire »[36]. Compte tenu des spécificités du monde numérique, le second aspect du rattachement territorial est prépondérant par rapport au premier aspect de ce dernier. On en trouve une illustration dans l'affaire *Lotus* au sujet de l'applicabilité d'une loi pénale nationale. La Cour y affirmait :

« il est constant que les tribunaux de beaucoup de pays, même de pays qui donnent à leur législation pénale un caractère strictement territorial, interprètent la loi pénale dans ce sens que les délits dont les auteurs au moment de l'acte délictueux se trouvent sur le territoire d'un autre État, doivent néanmoins être considérés comme ayant été commis sur le territoire national, *si c'est là que s'est produit un des éléments constitutifs du délit et surtout ses effets* »[37].

34 - C. Ryngaert, *Jurisdiction in International Law*, Oxford Univ. Press, Oxford, New York, 2ème éd., 2015, § 46.

35 - B. Stern, *op. cit.*, p. 24.

36 - *Ibid.*

37 - CPJI, *Lotus*, préc., p. 23.

Le recours à cette conception pour établir la juridiction de l'Union européenne en matière de protection des données n'est pas nouveau : à la fois l'application de la directive et les critères de rattachement retenus dans le règlement illustrent une volonté de gommer les limites que peuvent représenter les frontières sans pour autant complètement effacer tout rattachement territorial. En ce sens, la conception objective du rattachement territorial peut être une solution efficace. Toutefois, l'interprétation extensive par la CJUE et le choix des critères retenus par le règlement inquiètent : à moins que l'on affine la lecture de la conception objective (2), l'interprétation trop extensive de cette dernière pourrait mener à une dérive qui échouerait à justifier la portée extraterritoriale de la réglementation européenne (1).

1. L'inadéquation partielle de la conception territoriale objective comme fondement à la réglementation européenne

Dans l'affaire *Google Spain* la Cour a fondé l'application de la directive 95/46/CE sur l'approche objective du rattachement territorial[38]. Elle a jugé que, conformément à la directive 95/46/CE sur la protection des données à caractère personnel, Google Inc., en tant que responsable du traitement des données personnelles, doit effacer les liens vers des pages web pouvant contenir des données personnelles d'un usager dès lors que ces données apparaissent inadéquates, pas ou plus pertinentes ou excessives au regard des finalités pour lesquelles elles ont été traitées et du temps qui s'est écoulé[39]. Pour reprocher à la société américaine le non-respect de la réglementation européenne, la Cour a relevé que l'établissement situé en Espagne « se livr[ait] à l'exercice effectif et réel d'une activité au moyen d'une installation stable en Espagne ». Elle constituait donc un « établissement » au sens de l'article 4 § 1 a) de la directive. L'approche objective du fondement territorial apparaît précisément lorsque la Cour observe que cet établissement espagnol menait des activités « indissociablement liées » au traitement des données

38 - M. Taylor, « Permissions and Prohibitions in Data Protection Jurisdiction », Brussel Privacy HUB, VUB, Working Paper, vol. 2, n° 6, mai 2016, pp. 14-15.

39 - CJUE, Gr. Ch., aff. C-131/12, *Google Spain SL, Google Inc c. Agencia Española de Protección de Datos, Mario Costeja Gonzalez*, Communiqué de presse n° 70/14, 13 mai 2014. Voir le commentaire de G. Busseuil, « Arrêt Google : du droit à l'oubli de la neutralité du moteur de recherche », *JCP E*, 2014, pp. 1327 et s.

réalisé par Google Inc. Selon la Cour, ces « activités relatives aux espaces publicitaires constituent [...] le moyen permettant l'accomplissement de ces activités »[40]. L'approche par la Cour est particulièrement extensive : les activités menées par Google Spain se limitaient à la vente et à la promotion d'espaces publicitaires, alors que la requête intéressait surtout le service offert par le moteur de recherche, en particulier celui consistant à indexer les informations sur le site Internet de Google. Or cette activité se déroulait essentiellement sur le territoire d'un État tiers. Toutefois, pour la Cour, l'établissement espagnol de Google Inc a participé à l'activité qui fait l'objet du litige dans la mesure où le service offert par Google Spain a assuré la rentabilité du moteur de recherche. Cette lecture large, qu'elle reconnait par ailleurs[41], a été confirmée plus tard dans l'affaire *Weltimmo*, dans laquelle la Cour admet l'application de la directive bien que l'activité de l'établissement situé sur le territoire de l'Union n'ait qu'un lien « minime » avec le traitement des données à caractère personnel[42]. Ainsi, c'est parce qu'une partie de l'activité litigieuse se déroule sur le territoire de l'Union, que le rattachement territorial a pu être affirmé.

Le règlement général sur les données personnelles bénéficie du même traitement : le législateur de l'Union fonde également l'applicabilité du règlement sur l'approche objective du rattachement territorial. Toutefois, il semble que la conception adoptée par le législateur dans le cadre de l'application du règlement soit encore plus extensive que celle adoptée du temps de la directive. Le lien de rattachement entre l'Union européenne et son territoire est bien plus indirect en ce que disparait l'exigence d'un établissement. Désormais, les responsables du traitement ou les sous-traitants, quel que soit le lieu de leur établissement, sont visés par le règlement dès lors que les activités de

40 - CJUE, Gr. Ch., aff. C-131/12, *Google Spain SL*, préc., § 56.

41 - *Ibid.* §§ 53-54 :
« [a]u vu de l'objectif de la directive 95/46 d'assurer une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée, à l'égard du traitement des données à caractère personnel, cette dernière expression ne saurait recevoir une interprétation restrictive [...].
Il convient de relever dans ce contexte qu'il ressort notamment des considérants 18 à 20 et de l'article 4 de la directive 95/46 que le législateur de l'Union a entendu éviter qu'une personne soit exclue de la protection garantie par celle-ci et que cette protection soit contournée, en prévoyant un champ d'application territorial particulièrement large ».

42 - CJUE, 3ème Ch., aff. C-230/14, *Weltimmo s. r. o.*, 1er octobre 2015, § 41.

ces derniers sont liées à l'offre de biens ou de services aux personnes qui se trouvent sur le territoire de l'Union ou au suivi du comportement de ces personnes. C'est donc la destination de l'activité de traitement des données qui guide l'applicabilité du règlement. Or, on peut discuter de la correspondance exacte avec la définition de la territorialité objective[43]. Si l'on constate que les effets de l'activité entrent en ligne de compte pour la détermination du droit applicable, ils n'en sont pas systématiquement des éléments constitutifs de l'activité litigieuse. À titre d'illustration, les effets d'un refus de déréférencement d'anciens articles relatant une dette importante d'une personne dont la recherche d'emploi est vaine peuvent difficilement être regardés comme éléments constitutifs de la violation de la réglementation européenne en matière de protection des données.

C'est sans doute le type d'application extraterritoriale qui pose problème : il s'agit « d'une application extraterritoriale du droit fondée sur une conception extensive du rattachement territorial, et en particulier du principe de territorialité objective »[44]. Cette doctrine, communément appelée théorie des effets, fonde les compétences extraterritoriales sur le seul fait que des agissements étrangers sont à l'origine d'effets ressentis sur le territoire. Appliquée pour la première fois par le juge américain dans l'affaire *Alcoa*, cette doctrine a été largement contestée. Dans cette affaire, il était question de savoir si les États-Unis pouvaient exercer leurs compétences normatives à l'égard d'un arrangement soupçonné d'être frauduleux entre deux sociétés étrangères, lequel risquait de produire une forte inflation des prix sur le marché américain de l'aluminium[45]. Le juge Learned Hand y affirmait alors qu'un État pouvait exercer des compétences extraterritoriales sur des actes accomplis en dehors de ses frontières, mais qui produisent des effets sur le territoire national[46].

43 - En ce sens, voir D.J.B. Svantesson, « The Extraterritoriality of EU Data Privacy Law – Its Theoritical Justification and its Practical Effect on U.S. Businesses », *Stanford Journal of International Law*, vol. 50, n° 1, 2014, pp. 84-86.

44 - B. Stern, *op. cit.*, p. 31.

45 - Court of Appeals, 2nd Cir., *Alcoa, US v. Aluminium Co. Of America*, 12 mars 1945, 148 *F.2d*, p. 421.

46 - *Ibid*., p. 443 : « it is settled law [...] that any state may impose liabilities [may exercise jurisdiction over], even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends ; and these liabilities other states will ordinarily recognize ».

Cette affaire, qui pourtant n'avait pas reçu au départ un accueil défavorable[47], a suscité de nombreuses oppositions, en particulier parce qu'elle ouvrait une boîte de Pandore, qui pouvait fonder des lois extraterritoriales dans de nombreux autres domaines[48] et dont les conséquences allaient être accentuées sous l'effet de la mondialisation[49].

Le monde de l'Internet est également affecté par ce phénomène d'effacement du rattachement territorial, au sens classique du terme, devant l'application de la doctrine des effets[50]. Dans le domaine du numérique, la doctrine des effets trouve une illustration dans l'affaire *Yahoo !*, dans laquelle le juge français a accepté qu'une loi française ait des effets extraterritoriaux dans la mesure où le site litigieux était accessible du territoire français[51]. En particulier le juge français s'est appuyé sur cette doctrine pour affirmer sa compétence. En effet, dans cette affaire, il était reproché à la compagnie américaine, de permettre la vente d'objets nazis *via* le site Yahoo Auctions. Cette activité était contraire au droit pénal français. Pour justifier la compétence du juge français, pour la demande dirigée à l'encontre deYahoo Inc., le juge a relevé que bien que le site s'adresse principalement aux internautes basés aux États-Unis, eu égard aux modes de paiement prévus, aux conditions de livraison ou encore à la langue et à la monnaie utilisées, « il n'en est pas de même des enchères d'objets représentant des symboles de l'idéologie nazie qui

47 - C. Ryngaert, *Jurisdiction in International Law*, *op. cit.*, § 299 ; K. M. Meessen, « Antitrust Jurisdiction under Customary International Law », *American Journal of International Law*, vol. 78, 1984, p. 791.

48 - C. Ryngaert, *Jurisdiction in International Law*, *op. cit.*, § 299. R. Jennings, « Extraterritorial Jurisdiction in the United States Antitrust Laws », *British Yearbook of International Law*, vol. 33, 1957, p. 159 ; F.A. Mann, « The Doctrine of Jurisdiction in International Law », *RCADI*, vol. 111, 1964-I, pp. 86-87 ; M. Akehurst, « Jurisdiction in International Law », *British Yearbook of International Law*, vol. 46, 1972-1973, p. 155.

49 - Ce qu'avait déjà souligné le juge américain Learned Hand dans l'affaire *Alcoa* : « almost any limitation of the supply of goods in Europe, for example, or in South America, may have repercussions in the United States if there is trade between the two », *in* Court of Appeals, 2nd Cir., *Alcoa, US v. Aluminium Co. Of America*, 12 mars 1945, 148 *F.2d*, p. 443. Voir également R. Michaels, « Territorial Jurisdiction after Territoriality », *in* P.-J. Slot et M. Bulterman (dir.), *Globalisation and Jurisdiction*, Kluwer Law International, 2004, p. 123.

50 - En ce sens voir A.-T. Norodom, « Propos introductifs. Internet et le droit international : défi ou opportunité ? », *in* SFDI (dir.), *Internet et le droit international*, Pedone, Paris, 2014, p. 29.

51 - TGI, *Licra et UEJF c. Yahoo Inc. et Yahoo France*, ordonnance en référé du 20 novembre 2000, *Comm. Comm. Électr.*, décembre 2000, comm. n° 92 132, observations J.-C. Gailloux.

peuvent intéresser et sont accessibles à toute personne qui souhaite les suivre, y compris aux Français »[52]. En particulier, selon le juge, « la simple visualisation en France de tels objets constitue une violation de l'article R. 645-1 du Code pénal et donc un trouble à l'ordre public interne [et] [q]u'en outre cette visualisation cause à l'évidence un dommage en France aux associations demanderesses ». C'est donc à l'appui des effets subis sur le territoire français consécutifs à la publication sur un site Internet d'objets prohibés en France que le juge français a pu se déclarer compétent.

L'application de cette doctrine dans le domaine de la protection des données à caractère personnel a également fait l'objet d'une levée de boucliers[53]. Une première critique est théorique. Les difficultés théoriques rencontrées ne sont pas propres à l'Internet ; tout comme pour les règles applicables en droit de la concurrence, il a pu être souligné que le lien entre les effets invoqués et l'acte étranger litigieux est difficilement identifiable[54]. Ainsi que le relève à raison Mistale Taylor, « [t]his is due to the fact that everyone with Internet access could in theory access every website, indiscriminately establishing this act-effect link »[55]. La critique porte dès lors sur la crainte d'un champ d'application *ratione loci* de la réglementation européenne en matière de protection des données « too open-ended »[56], au point que certains rejettent toute application de la théorie des effets à la matière[57]. La crainte de la « general application »[58] soulignée auparavant peut toutefois être tempérée

52 - *Ibid.*

53 - T. Schultz, « Carving up the Internet : Jurisdiction, Legal Orders, and the Private/Public International Law Interface », *European Journal of International Law*, vol. 19, n° 4, 2008, pp. 811-816.

54 - *Ibid.*, pp. 814-815.

55 - M. Taylor, « Permissions and Prohibitions in Data Protection Jurisdiction », *op. cit.*, p. 19. Voir dans le même sens Zittrain J., « Be Careful What You Ask For : Reconciling a Global Internet and Local Law », The Berkman Center for Internet & Society at Harvard Law School, Research Paper n° 2003-03 5/2003, disponible sur https://cyber.harvard.edu/wg_home/uploads/204/2003-03.pdf [consulté en dernier lieu le 22 février 2018], p. 5.

56 - C. Kuner, « Data Protection Law and International Jurisdiction on the Internet (Part 1) », *International Journal of Law and Information Technology*, vol. 18, n° 2, 2010, p. 190 ; M. Taylor, « Permissions and Prohibitions in Data Protection Jurisdiction », *op. cit.*, p. 19.

57 - T. Schultz, *op. cit.*, p. 815.

58 - O. Tene, C. Wolf, *op. cit.*

par la distinction entre l'exercice des compétences normative et coercitive. L'exercice de compétences coercitives extraterritoriales est strictement prohibé par le droit international. En conséquence, nous y reviendrons[59], cette forme de compétences a exclusivement un fondement territorial[60]. En d'autres termes, sans la coopération de l'État étranger, la décision rendue par une juridiction d'un État membre de l'Union pourrait ne produire aucun effet à l'égard de la société étrangère[61]. Toutefois ce tempérament peut aussi être source d'inquiétudes pour les entreprises étrangères. Cette source d'inquiétudes cristallise une seconde forme d'opposition qui porte cette fois-ci sur des considérations pratiques. Si la réalisation d'une décision prononcée en application d'une loi extraterritoriale est fonction de la coopération de l'État étranger, alors elle peut aussi être source d'insécurité pour l'entreprise américaine qui ne sait pas si la décision sera exécutée par sa juridiction nationale.

Pour autant, cette doctrine est-elle dénuée de toute pertinence en ce qui concerne la réglementation en matière de protection des données à caractère personnel ? Elle est certainement utile pour éviter les contournements de la réglementation européenne des entreprises qui traitent les données de personnes sur le territoire de l'Union et qui s'installent dans un État avec une législation plus favorable. La difficulté réside alors dans la lecture des critères du prochain règlement. Pour éviter toute dérive, le critère du lien entre l'activité de traitement et l'offre de biens ou de services d'un côté et le suivi du comportement des personnes de l'autre devrait être à l'avenir affiné.

2. L'affinement de la conception objective du rattachement territorial : la technique du *targeting*

La solution la plus adéquate serait d'adopter une lecture restrictive des critères posés par le règlement. Il ne s'agit pas de réduire

59 - Voir *Infra*, 2ème partie.

60 - U. Kohl, *Jurisdiction and the Internet – Regulatory Competence over Online Activity – Regulatory Competence in the Online World*, Cambridge Univ. Press, 2007, p. 200 ; P. Trudel, « Jurisdiction over the Internet : A Canadian Perspective », *International Lawyer*, vol. 32, 1998, p. 1047.

61 - J. L Goldsmith., « The Internet, Conflicts of Regulation, and International Harmonization », *in* C.Engel et K.H. Keller (dir.), *Governance in the Light of Differing Local Values*, Nomos, Baden-Baden, 2000, pp. 198-200.

l'applicabilité du règlement à néant, mais d'éviter une application illimitée qui ferait de toute manière l'objet de contestations étatiques. L'une des techniques suggérées par la doctrine et la jurisprudence pour établir un « rattachement raisonnable »[62] avec l'État à l'origine de la réglementation est celle du principe du *targeting.* Il s'agit d'une version plus stricte de la théorie des effets, déjà connue et appliquée dans d'autres domaines que l'Internet[63], selon laquelle le rattachement territorial n'est constitué que dans la mesure où l'activité produit intentionnellement des effets sur le territoire de l'État qui souhaite exercer sa compétence normative[64].

Sans que cela ait été consacré explicitement, le juge français avait eu recours à cette méthode dans l'affaire *Yahoo* : pour établir le rattachement avec la France et reconnaitre sa compétence pour rendre l'ordonnance, le juge français avait observé que « Yahoo *sa[vait]* qu'elle s'adress[ait] à des Français puisque, à une connexion à son site d'enchères réalisée à partir d'un poste situé en France, elle répond[ait] par l'envoi de bandeaux publicitaires rédigés en langue française »[65]. Parce que Yahoo s'adressait directement à un auditoire français par l'intermédiaire de bandeaux publicitaires, rédigés en français ; elle ne pouvait donc ni ignorer ni nier le caractère

62 - Cette expression traduit l'état de la doctrine quant à l'opportunité d'appliquer une loi extraterritoriale. L'expression a été utilisée dans les travaux de Frederic Alexander Mann, *in* F.A. Mann, « The Doctrine of Jurisdiction in International Law », *RCADI*, vol. 111, 1964-I, p. 49 ; Dans le même sens, le juge Fitzmaurice dans une opinion individuelle dans l'affaire *Barcelona Traction* a affirmé que les États sont soumis à une « obligation de modération et de mesure » lorsqu'ils souhaitent exercer une compétence normative extraterritoriale, *in* CIJ, *Barcelona Traction* , préc., p. 105.

63 - Cette théorie n'est pas inconnue du prétoire de la Cour de justice de l'Union européenne : voir par exemple l'affaire de la CJUE, Gde. Ch., *Peter Pammer c. Reederei Karl Schlüter GmbH et Hotel Alpenhof GesmbH c. Olivier Heller*, aff. jointes n° C-585/08 et C-144/09, *Dalloz actualité*, 3 janvier 2011, observations C. Manara, *Revue critique de Droit international privé,* 2011, p. 414, note O. Cachard, *Revue trimestrielle de droit européen*, 2011, p. 475, observations E. Guinchard. La jurisprudence française a régulièrement recours à cette technique dans les différends relatifs au droit de la concurrence, comme en témoignent les nombreuses affaires devant la Chambre commerciale de la Cour de cassation : Voir par exemple, Cass. Com., 9 mars 2010, n° 08-16.752 ; 13 juillet 2010, n° 06-20.230 ; 3 mai 2012, n° 11-10.505, n° 11-10.507 et n° 11-10.508. Voir sur cette mise en œuvre de la théorie du *targeting*, Jault-Seseke F., « Internet, vecteur d'affinement des règles de compétence juridictionnelle », *in* SFDI (dir.), *Internet et le droit international*, *op. cit.*, pp. 167-180, en particulier pp. 170-174.

64 - T. Schultz, *op. cit.*, p. 817.

65 - TGI, *Licra et UEJF c. Yahoo Inc. et Yahoo France*, préc.

intentionnel de s'adresser à un public français. L'intention était constituée[66].

La théorie dite du *targeting* présente les mêmes avantages que la doctrine des effets, mais elle permet également d'apaiser les tensions que pourrait soulever l'application d'une conception trop extensive du principe de territorialité objective au droit de la protection des données personnelles. L'un des avantages de cette conception est qu'elle circonscrit le nombre d'États pouvant prétendre à l'exercice de compétences normatives : désormais seuls ceux qui pourront justifier d'un lien suffisant – c'est-à-dire démontrant l'intention de produire des effets sur l'État qui invoque la violation de son droit national – pourront appliquer leurs normes à la situation étrangère. En d'autres termes, la réglementation européenne ne sera applicable aux situations étrangères que si ces dernières font état d'une intention de produire des effets à l'égard des personnes qui se trouvent sur le territoire de l'Union. Un second avantage permet également de tempérer l'une des critiques soulevées à l'égard de la doctrine des effets : cette conception restreinte assure une meilleure prévisibilité des réglementations applicables à une activité[67]. Les entreprises ne seront soumises qu'aux réglementations des États qui constituent leur marché.

Il semble que ce soit précisément cette technique qui a inspiré les travaux du G29 alors qu'ils examinaient l'applicabilité de la réglementation européenne avant même que ne soit rendu l'arrêt *Weltimmo*[68]. Le G29 avait ainsi proposé des critères supplémentaires

66 - T. Schultz, *op. cit.*, p. 817. L'auteur cite également un second exemple : l'affaire *Gutnick c. Dow Jones*. Dans cette affaire, un ressortissant australien reprochait à un journal disponible sur Internet de reproduire des éléments diffamatoires. Même si le journal s'adresse essentiellement à des ressortissants américains, il demeure que le journal compte parmi ses abonnés un bon nombre de lecteurs australiens. Dès lors, le journal ne pouvait ignorer avoir des lecteurs en Australie et ne pouvait ignorer les effets qu'allaient produire la publication de tels éléments sur le territoire australien. Le juge australien a conclu à l'établissement d'un lien suffisant entre l'acte litigieux et l'Australie. Supreme Court of Victoria, Melbourne, Common Law Division, *Joseph Gutnick v. Dow Jones & Company Inc.*, 28 juin 2001, n° 7763, [2001] VSC 305, disponible sur https://jade.io/article/74115 [consulté en dernier lieu le 22 février 2018].

67 - F. Jault-Seseke, *op. cit.*, p. 170 ; T. Schultz, *op. cit.*, pp. 817-819 ; *Contra* : D.J.B. Svantesson, « Extraterritoriality and Targeting in EU Data Privacy Law : the Weak Spot Undermining the Regulation », *International Data Privacy Law*, vol. 5, n° 4, 2015, p. 232.

68 - Groupe de travail « Article 29 » sur le droit applicable, Avis 8/2010, adopté le 16 décembre 2010, 0836-02/10/FR, WP 179.

lorsque le responsable du traitement est établi en dehors de l'Union européenne en vue de « garantir l'existence d'un lien suffisant avec le territoire »[69]. Parmi les critères proposés par le Groupe de travail, on peut lire le « ciblage des personnes ou l'"approche axée sur le service" ». Selon le Groupe de Travail, l'activité impliquant le traitement de données à caractère personnel doit cibler des personnes résidant dans l'UE pour entraîner l'application du droit de l'UE en matière de protection des données. Le groupe de Travail compare cette pratique à ce qui se passe dans le domaine de la protection des consommateurs. Des indices tels que la langue employée sur le site, la livraison de produits dans les États de l'Union européenne, le fait que l'accessibilité d'un service soit subordonnée à l'utilisation d'une carte de crédit européenne, etc. sont au sens du Groupe de travail suffisants à établir l'accessibilité des ressortissants de l'Union européenne au service proposé par le responsable du traitement des données[70]. Ainsi un site de vente d'objets domicilié en Chine dont l'affichage est en mandarin, qui n'envoie pas de publicités dans la langue parlée par le destinataire, dont un ressortissant de l'Union européenne qui aurait des notions de mandarin viendrait à acheter un produit sur ce site ne devrait pas être soumis à la réglementation européenne dans la mesure où celui-ci ne vise pas la clientèle européenne. En revanche, un site de réservations de chambre dans un hôtel aux États-Unis qui viendrait à proposer plusieurs langues parlées dans l'Union européenne et qui accepte le paiement par carte bancaire utilisée sur le territoire de l'Union européenne serait en revanche soumis à la réglementation européenne.

B. L'absence de contestation du caractère extraterritorial de la réglementation

Les objections de la communauté internationale et les réactions individuelles des États visés jouent un rôle de première importance dans l'établissement de l'admissibilité de la réglementation européenne en matière de protection des données. La recension de réactions négatives visant le caractère extraterritorial de la réglementation européenne suffit à démontrer l'impossibilité pour

69 - *Ibid.*, p. 36.

70 - *Ibid.*

la théorie du *targeting* à être reconnue par le droit international. Ainsi que l'indiquait Michel Cosnard, au sujet des critères de compétences extraterritoriales, « [c]e n'est qu'à partir du moment où un État prétend fonder sa compétence sur [un] titre [de compétence] que l'on pourra évaluer sa licéité, notamment au regard des réactions des autres États, qui lui donneront une validité, une opposabilité internationale »[71].

Il suffit pour s'en convaincre de citer l'affaire du gazoduc sibérien[72]. Au cours de cette affaire, les États-Unis ont cherché à étendre l'interdiction de toute exportation de technologies d'origine américaine à l'URSS à des entreprises étrangères. Les États-Unis prétendaient exercer une forme de compétence personnelle, selon laquelle ces biens et technologies étaient de nationalité américaine[73].

71 - M. Cosnard, *op.cit.*, p. 38.

72 - De la même manière, on peut citer l'épisode des lois Helms-Burton et d'Amato-Kennedy qui a donné lieu à de vives protestations de l'Union européenne. Ces lois avaient pour objet toute une série de mesures à portée extraterritoriale interdisant toute relation commerciale avec respectivement Cuba d'un côté et la Syrie et l'Iran de l'autre. Les États européens, le Canada, et le Mexique ont fermement condamné à de nombreuses occasions les deux lois tant sur leur contenu que sur l'absence de fondement à leur caractère extraterritorial (Voir par exemple, l'adoption par l'Assemblée générale de l'ONU d'une résolution dénonçant l'embargo américain qui a été à de nombreuses reprises réaffirmée. Voir par exemple, ONU, « L'assemblée générale demande une nouvelle fois aux États-Unis de lever l'embargo économique, commercial et financier contre Cuba », Communiqué de presse du 5 novembre 1997, *Doc ONU*, AG/714 disponible sur https://www.un.org/press/fr/1997/19971105.AG714.html [consulté en dernier lieu le 22 février 2018] ; « Pour la onzième année consécutive l'Assemblée générale appelle à la levée du blocus contre Cuba », Communiqué de presse du 12 novembre 2002, *Doc ONU*, AG/1357, disponible sur https://www.un.org/press/fr/2002/AG1357.doc.htm [consulté en dernier lieu le 22 février 2018]. Pour d'autres exemples voir M. Cosnard, *op. cit.*, pp. 45-46.). Ainsi par exemple, le Conseil des ministres de l'Union européenne a adopté en novembre 1996 une réglementation érigeant en infraction le respect de la loi Helms-Burton (Voir en ce sens, la position du Représentant de la présidence du Conseil des ministres de l'Union européenne *in* Secrétaire Général de l'ONU, « Nécessité de lever le blocus économique, commercial et financier appliqué à Cuba par les États-Unis d'Amérique », 52ème session, *Doc ONU A/52/342*, p. 16.). Le Canada et le Mexique ont adopté des lois protégeant les sociétés ayant leur nationalité contre la loi Helms-Burton (Canada, Loi complétant et modifiant la « Loi sur les mesures extraterritoriales étrangères », adoptée le 9 octobre 1996, reproduite *in International Legal Materials*, vol. 36, 1997, p. 111 ; Mexique, loi adoptée le 23 octobre 1996, reproduite *in International Legal Materials*, vol. 36, 1997, p. 133. Voir M. Cosnard, *op. cit.*, p. 46.). L'illicéité du caractère extraterritorial des mesures adoptées dans ces affaires a systématiquement été reconnue.

73 - Sur cette affaire, voir P. Merciai, « The Euro-Siberian Gas Pipeline Dispute – A Compelling Case for the Adoption of Jurisdictional Codes of Conduct », *Maryland Journal of International Law & Trade*, vol. 8, n 1, 1984, pp. 1-51 ; et, dans une moindre mesure, R. Bismuth, *op. cit.*, pp. 795-796.

La CEE, impliquée dans l'affaire[74], s'était fortement élevée contre cet embargo. Les ministres des Affaires étrangères, réunis au sein du Conseil des ministres pour les Communautés européennes avaient ainsi estimé que :

« [c]es mesures, prises sans qu'aucune consultation avec la Communauté n'ait eu lieu, impliquent une extension extra-territoriale de la compétence juridictionnelle des États-Unis qui, en l'occurrence, est contraire aux principes du droit international, est inacceptable pour la Communauté et n'est pas susceptible d'être reconnue par les tribunaux des États membres de la CEE »[75].

Au surplus, selon le Conseil, non seulement les technologies ne peuvent avoir de nationalité, mais au surplus le droit international ne permet pas à un État d'exercer ses compétences sur les personnes qui contrôlent ces objets[76].

Dans le cas de l'extraterritorialité de la réglementation européenne, on peut relever que les États tiers ne se sont pas montrés offensifs[77]. Au contraire, dans le domaine de la protection des données, la protestation n'est pas l'œuvre des États tiers, mais de quelques sociétés multinationales[78].

74 - Les sociétés étrangères qui réexpédiaient les technologies américaines en URSS étaient françaises, allemandes, italiennes et britanniques.

75 - Propos rapportés *in Bull. CE*, 15ème année, n° 6, 1982, p. 78, § 2.2.44.

76 - European Communities, « Comments on the US Regulations Concerning Trade with the USSR », *International Legal Materials*, vol. 21, 1982, p. 894 : « [g]oods and technology do not have any nationality and there are no known rules under international law for using goods or technology situated abroad as a basis of establishing jurisdiction over the persons controlling them ».

77 - C. Ryngaert, « Guest Editorial. Symposium Issue on Extraterritoriality and EU Data Protection », *International Data Privacy Law*, vol. 5, n° 4, 2015, p. 222.

78 - Voir par exemple le billet du directeur juridique de Google, K. Walker, « Defending access to lawful information at Europe's highest court », publié le 15 novembre 2017, disponible sur https://www.blog.google/topics/google-europe/defending-access-lawful-information-europes-highest-court/ [consulté en dernier lieu le 22 février 2018] . Dans le même sens, voir également le billet du responsable de la protection des données à caractère personnel de Google, P. Fleischer, « Implementing a European, not global, right to be forgotten », publié le 30 juillet 2015, disponible sur https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html [consulté en dernier lieu le 22 février 2018].

Parfois certains ont appliqué les mêmes titres de compétences, ceux-là mêmes qui pourraient faire l'objet de contestations. C'est ainsi que le juge canadien dans l'affaire *Globe24h.com* a appliqué la théorie du *targeting* pour justifier l'application extraterritoriale de la loi canadienne en matière de protection des données. Dans cette affaire, il était reproché au site Internet *Globe24h.com* de republier des décisions judiciaires canadiennes comportant des renseignements personnels. Ce n'est pas tant la republication qui posait problème en elle-même, mais davantage le fait que les décisions nouvellement publiées sur ce site sont désormais indexées par les moteurs de recherche, contrairement aux décisions publiées sur certains sites dédiés à la publication des décisions des tribunaux canadiens. Dès lors, une recherche avec le nom d'une personne aboutissait à ces décisions. Or, l'entreprise est basée en Roumanie. Pour justifier de l'application de la loi canadienne de protection des données, le juge a souligné le « lien suffisant » entre les activités de l'entreprise établie en Roumanie et le Canada. Ainsi, selon le juge canadien, « parmi les facteurs de rattachement pertinents figurent 1) l'emplacement du public cible du site Web 2) la source du contenu du site Web, 3) l'emplacement de l'exploitant du site Web et 4) l'emplacement du serveur hôte »[79]. On retrouve ici le même procédé de rattachement à la juridiction du Canada que celui qui est mis en place par la réglementation européenne.

L'absence de contestation semble dénoter d'une certaine reconnaissance de la théorie du *targeting* et la licéité du caractère extraterritorial de la réglementation européenne. Toutefois, l'efficacité de la réglementation ne suit pas systématiquement la licéité.

§2 : L'efficacité de la réglementation extraterritoriale

Lorsque l'on examine l'efficacité d'une norme, on entend sans aucun doute son caractère effectif, en ce sens que la norme soit « appliquée réellement »[80]. Sans réduire à néant l'efficacité du caractère obligatoire, détaché du caractère exécutoire de la norme

79 - Cour fédérale (Canada), Ontario, *A.T. c. Globe24h.com. et le Commissaire à la protection de la vie privée du Canada*, 30 janvier 2017, *Documents Can LII*, § 53.

80 - G. Cornu *et al.*, *Vocabulaire juridique*, PUF, 12ème éd., 2018, voir « effectivité ».

– ce dont nous ne discuterons pas ici, l'absence d'exécution d'une réglementation rend difficile son application, ou à tout le moins le retour à la légalité d'un comportement indu. Or, le droit international interdit tout acte d'exécution en territoire étranger. Dès lors, seule la coopération des États concernés peut permettre l'exécution de la norme extraterritoriale[81]. Or, tous les États ne défendent pas avec la même ferveur la protection des données à caractère personnel. La perception de l'équilibre entre le droit à la protection des données à caractère personnel et les autres valeurs n'est pas toujours identique au point que la place du curseur entre ces différents droits peut être source de difficultés pour obtenir de la réglementation européenne qu'elle soit effective (A). Toutefois ces difficultés n'anéantissent pas complètement l'efficacité des principes défendus par la réglementation européenne en matière de protection des données à caractère personnel. Pour pouvoir être efficace, il suffit que la norme « produise l'effet recherché »[82]. Il s'agit plutôt ici d'examiner le résultat obtenu, et ce, qu'il l'ait été par l'effet de persuasion ou par l'exportation du modèle européen de protection des données (B).

A. L'obstacle du conflit de valeurs

Rien n'est plus difficile que d'attendre d'un État qu'il coopère alors que la législation extraterritoriale est incompatible avec les principes défendus dans l'État de nationalité de l'entreprise qui fait l'objet de la demande d'exécution. Bien que ne portant pas sur une question relative à la protection des données à caractère personnel, l'affaire récente *Google Inc. c. Equustek Solutions Inc.* illustre les

81 - B. Stern, *op. cit.*, p. 12 ; J. Bourguignon, *op. cit.*, p. 13.

82 - F. Rouvillois, « L'efficacité des normes », Fondation pour l'Innovation politique, Working paper, novembre 2006, disponible sur http://www.fondapol.org/wp-content/uploads/pdf/documents/Etude_Efficacite_des_normes.pdf [consulté en dernier lieu le 22 février 2018], p. 3.

points de vue divergents entre les juges canadien et américain[83]. La société Equustek a obtenu des juridictions canadiennes une injonction interlocutoire intimant Google à déréférencer sur toutes les extensions du moteur de recherche les sites Internet liés aux activités frauduleuses d'une troisième société, Datalink. Google qui avait déjà déréférencé tous les liens accessibles depuis Google.ca avait estimé que la portée extraterritoriale de l'injonction soulevait des questions relatives à la liberté d'expression, qui selon la société « aurait dû faire pencher la balance contre l'octroi de l'ordonnance [d'injonction interlocutoire] »[84]. La Cour Suprême du Canada, de son côté, a rejeté les arguments fondés sur l'atteinte portée à la liberté d'expression pour plusieurs motifs. D'une part « [l]'Internet n'a pas de frontières – son habitat naturel est mondial [et en conséquence] [l]a seule façon de s'assurer que l'injonction interlocutoire atteint son objectif est de la faire appliquer là où Google exerce ses activités, c'est-à-dire mondialement »[85]. D'autre part, pour les juges canadiens, le moteur de recherche américain n'a pas apporté la preuve démontrant que « pour se conformer à [cette] injonction, elle doit [...] porter atteinte à la liberté d'expression »[86]. En tout état de cause, si l'atteinte était établie, elle dispose de la possibilité de demander la modification de l'ordonnance devant les juridictions canadiennes[87]. La société Google a alors décidé de soumettre une demande devant la Cour de district fédérale de Californie du Nord,

83 - Cour Suprême du Canada, *Google Inc. c. Equustek Solutions Inc.*, 28 juin 2017, *RCS*, vol. 1, 2017, p. 824. Equustek Solutions Inc. (ci-après Equustek) avait au départ agi en 2011 contre Datalink, lequel agissait comme distributeur de ses produits : la première société accusait entre-autres la seconde d'avoir réétiqueté un de ceux-ci et à le faire passer pour le sien. Equustek avait obtenu une injonction en vertu de laquelle Datalink devait cesser d'exercer des activités sur tout site Web. Contournant l'ordonnance de la juridiction canadienne, Datalink a déménagé en dehors du Canada et a continué à exercer ses activités frauduleuses. Equustek a alors demandé à Google de délister les sites Web de Datalink, mais s'est heurté à un refus de ce dernier, à moins que la société canadienne n'obtienne des juridictions canadiennes une injonction intimant à Datalink de cesser ses activités sur tout site Web ; ce qu'elle obtiendra un peu plus tard. Google avait alors exécuté partiellement la demande de la société canadienne, limitant le déréférencement des pages Web à Google.ca. Estimant cette action inefficace, d'autant plus que Datalink avait déplacé le contenu litigieux vers de nouveaux sites Web, Equustek a obtenu des juridictions canadiennes une injonction à l'encontre de Google visant à interdire le moteur de recherche d'afficher tous les sites liés aux activités de Datalink.

84 - Cour Suprême du Canada, *Google Inc. c. Equustek Solutions Inc.*, *op. cit.*, p. 840, § 27.

85 - *Ibid.*, pp. 845-846, § 41.

86 - *Ibid.*, p. 847, §§ 45-46.

87 - *Ibid.*

afin d'empêcher l'exécution de l'injonction canadienne à toutes les extensions.

Les arguments qui avaient été invoqués en vain devant la juridiction canadienne ont reçu un accueil plus favorable par la Cour américaine. En particulier, Google s'est prévalu du droit à la liberté d'expression formulée dans le premier amendement de la Constitution américaine et de l'immunité qui lui est offerte par la Section 230 du *Communications Decency Act* qui « immunizes providers of interative computer services against liability arising from content created by third parties »[88]. La Section 230 avait été adoptée pour encourager « the unfettered and unregulated development of free speech on the Internet » et parce que « free speech on the Internet would be serverely restricted if websites were to face tort liability for hosting user-generated content »[89]. Or, pour la Cour américaine, l'application de l'injonction prive Google du bénéfice de l'immunité accordée par la Section 230[90]. Elle a ainsi prononcé, sans juger nécessaire de se prononcer sur la violation du premier amendement de la Constitution américaine, une suspension temporaire puis permanente de l'injonction canadienne[91].

L'injonction canadienne a, à nouveau, été l'objet d'une action devant les juridictions canadiennes. Les représentants de la société Datalink ont demandé à la Cour suprême de la Colombie-Britannique une modification de l'ordonnance[92]. Google, Google, qui n'était pas partie

88 - Section 230, *Communications Decency Act*, 47 *USC*, adopté le 1er février 1996, disponible sur https://www.law.cornell.edu/uscode/text/47/230 [consulté en dernier lieu le 20 septembre 2018].

89 - USDC, Northern District of California, San Jose Division, *Google LLC v. Equustek Solutions et al.*, 2 novembre 2017, Case N° 5 :17-cv-04207-EJD, disponible sur https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2589&context=historical [consulté en dernier lieu le 20 septembre 2018] ; Voir également US Court of Appeals, Ninth Circuit, *Batzel v. Smith*, 333 F.3d 1018, p. 1027.

90 - USDC, Northern District of California, San Jose Division, *Google LLC v. Equustek Solutions et al.*, 2 novembre 2017, préc.

91 - *Ibid.* ; pour la suspension permanente, voir USDC, Northern District of California, San Jose Division, *Google LLC v. Equustek Solutions et al.*, 14 novembre 2017, Case N° 5 :17-cv-04207-EJD, disponible sur https://casetext.com/case/google-llc-v-equustek-solutions-inc [consulté en dernier lieu le 20 septembre 2018].

92 - Cour Suprême de la Colombie-Britannique, *Equustek Solutions Inc., Robert Angus, and Clarma Enterprises. Ltd c. Datalink Technology Gateways Inc. et al.*, 16 avril 2018, 2018 BCSC 610, disponible sur https://www.canlii.org/en/bc/bcsc/doc/2018/2018bcsc610/2018bcsc610.html [consulté en dernier lieu le 20 septembre 2018].

à l'affaire, mais était néanmoins présent pour soutenir les arguments de Datalink, a réaffirmé que l'injonction porte atteinte à la liberté d'expression, à l'appui de la décision de la juridiction américaine[93]. L'argument n'a toutefois pas convaincu le juge canadien selon lequel « there is no suggestion that any U.S. law prohibits Google from de-indexing those websites, either in compliance with the injonction or for any other reason ». La décision canadienne repose sur le fait que le juge américain ne s'est pas prononcé sur la question de la violation de la liberté d'expression, mais uniquement sur la restriction de l'immunité, octroyée par la Section 230. La confusion de Google réside dans le fait que l'une des raisons qui ont justifié l'adoption de ce texte est la protection de la liberté d'expression. Toutefois, ainsi que l'a souligné le juge canadien, « Google has not demonstrated that the injunction violates core American values. [...] [R]ights guaranteed by the First Amendment can be regarded as core values, but [the District Court] expressly declined to rule on Google's submissions that its First Amendment rights were violated by the injunction »[94]. Bien que le refus de la Cour américaine de donner effet à l'injonction canadienne sur le territoire américain ne soit pas fondé sur une violation du premier amendement de la Constitution américaine, il semble à notre sens que, contrairement à ce qu'affirme le juge canadien, le refus de se prononcer sur cette question tienne davantage de l'économie de moyens que de l'absence de violation. En réalité, la Cour a jugé qu'il n'était pas nécessaire de se prononcer sur la méconnaissance de cet amendement dans la mesure où elle avait déjà reconnu un motif suffisant pour suspendre l'injonction canadienne.

En matière de protection des données, le litige qui a opposé Google aux autorités européennes de protection des données au sujet de l'application du droit au déréférencement à toutes les extensions de la société illustre parfaitement l'incompatibilité des valeurs défendues. Après l'affaire *Google Spain*, la société américaine avait décidé de limiter la désindexation des résultats des recherches qu'aux versions européennes du moteur de

93 - *Ibid.*, § 12.

94 - *Ibid.*, § 21.

recherche[95]. Toutefois le G29 avait rappelé que les propos de la Cour dans l'affaire *Google Spain* devaient s'entendre de manière à ce que le droit au déréférencement soit effectif « on all relevant domains, including .com »[96]. La position du G29, semblant exclure toute alternative à un déréférencement mondial[97], a fait l'objet de nombreuses inquiétudes, parmi lesquelles le fait que l'Union européenne impose ses valeurs aux États tiers[98], alors même que « each State is free to decide how to balance privacy with [other liberties] »[99]. Ainsi aux États-Unis, après la publication de l'affaire *Google Spain*, et la reconnaissance du droit au déréférencement d'informations indexées par les moteurs de recherche, de nombreux universitaires américains soulèvent une incompatibilité entre la liberté d'expression, protégée par le premier amendement de la

95 - L. Abboud, J. Fioretti, « Europe debates how far to push "right to be forgotten" », *Reuters*, publié le 25 juillet 2014, disponible sur https://www.reuters.com/article/google-eu-privacy/europe-debates-how-far-to-push-right-to-be-forgotten-idUSL6N0Q02JR20140725 [consulté en dernier lieu le 22 février 2018].

96 - Groupe de travail « Article 29 », Lignes directrices sur la mise en œuvre de l'arrêt de la Cour de justice de l'Union européenne *Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, adoptées le 26 novembre 2014,WP 225, p. 3.

97 - La position du Groupe de Travail est sans appel : l'approche de Google fondée sur l'extension est inappropriée pour l'application du droit au déréférencement. Par ailleurs le vocabulaire employé par le Groupe de travail suggère que la seule solution satisfaisante est un déréférencement général. Certains auteurs ont suggéré d'autres approches qui pourraient selon eux satisfaire aux standards de la protection des données sans pour autant porter une atteinte excessive à la liberté d'expression. Voir en ce sens, B. Van Alsenoy, M. Koekkoek , « Internet and Jurisdiction after *Google Spain* : the Extra-Territorial Reach of the EU's "Right to Be Forgotten" », Ku Leuven, Leven Centre for Global Governance Studies, Working Paper n° 152, Mars 2015, disponible sur https://ghum.kuleuven.be/ggs/publications/working_papers/2015/152vanalsenoykoekkoek [consulté en dernier lieu le 22 février 2018], pp. 17-23.

98 - Voir par exemple, D. Meyer, « Why the EU's "right to be delinked" should not go global », *Gigaom*, publié le 26 novembre 2014, disponible sur https://gigaom.com/2014/11/26/why-the-eus-right-to-be-de-linked-should-not-go-global/ [consulté en dernier lieu le 22 février 2018] ; Voir le billet déjà mentionné du directeur juridique de Google, K. Walker, « Defending access to lawful information at Europe's highest court » : « We — and a wide range of human rights and media organizations, and others, like Wikimedia — believe that this runs contrary to the basic principles of international law : no one country should be able to impose its rules on the citizens of another country, especially when it comes to linking to lawful content. Adopting such a rule would encourage other countries, including less democratic regimes, to try to impose their values on citizens in the rest of the world ». Ce billet fait suite à la saisine de la Cour de justice de l'Union européenne par le Conseil d'État français d'une question préjudicielle : le Conseil d'État interroge la Cour sur le fait de savoir si le droit au déréférencement doit s'étendre aux extensions étrangères de Google, *in* Conseil d'État, 10ème et 9ème Chambres réunies, 19 juillet 2017, n° 399922.

99 - B. Van Alsenoy, M. Koekkoek, *op. cit.*, p. 6.

Constitution américaine, et la législation européenne en matière de protection des données à caractère personnel[100]. Les États-Unis craignent que l'application extraterritoriale de la réglementation européenne en matière de protection des données et en particulier d'un droit au déréférencement « mondial » produise un *chilling effect*[101]. Le *chilling effect* traduit le risque de débordement d'une règle qui vise au départ un contenu illicite vers des contenus licites. L'une des conséquences de ce phénomène est de tendre vers l'autocensure. Winston Maxwell résume les conséquences sur la liberté d'expression en ayant recours à la métaphore de la marmite d'eau bouillante. Cette dernière représente le « marché des idées ». Selon l'auteur, « tout règlement de l'État qui tend à contraindre les moyens d'expression des citoyens entraîne une baisse de température de la marmite en créant un effet réfrigérant sur le marché des idées »[102]. La conséquence directe étant celle de l'appauvrissement du marché des idées[103]. Dès lors, compte tenu de

100 - E. Lee, « The Right to Be Forgotten v. Free Speech », *Journal of Law and Policy for the Information Society*, vol. 12, n° 1, 2015, p. 91. B. Van Alsenoy, M. Koekkoek, *op. cit.*, p. 15 ; Les médias américains ont parfois été bien plus alarmistes : voir par exemple les propos de James L. Gattuso, *in* « Europe's Latest Export : Internet Censorship », *Wall Street Journal*, publié le 11 août 2015, disponible sur https://www.wsj.com/articles/europes-latest-export-Internet-censorship-1439333404 [consulté en dernier lieu le 22 février 2018] : « If Google is forced to comply with the EU rules globally, the result would be unprecedented censorship of Internet content worldwide, as well as a dangerous expansion of foreign regulators' control over what Americans can see on the Web ». De manière plus générale, l'articulation entre la protection de la vie privée et la liberté d'expression a toujours été malaisée. En ce sens, Chris Reed reconnait que « even a cursory examination of the two human rights which are most affected by Internet communications – privacy and free speech – reveals that these rights themselves are potentially conflicting », *in* C. Reed, *op. cit.*, p. 256. Voir également les travaux de B. Van Alsenoy, A. Kuczerawy, J. Ausloos, « Search Engines after Google Spain : Internet@liberty or privacy@peril ? », ICRI Working Paper Series, KU Leuven, disponible sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494 [consulté en dernier lieu le 22 février 2018], pp. 51-58.

101 - W.J. Maxwell, « La France dans la transformation numérique : quelle protection des droits fondamentaux ? », commentaires publiés du colloque organisé par le Conseil d'État le 6 février 2015, *in La Documentation française*, n° 16, 2016, p. 119.

102 - *Ibid.*

103 - C'est précisément l'argument qui est avancé par l'avocat général M. Szpunar dans ses conclusions pour la demande de décision préjudicielle formée par le Conseil d'État à l'égard de la CJUE (*Google LLC c. CNIL*, C-507/17, § 61). L'avocat général a alerté du danger qu'une application mondiale du droit au déréférencement pourrait emporter : autoriser un déréférencement à l'échelle mondiale enverrait selon lui « un signal fatal [...] aux pays tiers, lesquels pourraient ordonner également un déréférencement en vertu de leurs propres lois ». Le risque est donc celui d'un « nivellement vers le bas » au détriment du droit d'accès à l'information et de la liberté d'expression.

la place accordée à la protection des données aux États-Unis, moins importante que celle que l'on attribue dans l'Union européenne, et au contraire de l'importance reconnue à la liberté d'expression[104], la coopération des États-Unis pour l'exécution d'une décision d'une juridiction européenne doit certainement être exclue.

B. De l'effet de persuasion à l'exportation du modèle européen en matière de protection des données

Si les controverses quant aux effets extraterritoriaux et ces conflits de valeurs opposent une barrière à l'efficacité complète de ces normes, elles n'en sont pas moins dénuées de tout effet. Les juges étatiques en ont pris conscience et ont souhaité tenir compte des vues des différentes législations y compris la réglementation européenne en protection des données. Pour paraphraser Cédric Ryngaert, « [g]iven the plurality of values in international society, [...] [a] [...] promising avenue is for domestic or regional law enforcement agencies and courts to give due regard to rival views of foreign affected persons and states, for example, through broad-based consultations or *amicus curiae* briefs »[105]. Quelques décisions canadiennes illustrent cet aspect de l'application extraterritoriale d'une loi nationale. Avant de rendre sa décision dans l'affaire *Globe24h.com*, le juge canadien s'était interrogé sur l'opportunité de cette décision et en particulier sur la possibilité que la décision produise les effets qu'elle vise. En effet, le site est domicilié en Roumanie et le juge reconnait avoir « des réserves au sujet de la force exécutoire de toute ordonnance émise contre le défendeur, étant donné que celui-ci et son serveur ne sont pas présents physiquement au Canada »[106]. Pour autant, le juge décide finalement de rendre la décision dans la mesure où sans qu'il soit certain de l'exécution de cette décision, cette décision pourrait persuader les juges roumains de rendre une décision favorable au requérant ou tout au moins dissuader l'entreprise contrevenante de poursuivre le comportement litigieux. En effet le juge estime que « l'émission d'une ordonnance de mesure corrective au Canada peut

104 - C. Reed, *op. cit.*, pp. 258-259.

105 - C. Ryngaert, « Guest Editorial. Symposium Issue on Extraterritoriality and EU Data Protection », *op. cit.*, p. 223.

106 - Cour fédérale (Canada), Ontario, *A.T. c. Globe24h.com. et le Commissaire à la protection de la vie privée du Canada*, 30 janvier 2017, *Documents Can LII*, § 85.

aider le demandeur à poursuivre ses recours en Roumanie. En outre [...] une telle ordonnance peut aider à persuader les exploitants de moteurs de recherche à désindexer les pages affichées sur le site Web du défendeur »[107].

Le juge canadien ne cherche pas tant à justifier la licéité ni même l'opportunité du caractère extraterritorial de la réglementation canadienne en matière de protection des données à caractère personnel. Surtout, il reste conscient que l'exécution de cette norme dépend du bon vouloir du juge roumain. L'efficacité de la norme extraterritoriale tient alors plus du pouvoir de persuasion des juges appliquant la loi extraterritoriale et de dissuasion des entreprises de violer la norme, qu'à l'exécution véritable du jugement.

Dans le même ordre d'idées, certains auteurs soutiennent que l'utilité des normes extraterritoriales ne dépend pas nécessairement de l'exécution de la norme. Les raisons invoquées pour justifier des prétentions extraterritoriales malgré les difficultés rencontrées pour l'exécution de ces normes peuvent être résumées par la valeur symbolique de ces normes : plutôt que d'essayer d'obtenir des juges du for, l'exécution de la norme étrangère, les prétentions extraterritoriales produisent au moins un effet dissuasif à l'égard des sociétés « at least if we assume that companies generally prefer not to violate any laws »[108]. Pour paraphraser Uta Kohl, « [i]t is enforceability that really matters, not actual enforcement »[109]. L'effet de la norme extraterritoriale se matérialise davantage dans la légitimité de la norme étrangère que dans la menace d'une potentielle sanction prononcée par le juge du for qui appliquerait la loi étrangère. Cette légitimité dépendrait dès lors du caractère « morally justifiable » de la réglementation. Dan Jerker B. Svantesson explique qu'il serait délicat pour une société de refuser de se conformer à une règle moralement justifiable, sans que cela n'affecte l'image de cette

107 - *Ibid.*

108 - D.J.B. Svantesson, « Extraterritoriality and Targeting in EU Data Privacy Law : the Weak Spot Undermining the Regulation », *International Data Privacy Law*, vol. 5, n° 4, 2015, p. 233.

109 - U. Kohl, *Jurisdiction and the Internet – Regulatory Competence over Online Activity – Regulatory Competence in the Online World*, Cambridge Univ. Press, 2007, p. 205.

société à l'égard du marché que cette dernière souhaite conquérir[110]. Sans doute est-ce la raison pour laquelle Yahoo ! Inc. a modifié ses conditions générales concernant la vente d'objets nazis après la décision rendue par les juges français[111]. Ainsi expliqué, « [s]uccess in the market, particularly the online market, demands respectability and respectability demands respect for the law »[112].

A contrario, une norme extraterritoriale qui ne serait pas justifiée moralement a peu de chances de succès à l'étranger dans la mesure où elle perdrait tout son caractère dissuasif sur les sociétés qu'elle vise. À la lumière de ces éléments, la réglementation européenne ne pourrait produire des effets sur le territoire d'États tiers que dans la mesure où les principes qui y sont posés se justifient moralement : ainsi, la légitimité de l'exigence du consentement de l'article 6 du règlement pourrait être difficilement contestable quand, au contraire, on pourrait émettre plus de doute concernant l'obligation de désigner un délégué à la protection des données formulée à l'article 37 du règlement[113].

Un autre effet, plus inattendu de la norme extraterritoriale est celui de l'exportation du modèle européen. La norme européenne ne s'appliquerait plus en tant que telle ; les États tiers auraient en effet cherché à modifier leur propre législation pour la rapprocher de la réglementation européenne. L'objectif est clairement affiché : celui de neutraliser l'application extraterritoriale de la réglementation européenne. Dans la décision *Globe24h.com* mentionnée auparavant, le juge canadien reconnaissait que la législation canadienne avait été

« conçue afin de s'intégrer à un système international visant à protéger la vie privée des personnes, comme en témoigne la directive européenne sur la protection des données adoptée en

110 - D.J.B. Svantesson, « Extraterritoriality and Targeting in EU Data Privacy Law : the Weak Spot Undermining the Regulation », *op. cit.*, p. 233 ; U. Kohl, *op. cit.*, p. 208.

111 - Bien que la société prétende le contraire. Sans doute la décision française a accéléré la modification des règles concernant la vente de ces objets. « Yahoo ! to stop auctions of Nazi memorabilia », *The Guardian*, publié le 3 janvier 2001, disponible sur https://www.theguardian.com/technology/2001/jan/03/Internetnews [consulté en dernier lieu le 22 février 2018].

112 - U. Kohl, *op. cit.*, p. 208.

113 - Dans ce sens, D.J.B. Svantesson, « Extraterritoriality and Targeting in EU Data Privacy Law : the Weak Spot Undermining the Regulation », *op. cit.*, p. 233.

octobre 1995. Entre autres, la directive européenne comprenait une disposition qui empêchait la transmission de renseignements personnels en dehors de l'Union européenne, à moins que le pays destinataire ne dispose d'une législation en vigueur qui offrirait une protection similaire. La [Loi sur la protection des renseignements personnels et les documents électroniques] visait à offrir cette protection au Canada afin d'éviter que ce dernier ne soit concerné par la portée extraterritoriale de la directive européenne »[114].

Par l'application du principe *non bis in idem*, il ne serait plus possible pour les juridictions de poursuivre pour la même violation dès lors que le litige aurait été porté en premier lieu devant les juridictions d'un autre État[115]. Le résultat est alors très proche de celui recherché par l'application effective de la réglementation européenne. Cette méthode n'est toutefois appropriée que pour les États qui partagent des positions similaires avec celle de l'Union européenne. La convergence de législations est d'autant plus accentuée qu'elle est « provoquée » sous l'effet des articles 25 de la directive[116] et 45 du règlement[117]. Au regard de ces dispositions, le transfert des données dans un État tiers n'est autorisé que si ce dernier assure « un niveau de protection adéquat ». Dès lors, pour pouvoir opérer un transfert des données en dehors du territoire européen, l'État étranger n'a d'autre choix que celui de modifier sa législation. À titre d'illustration, la Commission européenne a décidé d'entamer en 2017 des négociations avec le Japon et la Corée

114 - Cour fédérale (Canada), Ontario, *A.T. c. Globe24h.com. et le Commissaire à la protection de la vie privée du Canada*, préc., § 49.

115 - R. Bismuth, *op. cit.*, p. 799 ; Pour une définition du principe, voir également A. Lobry, « De la "convergence" des jurisprudences de la CJUE et de la CEDH : l'élaboration d'une définition commune du principe *ne bis in idem* », Geneva Jean Monnet Working Paper, n° 25/2016, disponible sur https://www.ceje.ch/files/8514/7377/3116/Couverture_25.pdf [consulté en dernier lieu le 22 février 2018].

116 - Directive 95/46/CE, préc., Article 25 : « 1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat. [...] ».

117 - Règlement (UE) 2016/679, préc., Article 45 : « 1. Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. [...] ».

qui ont récemment adopté ou modernisé leur législation en matière de protection des données[118]. La Commission a déjà reconnu le caractère adéquat des législations de plusieurs États tels que la Suisse, l'Argentine, Israël, la Nouvelle-Zélande et l'Uruguay. Sans être identiques à la réglementation européenne, la Commission a considéré que ces systèmes de protection des données assuraient un niveau de protection comparable à celui garanti au sein de l'Union[119]. En d'autres termes, d'un côté les États tiers qui souhaitent court-circuiter la portée extraterritoriale de la réglementation européenne, à l'instar du Canada[120], peuvent en neutraliser les effets par l'adoption d'une nouvelle réglementation et de l'autre l'application des législations « adéquates » devrait obtenir un résultat similaire à celui recherché par la réglementation européenne. C'est précisément en ce sens que la réglementation européenne devient efficace.

En somme, compte tenu du choix des critères retenus quant à l'application *ratione loci* du règlement nul doute que la portée extraterritoriale du règlement européen sera davantage contestée que ne l'était celle de la directive. Toutefois, si la lecture de ces critères par la Cour de justice converge avec celle, affinée, du G29, et si les entreprises étrangères restent les seuls auteurs des différentes oppositions à l'application du texte européen, le rattachement territorial formulé à l'article 4 du règlement devrait suffire à fonder la portée extraterritoriale de cette dernière. Les contestataires devraient être néanmoins rassurés : l'effectivité de la réglementation européenne est limitée en ce qu'elle est fonction de la coopération des États étrangers. L'efficacité du règlement ne devrait toutefois pas être inexistante : la volonté de neutraliser la portée extraterritoriale du texte européen devrait paradoxalement lui permettre de réaliser les effets recherchés.

118 - Commission européenne, Communication de la Commission au Parlement européen et au Conseil – Échange et protection de données à caractère personnel à l'ère de la mondialisation, le 10 janvier 2017, disponible sur http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-7-F1-FR-MAIN-PART-1.PDF [consulté en dernier lieu le 22 février 2018], p. 8.

119 - *Ibid.*, p. 7.

120 - La Commission européenne a d'ailleurs constaté une adéquation partielle avec la législation du Canada : « La décision relative au Canada s'applique uniquement aux entités privées relevant de la loi canadienne sur la protection des renseignements personnels et les documents électroniques », *in ibid.*, p. 7.

DEUXIÈME PARTIE :

APPROCHE SECTORIELLE

LA GOUVERNANCE DES DONNÉES PERSONNELLES DANS LA BANQUE

Aurélie Banck
Juriste
Responsable pédagogique du DU Data Protection Officer, Université Paris Nanterre
Co-auteur du Vade-mecum de la protection des données personnelles pour le secteur bancaire et financier, Essentiel de la banque et de la Finance, 2018.

Le Règlement Général sur la Protection des Données Personnelles (RGPD) adopté le 27 avril 2016 et applicable depuis le 25 Mai 2018 constitue un vrai changement de paradigme en matière de régulation de la protection des données. Il impose, en effet, de passer d'un régime de formalités préalables – administratif - à un principe de responsabilité globale de l'ensemble des acteurs impliqués dans la chaine de traitement des données. Les entreprises du secteur bancaire comme l'ensemble des secteurs d'activités vont donc devoir passer d'une approche statique à une approche dynamique, pour être en mesure de démontrer à tout moment qu'elles respectent les dispositions du Règlement, conformément au principe d'*accountability*. Ce principe s'accompagne de la consécration d'une approche par les risques, les mesures techniques et organisationnelles à mettre en place en matière de protection des données personnelles devant être adaptées au niveau de risque présenté par le traitement pour les droits et libertés des personnes concernées.

Les établissements bancaires et financiers sont pleinement impactés par cette réglementation. Ils collectent effectivement de nombreuses données à caractère personnel, c'est-à-dire de données permettant d'identifier directement ou indirectement, par référence à un numéro d'identification, une personne physique. Cette collecte est continue, pendant toute la durée de la relation contractuelle, qu'il s'agisse de procéder à l'identification du client conformément aux dispositions applicables en matière de lutte contre le blanchiment d'argent ou le financement du terrorisme, d'évaluer son appétence aux risques pour lui proposer tel ou tel produit financier, ou sa solvabilité dans le cadre d'une demande de crédit en passant par les informations

que la banque peut déduire des données de transactions. En outre, elle est accrue par le phénomène de digitalisation des banques.

Ces données sont couvertes par le secret bancaire[1], mais elles ne font pas partie des catégories particulières de données listées aux articles 9 et 10 du RGPD imposant un niveau de protection supplémentaire. Elles ont cependant un caractère sensible au sens commun du terme, étant considérées comme particulièrement confidentielles par les clients[2]. Le Groupe des CNIL européennes les a, ainsi, qualifiés de « données hautement personnelles » « dans la mesure où leur violation aurait clairement des incidences graves sur la vie quotidienne de la personne concernée »[3]. Les données collectées et traitées par les établissements financiers ne sont donc pas neutres. Le RGPD responsabilise l'ensemble des entités intervenant dans le cadre du traitement de ces données : le responsable du traitement, c'est-à-dire l'entité qui en définit les finalités et les moyens, mais également les sous-traitants, qui agissent au nom et pour le compte de ces responsables. Les sous-traitants sont désormais investis d'une responsabilité en propre. Enfin, le RGPD permet de mettre en place des co-responsabilités de traitement. Les Groupes bancaires, polymorphes, souvent composés de filiales et de succursales dont les rapports peuvent être très imbriqués. Dès lors, il apparait nécessaire de délimiter les responsabilités de chaque entité du Groupe. Le tout dans un contexte d'augmentation exponentielle du montant des sanctions qui pour une entreprise peut aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

À cela s'ajoute une concurrence féroce d'acteurs non régulés comme les réseaux sociaux ou moins régulés comme les prestataires de service d'information sur les comptes et la multiplication des normes relatives aux données. L'ensemble de ces facteurs incitent

1 - Même si la portée du secret bancaire s'est amoindrie ces dernières années notamment dans le cadre de la lutte contre la fraude fiscale.

2 - CSA, *La protection des données personnelles*, septembre 2017, étude n°1700780 réalisée auprès d'un échantillon de 1002 Français âgés de 18 ans et plus, interrogés du 28 au 30 août 2017.

3 - *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) 2016/69*, *Working paper* 248, rev.01, modifiées et adoptées le 4 octobre 2017.

les établissements financiers à s'interroger sur la gouvernance des données dans la banque. En matière de données personnelles, la mise en place de cette gouvernance s'articule autour d'un acteur le Délégué à la protection des données (I), nécessite de s'interroger sur l'adhésion au mécanisme du *one stop shop* (II) et de procéder à une allocation des responsabilités au sein des Groupes bancaires (III).

§1 : Le Délégué à la protection des données

La modification de la loi Informatique et Libertés en 2004 suite à la transposition de la Directive 95/46/CE avait introduit dans le droit français la fonction de Correspondant à la protection des données à caractère personnel ou Correspondant Informatique et Libertés (CIL). Cette désignation facultative, donnant lieu à une notification de l'autorité de contrôle, était laissée au choix du responsable de traitement. Le texte prévoyait la possibilité de désigner un collaborateur en interne, c'est-à-dire d'un personnel du responsable de traitement ou en externe via un contrat de prestation de service, cette faculté n'était cependant applicable que lorsque moins de cinquante personnes étaient chargées de la mise en œuvre ou avait directement accès aux traitements.

En échange, le responsable de traitement ayant désigné un CIL bénéficiait d'un allégement des formalités préalables à effectuer auprès de la CNIL. Ainsi, l'organisme était dispensé des formalités relevant de la déclaration (déclaration normale et engagement de conformité à une norme simplifiée) qui devaient être enregistrées dans un registre, tenu à la disposition de l'autorité de contrôle.

Sa principale mission était de veiller « au respect des obligations prévues par la loi du 6 janvier 1978 pour les traitements au titre desquels il a été désigné ». La compétence « naturelle » du CIL dépendait, en effet, de son périmètre de désignation stipulé dans la notification faite à l'autorité. Celui-ci pouvait être au choix du responsable de traitement restreint aux traitements relevant de la déclaration ou sa compétence pouvait être étendue à l'ensemble des traitements de l'organisme. À cette fin, il était investi d'un pouvoir général de recommandation, devant notamment être consulté, préalablement à la mise en œuvre des traitements appelés à figurer dans son registre.

Le correspondant devait « bénéfici[er] des qualités requises pour exercer ses missions ». Dans les faits, la CNIL ne procédait pas à un contrôle des compétences des CIL mais s'assurait qu'il ne soit pas dans une situation engendrant un conflit d'intérêts (notamment avec une fonction de responsable de traitement) et a mis en place un service dédié.

Fin 2016, 17 500 entreprises avaient désigné un CIL[4] ; cette mission venant généralement en plus d'une autre comme de celle de responsable de la conformité. En outre, les banques avaient majoritairement choisi de ne pas en désigner. Ce rôle apparaissait donc bien plus comme une mission, que comme une fonction à part entière.La transposition de la Directive 95/46/CE dans les différents États membres a été réalisée de manière très hétérogène, y compris en ce qui concerne le statut et les missions du Cil. Celui-ci était par exemple obligatoire en Allemagne. Le Règlement qui vise à remédier à cette fragmentation législative crée la fonction de Délégué à la protection des données ou Data Protection Officer (DPO) et la rend obligatoire dans certains cas.

L'article 37 du RGPD fixe trois cas dans lesquels un responsable du traitement ou un sous-traitant doit procéder à cette nomination. Ainsi, un DPO doit être désigné lorsque :

- « Le traitement est effectué par une autorité publique ou un organisme public » (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle)

- « Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou

- Les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de

4 - http://www.archimag.com/univers-data/2017/06/09/donnees-personnelles-correspondant-informatique-libertes-delegue-protection

> données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».

La désignation d'un DPO n'est donc systématique ; il est toutefois toujours possible de désigner un DPO à titre facultatif. Il sera, dans ce cas, investi des mêmes missions (cf. infra) que le DPO relevant des dispositions de l'article 37.

Dès lors, qu'en est-il des établissements financiers ? Face à des critères assez imprécis notamment la notion d' « activité de base du responsable de traitement ou du sous-traitant » ou celle de « traitement à grande échelle », le G29, devenu le 25 mai le Comité européen à la protection des données (CEPD), a émis des lignes directrices afin d'aider à l'interprétation du texte. Les traitements de données de clients effectués par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités figurent parmi les exemples de traitements à grande échelle[5]. Les opérations de « profilage et [de] notation à des fins d'évaluation des risques (par exemple aux fins de l'évaluation du risque de crédit, (...] de la prévention de la fraude ou de la détection du blanchiment d'argent) » sont également citées au titre des traitements comportant un suivi régulier et systématique des personnes concernées. La nomination d'un DPO par les banques semble donc inévitable, les traitements cités par le CEPD étant inhérents à une activité bancaire de base. Cette désignation peut être effectuée en interne ou en externe, via un contrat de prestation de service, le RGPD ne fixant pas de limites pour ce type de désignation. L'internalisation ou l'externalisation est un choix stratégique de l'organisme qui dépend de nombreux critères comme de son organisation et de sa culture, du volume de problématiques à traiter nécessitant la mise en place de moyens proportionnés, etc. Les particularités du secteur bancaire et financier, notamment son caractère ultra-réglementé, obligeant le DPO à jongler entre la réglementation relative à la protection des données et les réglementations sectorielles, et la concurrence accrue entre les différents acteurs du marché, plaident plutôt en faveur d'un DPO internalisé, en particulier pour les grands Groupes, une externalisation pouvant être envisagée pour de plus petits établissements.

5 - *Lignes directrices concernant les délégués à la protection des données (DPD)*, *Working Paper* 243, version révisée et adoptée le 5 avril 2017.

Les missions du DPO sont détaillées à l'article 39 du RGPD. Le DPO est investi d'une mission générale de conseil du responsable de traitement ainsi que de ses employés quant aux obligations qui leur incombent en vertu du Règlement , ais également des autres dispositions du droit de l'UE ou du droit des États membres en matière de protection des données. Ce périmètre apparaît particulièrement large, obligeant le DPO à être quasi omniscient en matière de législation relative à la protection des données pour l'ensemble des lieux d'établissement du responsable de traitement ou du sous-traitant, ce qui semble particulièrement difficile.

Il doit également contrôler le respect du Règlement, des autres dispositions (cf. supra) et des règles internes mises en place par l'organisme « en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ». Il dispense des conseils « sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 » et fait office de point de contact pour l'autorité de contrôle et pour les personnes concernées. La mission du DPO est donc complétée par rapport à celle du CIL qui se limitait à une mission de conseil ; le DPO est, en effet, investi d'une mission de contrôle, incitant certains à la comparaison avec la fonction de commissaire aux comptes. Le responsable du traitement ou le sous-traitant doit veiller à ce que le DPO soit « associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ». L'organisme a donc également des obligations vis-à-vis de son délégué. Attention, s'il est le « chef d'orchestre de la conformité », il ne se substitue pas au responsable du traitement ou au sous-traitant, qui assume la responsabilité du traitement mis en œuvre et peut voir sa responsabilité engagée.

Le DPO « fait directement rapport au niveau le plus élevé de la direction » de l'établissement[6]. Dès lors, il convient de trouver un positionnement permettant de garantir son indépendance et de nature à éviter les conflits d'intérêts. Il peut dépendre directement du

6 - Article 38, §3 du RGPD.

secrétariat général ou d'une Direction support comme la Direction juridique ou de la Conformité. Les nouveaux enjeux autour de la data propulsent le DPO au niveau stratégique de l'entreprise. La Société Générale a ainsi choisi de positionner son DPO à la conformité[7]. Le RGPD offre la possibilité à un groupe d'entreprises[8] de désigner un DPO unique, sous réserve qu'il puisse, en tant que point de contact des personnes concernées, être « facilement joignable »[9] depuis chaque lieu d'établissement, ce qui pose nécessairement la question de l'accessibilité. En effet, cela signifie que ce DPO Groupe doit pouvoir être sollicité et répondre aux personnes concernées dans leur langue, ce qui peut vite être assez compliqué, notamment au regard des délais prévus par le RGDP[10]. Il ne s'agit cependant que d'une faculté, l'évaluation de la pertinence de ce mode d'organisation est donc laissée à l'appréciation du responsable de traitement ou du sous-traitant. Plusieurs modes d'organisation de la fonction de DPO sont possibles : il peut être centralisé ou décentralisé. Il appartiendra à l'établissement de déterminer quel est le mode d'organisation le plus approprié en fonction de facteurs qui lui sont propres comme l'organisation déjà en place, la proportion de traitements transfrontaliers (cf. infra), des moyens alloués, etc. Ce choix dépendra également de la décision qui sera prise quant à l'adhésion ou non au mécanisme du *one stop shop* et de l'analyse du niveau de responsabilité des entités au sein du Groupe.

§2 : L'adhésion au mécanisme du *one stop shop*

Le Règlement s'inscrit dans une logique de simplification des règles relatives à la protection des données en Europe, notamment pour les Groupes installés dans plusieurs états membres. Jusqu'à l'entrée en application du RGPD, ces Groupes étaient susceptibles d'être réglementés par autant d'autorités de protection des données que de pays dans lesquels ils étaient installés. Afin d'alléger cette contrainte,

7 - https://www.societegenerale.com/fr/Societe-Generale-nomme-Antoine-Pichot-Delegue-a-la-Protection-des-Donnees.

8 - L'article 4, §19 du RGPD définit la notion de groupe d'entreprise comme « une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle ».

9 - Article 37, §2 du RGPD.

10 - L'article 12 prévoit désormais un délai d'un mois pour répondre aux sollicitations des personnes concernées, délai qui peut être porté à trois mois en raison de la complexité et du nombre de demandes.

la Commission européenne a proposé d'introduire un mécanisme de « guichet unique »[11]. Cette disposition a donné lieu à de longs débats dans le cadre du processus d'adoption du Règlement, les autorités craignant que l'introduction de ce mécanisme ne donne lieu à un forum shopping, c'est-à-dire à la sélection de l'autorité lead en fonction de son niveau de sévérité et ne « concentre la régulation entre les mains de quelques autorités » et que le citoyen soit privé de son droit à un recours dans son propre pays[12]. Les dispositions finales sont donc le fruit d'un compromis. L'article 56 du RGPD stipule que « l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file, concernant le traitement transfrontalier effectué par le Responsable du traitement ou le sous-traitant ». Il est donc possible de désigner une seule autorité compétente. Toutefois, force est de constater qu'une première limite à ce mécanisme apparait déjà. Cette autorité ne sera, en effet, compétente que pour les traitements transfrontaliers. Cette nouvelle catégorie de traitement est définie à l'article 4 du RGPD comme les traitements mis en œuvre dans :

- plusieurs États membres alors que le responsable du traitement ou le sous-traitant est établis dans plusieurs de ces États membres, et,

- un seul établissement, mais qui affectent sensiblement ou peuvent affecter des personnes concernées dans plusieurs États membres.

Cette définition soulève de nombreuses questions notamment s'agissant de la prise en compte des éventuelles spécificités locales. Ainsi pour être qualifié de transfrontalier, un traitement doit-il être déployé de la même manière dans l'ensemble des entités ? Ou certaines variations sont-elles possibles pour prendre en compte les règles locales (par exemple en Suède le numéro de sécurité sociale est utilisé couramment ce qui n'est pas le cas en France) ?

11 - Considérant 98 de la proposition de Règlement

12 - http://www.zdnet.fr/actualites/donnees-personnelles-le-guichet-unique-solution-d-impunite-pour-les-geants-du-web-39797493.htm.

En outre, l'article 55 du RGPD introduit une exception à ce principe. Il précise que « lorsque le traitement est effectué par des autorités publiques ou des organismes privés agissant sur la base de l'article 6, § 1, point c) (respect d'une obligation légale) ou e) (exécution d'une mission d'intérêt public), l'autorité de contrôle de l'État membre concerné est compétente. Dans ce cas, l'article 56 (concernant l'autorité chef de file) n'est pas applicable ». L'autorité de l'État membre d'établissement reste donc compétente pour réguler les traitements relatifs à l'exécution d'une mission de service public au respect d'une obligation légale quand bien même il s'agirait d'un traitement transfrontalier. Cette seconde limite au mécanisme du *one stop shop* apparaît particulièrement importante car les traitements visant à satisfaire une obligation légale, par exemple en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, sont très nombreux dans les banques. Le périmètre de compétence d'une autorité chef de file dans la banque apparait donc réduit par cette exception, alors même que le déploiement de traitements susceptibles d'être qualifiés de transfrontaliers en la matière est fréquent.

Enfin, la désignation de cette autorité n'a pas pour effet d'exclure complètement la compétence des autres autorités de protection des données qui restent compétentes pour traiter les « réclamations introduites auprès d'elle ou une éventuelle violation du présent règlement, si son objet concerne uniquement un établissement dans l'État membre dont elle relève ou affecte sensiblement des personnes concernées dans cet État membre uniquement »[13]. Dans l'hypothèse où l'organisme objet de la plainte aurait désigné une autorité chef de file, sa réception déclenche le mécanisme de contrôle de cohérence, obligeant l'autorité ayant réceptionné la plainte a sollicité l'autorité chef de file pour déterminer qui procédera à son traitement. Le souci d'offrir au citoyen la possibilité de défendre ses droits aisément en contactant directement son autorité locale a toutefois pour effet de poser une troisième limite au mécanisme du *one stop shop* et amoindri son intérêt.Une fois le périmètre des traitements pouvant relever du *one stop shop* identifié, il conviendra de déterminer quelle autorité peut être choisie comme autorité chef de file. Elle ne peut pas être choisie au hasard. Il doit s'agit de l'autorité du lieu de l'établissement principal du responsable du traitement ou du sous-

13 - Art 56, §2 du RGPD.

traitant, définie à l'article 4 du RGPD. Ainsi pour

- un responsable de traitement établi dans plusieurs États membres, il s'agit du « lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier [...] a[it] le pouvoir de faire appliquer ces décisions »

- un sous-traitant également établi dans plusieurs États membres, il s'agit du « lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement ».

La détermination de ce lieu d'établissement principal n'est pas sans poser de difficultés. Il doit s'agir du lieu de prise de décision effectif relatif aux traitements de données. Dans le cas des Groupes, le considérant 36 dispose que « Lorsque le traitement est effectué par un groupe d'entreprises, l'établissement principal de l'entreprise qui exerce le contrôle devrait être considéré comme étant l'établissement principal du groupe d'entreprises, excepté lorsque les finalités et les moyens du traitement sont déterminés par une autre entreprise ». Le fait que la maison mère ait la qualité d'autorité chef de file relève donc de la présomption simple qui pourra être renversée sur la base d'une analyse des modes de prise de décision.

Cette analyse réalisée « en fonction de critères objectifs »[14] devra donc résister à l'épreuve des faits et la simple volonté d'adhérer de ce mécanisme apparait insuffisante. Il doit s'agir d'une réalité opérationnelle et décisionnelle. Ainsi, dans sa décision du 21 janvier 2019[15], la formation restreinte de la Cnil relève que « pour être qualifié d'établissement principal, l'établissement concerné doit disposer d'un pouvoir de décision vis-à-vis des traitements de données à caractère personnel en cause. La qualité d'établissement

14 - Considérant 36.

15 - Délibération n°SAN 2019-001 du 21 janvier 2019.

principal suppose en effet l'exercice effectif et réel d'activités de gestion déterminant les décisions principales quant aux finalités et aux moyens du traitement ». Par conséquent, l'existence d'un établissement principal s'apprécie in concreto, au regard de critères objectifs comme le fait qu'il soit mentionné dans des règles de confidentialité ou la désignation d'un DPO. Dès lors, la mise en place du *one stop shop* peut nécessiter de revoir les process de prise de décision pour les centraliser au sein d'une même entité, susceptible, dès lors, de recevoir cette qualification.

La mise en place d'une gouvernance au sein d'un groupe nécessite également de déterminer la qualité de chacune des entités du Groupe.

§3 : La répartition des responsabilités au sein des groupes

Les établissements bancaires et financiers sont généralement polymorphes, avec des filiales et succursales dans plusieurs États membres et hors Union européenne. Ces différentes entités peuvent mutualiser des outils comme un outil de CRM, ou des centres de services (par exemple des capacités d'hébergement), voire même créer un centre de services partagés au sein du Groupe pour de mutualiser des ressources. Cette organisation s'inscrit dans une logique de rationalisation parfaitement légitime. Elle impose cependant de s'interroger et de déterminer la qualification juridique de chacune des entités au regard du RGPD afin de procéder à une allocation correcte des responsabilités en interne.

En matière de protection des données, on distingue le responsable du traitement qui définit les finalités, l'objectif poursuivi par le traitement, et les moyens qui doivent être mis en œuvre. À l'opposé, le sous-traitant agit au nom et pour le compte du responsable de traitement et sous son contrôle. Il n'est pas autorisé à utiliser les données qui lui sont confiées pour une autre finalité. Avant l'entrée en vigueur du RGPD, les sous-traitants n'avaient pas de responsabilité en propre. Les autorités de contrôle ne pouvaient donc pas engager leur responsabilité. Seuls les responsables de traitement pouvaient être sanctionnés, ce qui conduisait parfois à des situations où une entreprise se trouvait condamnée alors que tout ou partie du préjudice était imputable à son sous-traitant. Cette dernière disposait simplement d'une action récursoire à titre

contractuel à l'encontre de son sous-traitant, ce qui semble assez maigre au vu du préjudice d'image que peut générer une sanction de la CNIL. En outre, il était illusoire, avec le développement du Cloud computing et des services offerts par les GAFA[16], de croire que les responsables du traitement étaient toujours en mesure d'imposer à leurs sous-traitants les moyens, et en particulier les mesures de sécurité, mises en œuvre par leurs prestataires. Le RGPD met fin à cette « hypocrisie ». Les sous-traitants sont désormais investis d'une responsabilité autonome. Ils doivent respecter certaines obligations en propre[17] et dans le cadre de leur relation avec les responsables du traitement[18] dont ils traitent des données. Ils sont soumis aux mêmes procédures et aux mêmes sanctions que les responsables de traitements. Le RGPD instaure également des situations de responsabilité conjointe de traitement. L'article 26 du RGPD précise que « lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement ». Cette qualification juridique, non transposée en droit français jusqu'alors, vise à couvrir des cas dans lesquels deux responsables de traitement définissent ensemble les finalités et les moyens du traitement, dans des proportions qui ne sont pas nécessairement égalitaires. L'avis du G29 sur les notions de responsable du traitement et de sous-traitant[19] vient, en effet, préciser que « la participation des parties à la détermination conjointe peut revêtir différentes formes et n'est pas nécessairement partagée de manière égale ». Tous ces acteurs (responsables de traitement, sous-traitants et coresponsables) sont solidairement responsables du dommage subi par les personnes concernées devant les juridictions. L'article 82, §4 précise que « Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsqu' [...] ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-

16 - Google, Amazon, Facebook, Apple.

17 - L'obligation de tenir un registre, de désigner un DPO ou un représentant, de coopérer avec les autorités de contrôle.

18 - La notification des violations de données, l'obligation d'assurer la sécurité des données, les modalités de recours à un sous-traitant de 2nd rang, l'obligation d'assister le responsable de traitement dans différentes situations.

19 - *Avis n°1/2010 sur les notions de responsable du traitement et de sous-traitant*, adopté le 16 février 2010, *Working paper* 169.

traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective ». L'ensemble des parties est donc tenu responsable de l'intégralité du dommage. Le sous-traitant pourra s'exonérer de cette responsabilité s'il démontre qu'il a respecté les obligations qui lui incombent au titre du Règlement et qu'il a agi dans le cadre des instructions licites du responsable du traitement et conformément à celles-ci.

Cette nouvelle responsabilité impose donc de définir précisément les rôles et responsabilités de chacun au sein des Groupes bancaires qui sont généralement des environnements particulièrement complexes.

Le RGPD impose également une formalisation de ces relations. L'article 28 consacré à la sous-traitance dispose que « le traitement par un sous-traitant est régi par un contrat ou tout autre acte juridique du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement » et fixe une liste de mentions obligatoires. L'article 26 relatif aux responsables conjoints précise quant à lui que « Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement [...] par voie d'accord entre eux, sauf si [...] leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre ». Or, la formalisation de ces relations à l'intérieur du groupe est généralement problématique. La solution du contrat est surement la plus efficace. Elle n'est cependant pas toujours appropriée notamment pour des raisons culturelles et peut s'avérer particulièrement contraignante. En outre, il pourrait s'agir d'un moyen pour contingenter le montant des sanctions administratives.

Enfin, le RGPD est doté d'un effet extraterritorial. Il est non seulement applicable aux traitements réalisés par les organismes établis sur le territoire de l'Union européenne, mais également aux traitements de données relatifs à des personnes qui se trouvent sur le territoire de l'Union alors même que le responsable de traitement ou le sous-traitant n'y seraient pas établis si ces traitements visent à offrir des biens ou des services à des personnes concernées dans l'Union ou le suivi du comportement de ces personnes[20]. Les établissements

20 - Art. 3, §2 du RGPD.

bancaires ont souvent des entités hors UE, la question de la gouvernance des données personnelles au sein du Groupe impose donc de s'interroger sur le cas de ces filiales et de déterminer s'il convient ou non d'appliquer au sein du Groupe un seul programme de protection des données ou plusieurs.Stricto sensu le RGPD est applicable aux personnes situées sur le territoire européen et non aux citoyens ou aux résidents européens. Dès lors, la filiale brésilienne d'un établissement français ne serait pas tenue d'appliquer le RGPD sous réserve qu'elle ne vise pas le marché européen (ce qui est peu probable, l'établissement étant également installé en France) quand bien même elle traiterait des données de citoyens européens installés au Brésil (par exemple des expatriés). La solution serait bien entendu différente si cette filiale proposait des produits ou des services à des personnes situés sur le territoire européen via un site internet. Mais au-delà de ces strictes considérations juridiques, la définition et la mise en place d'une gouvernance de la protection des données au sein d'un Groupe peuvent parfois être simplifiées par le déploiement d'un standard unique, même s'il est mieux disant que certaines réglementations locales. Dupliquer différentes organisations peut s'avérer particulièrement compliqué à gérer. En outre, des outils conçus nativement pour respecter la vie privée sur le principe du *privacy by design*[21] le seront toujours, même s'ils sont déployés dans des pays n'imposant pas cette contrainte.La définition des rôles et responsabilités au sein des Groupes va influer sur le nombre de DPO et l'organisation de cette fonction. Le DPO doit être indépendant et à l'abri des conflits d'intérêts. Dès lors, il faut veiller à ce qu'un DPO Groupe ne se retrouve pas en situation de conflit d'intérêts dans l'hypothèse où il assumerait une fonction de DPO pour le compte de l'organe central et de ses filiales. En effet, si la maison mère met à disposition de ces filiales un outil et qu'un problème survient, il devra conseiller en même temps la maison mère et la filiale qui peuvent parfois avoir des intérêts divergents, situation qui semble délicate. Dans ce cas, il semblerait préférable de séparer les fonctions en désignant deux DPO au niveau central avec des périmètres différents ou des DPO en local.

21 - Principe de protection des données dès la conception qui vise à intégrer les principes de protection des données directement dans les outils et les applications traitant des données personnelles.

Conclusion

Le RGPD n'est pas le seul texte concernant les données applicable dans la banque. Les établissements financiers sont tenus au respect de multiples réglementations comme la norme BCBS 239[22], la directive sur les services de paiement 2[23], la directive NIS/SRI[24], les réglementations fiscales, etc. Le futur règlement *e-privacy* ainsi que le règlement relatif aux données non personnelles en date du 14 novembre 2018[25] devraient encore complexifier l'environnement réglementaire de la data dans les banques. Ce foisonnement impose d'adopter une approche transverse des sujets data afin d'assurer la cohérence des processus m, is également dans un souci de rationalisation des moyens. Les synergies à trouver sont nombreuses pour le DPO et apparaissent indispensables afin d'assurer la conformité de l'organisme à un coût maitrisé.

D'autres régulateurs pourraient également se saisir de ces sujets. La Banque de France et l'ANSSI sont, d'ores et déjà, destinataires des notifications des incidents de sécurité majeurs devant être notifiés dans le cadre de la DSP2[26] et les autorités de la concurrence s'intéressent aux acteurs du Big Data[27] qui, du fait des données massives qu'ils détiennent, pourraient acquérir une position dominante sur le marché. Les challenges inhérents à la gouvernance des données dans la banque sont donc nombreux.

---

22 - *Recommandations relatives au risque de crédit et à la comptabilisation des pertes de crédit attendues*, Comité de Bâle, décembre 2015 : http://www.bis.org/bcbs/publ/d350_fr.pdf.

23 - Directive n°2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, transposée par l'ordonnance n°2017-1252 du 9 août 2017.

24 - Directive n° 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union dite également directive NIS pour Network and Information Security.

25 - Règlement 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractères non personnel dans l'Union européenne.

26 - Directive n°2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

27 - "EU Asks: Does Control of Biga Data Kill Competition?», *The Wall Street Journal*, January 2th, 2018 https://www.wsj.com/articles/eu-competition-chief-tracks-how-companies-use-big-data-1514889000

LA PROTECTION DES DONNÉES PERSONNELLES EN ASSURANCE : DIALOGUE DU JURISTE AVEC L'ACTUAIRE[1]

Arthur Charpentier
Professeur de mathématiques à l'Université de Rennes
Delphine Cocteau-Senn
Maître de conférences en droit privé
à l'Université de Picardie - Jules Verne
Rodolphe Bigot
Maître de conférences en droit privé
à l'Université de Picardie - Jules Verne

Introduction : Les données, instruments de mesure du risque

A. De la donnée à la donnée « à caractère personnel »

DCS : Depuis toujours, les données de l'assuré sont au cœur de la relation instaurée par le contrat d'assurance. Elles servent la mesure du risque individuel, objet du contrat et déterminent tant la décision de l'assureur de prendre ce risque en charge que sa tarification. De son côté, l'assureur se trouve dans un cas d'inversion du cycle de production : il doit évaluer le coût réel de son produit par le biais d'analyses prédictives du coût du risque et fait appel à l'actuariat. Ces analyses reposent sur des observations statistiques, et donc d'un ensemble de données massées que l'on nommera « données actuarielles ». Dans cette perspective, il apparait que plus l'information est riche, plus les critères sont fins, mieux l'assureur pourra affiner la mesure des risques que sa mutualité prendra en charge et meilleure sera la coïncidence entre son offre de couverture et les besoins individuels de l'assuré (segmentation de l'offre). Or, dans une perspective concurrentielle, la segmentation est devenue

1 - Ce travail prend pour point de départ les échanges ayant eu lieu avec Arthur Charpentier lors de la table ronde relative aux données d'assurance lors du colloque « Droit des données personnelles » (Amiens, 7-8 nov. 2016) qu'il a pour but de développer tout en conservant la forme originelle du dialogue. Le débat s'est également enrichi de la contribution de notre collègue R. Bigot, que nous remercions vivement d'avoir accepté de se joindre à la discussion.

indispensable pour pallier les effets néfastes du phénomène d'antisélection[2]. Cette circonstance ne peut que pousser l'assureur à chercher toujours plus de données.

Depuis le renforcement des préoccupations sur la protection des données, et notamment en raison de l'entrée en vigueur imminente du Règlement pour la Protection des Données Personnelles (dit RGPD) [3], l'attention se focalise sur le caractère « personnel » de la donnée. La définition qu'en donne le Règlement est large, suivant sur ce point un chemin emprunté il y a déjà longtemps par le législateur français[4], mais ne coïncide pas toujours avec la compréhension plus étroite qu'en ont les acteurs de terrain ou les intéressés eux-mêmes, pour la majorité desquels la donnée personnelle se cantonnerait à la vie privée ou intime.

Au sens du nouveau texte européen, l'expression « donnée à caractère personnel » vise « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » (RGPD, art. 4.1). La protection assurée par les textes va ainsi bien au-delà de la simple donnée « nominative », mais vise tout élément permettant l'identification, même indirecte[5].

2 - En assurance, la théorie économique montre que si les agents sont rationnels et si l'assurance n'est pas obligatoire, les « mauvais risques » ont un intérêt supérieur à la moyenne à souscrire un contrat d'assurance (phénomène dit de l'antisélection).

3 - Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dont l'entrée en vigueur est prévue pour le 18 mai 2018.

4 - V. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Loi Informatique et Libertés ».

5 - C'est ainsi que la CJUE a pu considérer dans un arrêt du 19 oct. 2016 (affaire C-582/14) que l'adresse IP dynamique d'un internaute conservée par le FAI constituait une donnée personnelle au sens de la directive 95/46/CE du 24 octobre 1995, dès lors qu'elle elle permet de l'identifier une fois associée à une autre information (adresse mail, horaires de connexion, etc.).

Question à l'actuaire :

Sur quel type de données l'actuaire d'assurance travaille-t-il dans sa pratique de modélisation des risques, et cela comprend-il des données directement ou indirectement identifiantes, soit des données dites « à caractère personnel » ? Peut-être même des informations sensibles, comme la race ou la religion ?

Sous quelles formes vous parviennent ces données ? Et surtout, pour éclairer l'amalgame souvent fait entre la notion de donnée à caractère personnel et celle de vie privée, quels en sont l'objet et les sources ? L'assureur, au premier chef imagine-t-on s'agissant des données fournies par l'assuré, les données publiques, les réseaux sociaux ?

AC : La source première de données dont dispose l'actuaire pour modéliser les risques, et construire un tarif segmenté est la base constituée à partir des informations collectées dans les formulaires de souscription. Ces formulaires contiennent un numéro de police, le nom de l'assurée, son adresse, sa date de naissance, etc. Les actuaires ont souvent accès aux données brutes, directement. Le nom et le prénom peuvent être exclus, mais en assurance habitation, il est souvent utile d'avoir accès au lieu précis d'habitation : l'adresse, et l'étage (pour les immeubles). Ces données sont bien souvent utiles, car le risque dépend du quartier, mais aussi de l'étage : pour le cambriolage savoir si l'habitation est au rez-de-chaussée est important, pour le dégât des eaux, c'est souvent savoir si l'habitation est au dernier étage. En assurance automobile, on peut utiliser des informations relatives au lieu d'habitation (habiter en banlieue ou en campagne n'impose pas le même genre de conduite) donc le code postal est souvent utilisé, mais aussi le modèle de véhicule (indiqué sur la carte grise), et l'âge du conducteur principal. En regroupant ces trois variables dans une commune de quelques milliers d'habitants, la personne est bien souvent identifiable.

À partir de ces données provenant des questionnaires, il n'est pas rare de procéder ensuite à des croisements de données. Par exemple à partir du modèle du véhicule, on peut trouver sa cote à l'argus (ce qui donne un montant maximal de remboursement en cas de dommage matériel), sa puissance (dans certains pays, seule la puissance du véhicule est utilisée comme variable tarifaire), le nombre de places, la

marque (certaines marques ont des coûts de réparation plus élevés), etc. En assurance habitation, l'adresse permet d'avoir toutes sortes d'informations. Croisées avec des données du cadastre, on peut avoir l'âge du bâtiment, mais on peut aussi voir des informations sur le quartier (nombre de cambriolages par exemple).

Depuis quelques années, les assureurs réfléchissent à l'utilisation de données « connectées », comme les bracelets qui mesurent le rythme cardiaque ou le nombre de pas faits dans une journée, et les boitiers GPS dans les véhicules. Ces données sont intéressantes pour comprendre le risque, mais plus difficilement à des fins tarifaires. En effet, la prime d'assurance est fixée *ex-ante*, et ces données sont collectées *ex-post*. Une solution peut être de faire une offre commerciale indexée sur un engagement de l'assuré, vérifiable par ces données connectées : offrir un rabais de 15% si la personne s'engage à faire en moyenne sur une semaine au moins 10 000 pas par jour, ou moins de 7000 km avec le véhicule sur une année. Les boitiers GPS permettent en théorie d'avoir accès à énormément d'informations sur l'assuré (lieu du domicile, localisation du stationnement, lieu du travail, lieu de l'école des enfants et du club de sport, etc.). Mais les assureurs sont tributaires de données externes, fournies par le fournisseur du boitier GPS. Pour des assurances de véhicules commerciaux, certains assureurs demandent expressément à ne pas avoir d'information sur la vitesse des véhicules par exemple. Certains autres demandent à n'avoir accès qu'à des informations très synthétiques sur la conduite : nombre de trajets, nombre de kilomètres, temps de conduite la nuit, etc. Ces données sont alors non-identifiantes, contrairement à nombre de données de télématiques[6].

Enfin, pour les données sur les réseaux sociaux, c'est plus sensible. Plusieurs études (aux États-Unis et en Angleterre) ont montré que l'utilisation d'informations relatives aux réseaux d'amis était très prédictive d'un défaut ou d'un retard de remboursement de crédit hypothécaire. On peut imaginer aller encore plus loin en regardant

6 - Sur les données géolocalisées de téléphones cellulaires, certaines études ont montré que 4 points (lieux et heures approximatifs) suffisent à identifier 95% des individus dans une base de données (de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. Unique in the Crowd: The privacy bounds of human mobility. Nature srep. 3, 1376; DOI:10.1038/srep01376 (2013)).

le contenu de ce qui est mis en ligne. Là aussi des études ont montré que les photos publiées sur une page Facebook pouvaient être utilisées pour prévenir le suicide. Lire le contenu permet probablement d'avoir des informations sensibles. En lisant les tweets précédant une élection présidentielle, il est possible d'avoir une prévision (avec une probabilité assez élevée) des orientations politiques de l'assuré. Mais rares sont les études qui montrent un lien entre les orientations politiques, sexuelles, religieuses d'une personne et son nombre de dégâts des eaux, ou d'accidents de la route, donc rares sont les actuaires à regarder ce genre de variables. En revanche, regarder les réseaux d'amis sur Facebook est souvent utilisé lors d'études sur la fraude.

Quand un actuaire fait un tarif, c'est un exercice de statistiques prédictives : en utilisant les informations passées, on essaye de voir si les assurés qui avaient des caractéristiques proches ont eu ou pas d'accidents (dans le passé), combien, à quel coût. Compte tenu des délais de déclaration et de clôture des sinistres, il faut souvent un long historique. Par exemple pour estimer le coût potentiel d'un accident corporel, pour les contrats d'assurance automobile, on ne peut pas se limiter aux statistiques relatives aux cinq dernières années : les plus gros sinistres sont encore ouverts, certains patients (les états les plus graves et donc les plus coûteux) sont encore dans un état non stabilisé. Il est alors indispensable d'utiliser les données les plus anciennes possible, avec la difficulté de tenir compte d'améliorations techniques sur les véhicules améliorant la sécurité, les changements de conduite (radars automatiques incitant à réduire globalement la vitesse) et l'inflation (hospitalière et juridique) pour les sinistres relativement anciens. Les actuaires « recyclent » en permanence les anciennes bases de données.

B. De la donnée personnelle à la « donnée sensible »

DCS : Le terme de « données sensibles » n'est pas anodin pour le juriste. Un régime particulier est en effet réservé à ces données, dont le traitement n'est autorisé que très exceptionnellement (article 9). Mais qu'entend-on exactement par « données sensibles » ? Sont visées par là les données dont le traitement « *révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier*

une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». Il faut donc considérer qu'il y a des données directement sensibles du fait de leur contenu, à côté de données qualifiées « sensibles » indépendamment de l'objet direct de l'information qu'elles portent[7]... du simple fait qu'elles permettront de *déduire* l'information jugée sensible. L'assureur peut être destinataire de données dont l'information est directement sensible (ex. assureur santé ou invalidité), mais il l'est assurément de toute une série d'autres, non sensibles en elles-mêmes, qui sont cependant susceptibles d'être croisées entre elles et de révéler alors bien plus. Si l'on songe à la masse des informations susceptibles de figurer dans un dossier d'assuré, sans compter celles qui peuvent être déduites des données très fines des objets connectés, la marge de manœuvre de l'assureur semble étroite...

Questions à l'actuaire :

Dans les données d'assurés sur lesquelles travaillent actuellement les actuaires, y a-t-il des données « sensibles » au sens du RGPD ? Ces résultats ou celui du croisement des données vous semblent-ils suffisamment fiables ou éloquents pour que l'on puisse considérer que de nombreuses données apparemment anodines pourraient tomber dans le champ de la donnée « sensible » du fait de ce qu'elles sont « susceptibles de révéler » (ex. : opinion politique ou religieuse) ?

AC : Comme évoqué auparavant, un actuaire ne cherchera pas ces données, car aucun modèle n'a établi de relation causale entre les opinions politiques, les croyances religieuses, etc. Mais le fait est qu'il est aujourd'hui possible d'avoir accès à des données très informatives sur ces variables dites « sensibles ». Une question est de savoir si ce phénomène est nouveau. Avec l'adresse précise, on pouvait consulter les résultats électoraux par bureau de vote (voire par urne), et affirmer qu'une personne avait 65% de chances d'avoir voté pour tel ou tel candidat. Avec le prénom de la personne, je peux aussi prédire qu'un certain « Jean-Pierre » a 87% d'avoir plus de 50 ans (à partir de

7 - Ce que semble bien confirmer la rédaction de l'article 9, lequel vise, à côté de données identifiées comme sensibles par leur objet (données génétiques par exemple), des données qui sont sensibles dans la mesure où elles révèlent des informations jugées sensibles (race, opinion politique, etc.).

statistiques sur le prénom). Je peux affiner ma probabilité en croisant avec son type de véhicule (certains véhicules sont possédés par des personnes de tel ou tel âge, en majorité). Avec les données GPS, je vois qu'une personne stationne presque tous les vendredis matins à proximité d'une mosquée. S'il existe des enquêtes sur les pratiques des musulmans, je pourrais affirmer qu'il y a 98% de chances qu'elle soit musulmane. Mais je me trompe peut-être, et cette personne va en fait au club de gym en face de la mosquée, et en plus elle est assidue. Que signifie avoir accès à des « données sensibles » ? Faut-il être certain ? La certitude est un concept inconnu aux statisticiens, donc à partir de quel seuil peut-on affirmer que l'on a à disposition des « données sensibles » ? On peut aussi penser à cet exemple fameux d'une société qui avait pu affirmer qu'une personne était enceinte à partir de son changement de consommation (observé à l'aide de sa carte d'achat d'une chaîne de grands magasins) alors que cette personne l'ignorait. Quid du fait qu'il est (en théorie) possible d'avoir à des données encore plus précises (et justes) que celles que les actuaires rêvaient d'avoir ? Plusieurs études ont montré qu'il existait une relation très forte et très prédictive entre les infractions et les accidents de la route. Au Canada, le nombre de points sur le permis est une variable très importante pour prédire le nombre de sinistres l'an prochain (avec des effets complexes, en particulier quand une personne a perdu beaucoup de points, elle peut être beaucoup plus prudente qu'une autre ayant les mêmes caractéristiques, mais tous ses points, car elle ne souhaite pas perdre son permis). Tout statisticien rêve de croiser ces données, afin de mieux comprendre l'accidentologie de ses assurés. Le danger est que le fichier des points ou des infractions ne contient que des informations sur ce qui a été sanctionné. Or l'intuition dit qu'on préfère assurer la personne qui n'a pas eu de chance et qui s'est fait flasher trois fois 5 km/h au-delà de la limite qu'une personne qui refuse les priorités sans se faire prendre, et qui a la présence d'esprit de ralentir avant tous les radars. On pourrait imaginer un score construit à partir des données des boitiers GPS, sur le respect des stops, le respect des limitations de vitesse. En un sens, l'actuaire aurait à sa disposition non pas un fichier sensible (des infractions), mais des données beaucoup plus riches, et probablement plus pertinentes.

§1 : La collecte des données personnelles de l'assuré

DCS : Traditionnellement, l'assureur recueille les informations relatives à son futur assuré à l'aide du questionnaire rempli

à la souscription, autrement désigné comme « la proposition d'assurance » (A), et le cas échéant, à en collecter d'autres à l'occasion d'une déclaration de sinistre. Mais des pratiques nouvelles, comme le couplage du contrat d'assurance avec un objet connecté, émergent, qui invitent à se pencher sur une collecte de données qui seraient effectuée par ce biais (B).

A. Données recueillies via la proposition d'assurance

1) Des données pertinentes au regard du risque à évaluer

Le RGPD vient de modifier assez profondément les obligations des responsables de traitement et s'affiche comme un instrument venant renforcer les droits des individus[8]. À l'instar de la loi Informatique et Libertés de 1978 et de la Directive de 1995[9], le Règlement définit les fondements sur lesquels peut reposer un traitement de données, dont la collecte est le premier stade. Celle-ci doit être au premier chef consentie, et ce pour une finalité déterminée (art. 6.1, a). Pour traiter des données sans le consentement de l'intéressé, il faut pouvoir se prévaloir d'un autre fondement, ce qui sera notamment le cas si la donnée est « *nécessaire [...] à l'exécution de mesures précontractuelles* » (RGPD, art. 1.b). De ce point de vue, la collecte des données personnelles de l'assuré par l'assureur semble *a priori* fondée au titre de la mesure précontractuelle qu'est l'évaluation du risque, et ce donc, indépendamment du consentement de l'assuré.

La collecte d'informations, préalable au contrat d'assurance, doit cependant être envisagée d'un autre point de vue du fait que le recueil d'informations concernant l'assuré relève déjà d'une réglementation

8 - Le juriste français est néanmoins enclin à la réserve à cet égard dès lors que la loi n° 78-17 du 6 janvier 1978 a déjà depuis longtemps posé les fondements de la protection actuelle. Par ailleurs, les nombreuses imprécisions qui affectent les définitions du RGPD, ou la multiplication des exceptions aux règles prohibitives, sont autant de failles dans la protection. Ce, d'autant plus que le nouveau principe d'*accountability* (passage d'un système de contrôle a priori de la CNIL, par le biais des déclarations et autorisations, à un contrôle a posteriori) déplace en pratique l'interprétation de ces notions sur le responsable du traitement, qui n'aura pas toujours les ressources juridiques nécessaires, et pourrait, en tout état de cause, être tenté d'entendre de manière extensive les exceptions qui lui sont favorables.

9 - Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281, p. 31).

spécifique du Code des assurances. En effet, celui qui demande la prise en charge d'un risque est légalement tenu aux termes de l'article L. 113-2, 2° dudit Code de « *répondre exactement aux questions posées par l'assureur, notamment dans le formulaire de déclaration du risque par lequel l'assureur l'interroge lors de la conclusion du contrat, sur les circonstances qui sont de nature à faire apprécier par l'assureur les risques qu'il prend en charge* ». L'assuré doit donc fournir les informations qui lui sont demandées, la question ne se posant pas vraiment en termes de consentement au traitement de ses données, mais plutôt de consentement à la relation d'assurance, laquelle implique *ipso facto* une obligation de renseigner.

En résumé, si le recueil des données par l'assureur dans la proposition d'assurance apparaît fondé au sens du Règlement en ce qu'elle est nécessaire à une mesure précontractuelle déterminant la relation d'assurance, il est avant tout, au regard du Code des assurances, un droit de l'assureur opposable à l'assuré. Cette dualité de régime soulève notamment la question des limites de la collecte des données personnelles. S'agissant du texte européen, cet aspect relève de l'article 5 qui pose les principes de *limitation* au regard des finalités et de *minimisation* des données. Ainsi, et quel que soit son fondement, la collecte – ici des données de l'assuré - n'est licite que dans la mesure où elle sert des « *finalités déterminées, explicites et légitimes* » (art. 5.1.b) et qu'il s'agit de données « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités* » (art. 5.1.c). Le Code des assurances considère, quant à lui, que l'assuré n'a d'obligation de répondre aux questions de l'assureur que dans la mesure où il s'agit de« *circonstances qui sont de nature à faire apprécier par l'assureur les risques qu'il prend en charge* » (C. ass., art. L. 113-2,2°). Dans les deux cas, c'est l'évaluation du risque qui dessine les contours de ce qu'il est possible de collecter via la proposition d'assurance, car elle en constitue la finalité. Partant, les données qui ne seraient pas strictement nécessaires à cette évaluation du risque, par exemple des données qui ne seraient utiles à l'assureur qu'afin d'améliorer sa relation client[10], ne devraient pas pouvoir être recueillies via le questionnaire qui s'impose au candidat à l'assurance.

10 - Cf. remarque de J.-B. Beaume, *Chief data scientist* (Covea), intervenant lors de la table ronde du 8 novembre 2016, sur le fait que l'assureur sollicite nécessairement ce type de données à côté de celles nécessaires à l'appréciation du risque

Mais l'assureur étant celui qui détermine les risques qu'il accepte de prendre en charge (ainsi que les différentes catégories tarifaires au sein des populations concernées, selon des critères choisis par lui), il semble bien être seul maître de la « pertinence » des données qu'il peut *solliciter* au titre de l'obligation de déclaration, ou *collecter* de manière licite, sans avoir à solliciter le consentement de la personne intéressée au sens de l'article 5.1 du RGPD. Cela conduit naturellement le juriste à s'intéresser de plus près à la manière dont est effectuée la sélection des informations « pertinentes » pour l'assureur, s'agissant d'évaluer le risque, ainsi que leur traduction dans le formulaire de la proposition d'assurance.

Question à l'actuaire :

Pouvez-vous nous éclairer sur le travail de l'actuaire d'assurance, et notamment comment celui-ci détermine le type de données qui seront érigées en variables pertinentes d'un risque, et qui donc permettront à l'assureur de définir les conditions de sa prise en charge (exclusion, couverture sous conditions, tarification) ? Cette « pertinence » de la donnée ne dépend-elle pas du fait que vous en ayez disposé avant afin d'étudier son influence éventuelle sur le risque assuré ?

AC : Il y a deux philosophies en modélisation : soit on part d'un modèle structurel, et on estime les coefficients du modèle, statistiquement, soit on met toutes les variables à notre disposition, et on regarde ce qui a du sens. Ce sont les débats qui existent aujourd'hui sur le « big data » et la fin des modèles[11]. Des études épidémiologiques peuvent donner le délai d'incubation de maladies, et donc indiquer les durées d'attente nécessaire pour l'assurance des centres de transfusion par exemple. Des études sur les transports peuvent donner des liens entre la gravité des accidents de la route et l'heure de l'accident. Savoir qu'une personne conduit beaucoup la nuit sera alors une information que l'on cherche à avoir. Des enquêtes de psychologie peuvent établir des liens entre la couleur de la voiture, et le type de conduite. Savoir qu'une personne conduit une voiture rouge pourra alors être informatif. Les études d'ingénierie peuvent établir un lien

11 - C'est l'idée énoncée il y a 10 ans : C. Anderson "End of Theory: The Data Deluge Makes the Scientific Method" (*Wired*, juin 2008).

entre l'orientation d'un toit et sa probabilité d'être détruit lors du passage d'une tempête hivernale (souvent d'ouest en est). Connaître l'orientation de la maison devrait être intéressant pour tarifer une garantie tempête pour un contrat multirisque habitation. On peut alors avoir un modèle structurel en disant que la probabilité d'avoir un sinistre, ou le coût d'un sinistre doivent être fonction de telle ou telle variable. Les approches plus récentes, dites « data-driven » disent qu'il n'est pas nécessaire d'avoir un modèle formel présupposé, et qu'un algorithme de recherche de corrélations suffira. Ces débats se retrouvent actuellement dans tous les domaines de l'intelligence artificielle. Historiquement, pour faire de la traduction, on supposait qu'il fallait connaitre la grammaire, la structure de la langue. Mais les traducteurs automatiques actuels se contentent de chercher dans des corpus énormes des phrases proches, puis de mélanger de manière logique. C'est la même chose pour les jeux d'échec ou de go, ou la conduite automatique : on ne fait pas un modèle formel de conduite ou de mouvements de pièces sur l'échiquier (si le fou menace ma reine, je cherche à la protéger), mais on demande de regarder dans des millions de parties jouées s'il existe des situations semblables, et de regarder le mouvement qui a permis de gagner dans le plus grand nombre de cas.

Aussi, techniquement, on cherche des variables corrélées avec la sinistralité. Mais cela ne veut pas dire qu'on a une relation causale. La recherche de relations causales est fondamentale en assurance, car elle peut permettre de faire de la prévention. Si on sait que ne pas mettre deux verrous sur une porte d'entrée augmente la probabilité d'être cambriolé de 20%, un assureur peut inciter un assuré à poser un deuxième verrou (si le coût est inférieur à la surprime sur quelques années), et donc changer le risque. Mais bien souvent, les actuaires n'établissent pas de relations causales, ils observent juste des corrélations, et racontent alors une histoire causale. Le fait de conduire une voiture rouge n'est pas neutre sur la survenance de sinistres. La couleur est alors corrélée avec la survenance de sinistres. Établir une relation de causalité sera compliqué (et techniquement, la personne au volant ne *voit* pas la couleur extérieure de son véhicule, et si on repeint à son insu sa voiture, pourquoi cela impacterait sa conduite ?). C'est juste qu'on se raconte que les personnes qui achètent une voiture rouge, et pas grise, ont probablement une conduite particulière. La couleur est

alors un « proxy » d'une variable non observée, qui caractériserait le type de conduite. Mais ce n'est pas la couleur en tant que telle qui nous intéresse.

Le souci est que pour tester si la couleur est liée à la sinistralité, il faut l'avoir dans les données : on ne sait si une variable peut être utilisée dans un tarif que si on l'a collectée. On se retrouve dans un problème d'œuf et de poule : pour savoir si une variable peut être utilisée, il faut l'avoir récoltée au préalable, alors que la récolte est conditionnée par le fait qu'il faut avoir établi qu'elle était utile.

2) Des données « juridiquement disponibles »

RB : Depuis peu de temps, le législateur a instauré, en assurance emprunteur, un droit à l'oubli pour certains assurés atteints par le passé de graves pathologies[12]. En interdisant ainsi la prise en compte des antécédents médicaux d'une particulière gravité, classés dans une grille de référence, les assurés disposent d'une forme de droit de taire certaines informations sur leur santé, pour bénéficier de l'assurance, sans surprime ni exclusion. Concrètement, lors de la souscription d'un contrat assurance emprunteur, ils ne sont plus tenus de déclarer leur pathologie après l'écoulement de certains délais fixés d'un à dix ans selon les six types d'affection (hépatite virale C, cancer du testicule, cancer de la thyroïde, certains cancers du sein, mélanome de la peau et cancer du col de l'utérus) et intégrés dans une grille de référence adoptée le 4 février 2016. En l'absence de rechute, la fin du protocole thérapeutique est le point de départ

12 - La convention AERAS ou « s'Assurer et Emprunter avec un Risque Aggravé de Santé « est le fruit d'un accord entre les pouvoirs publics, les fédérations professionnelles de l'assurance, la banque et les associations de malades. Son but consiste à améliorer l'accès au crédit des malades. La convention et ses principales dispositions sont transposées aux articles L. 1141-2 à L. 1144-4 du Code de la santé publique. Après un premier avenant signé le 1er février 2011 et entré en vigueur le 1er mars 2011, un second avenant a été conclu le 2 septembre 2015. Il confère un droit à l'oubli aux personnes ayant eu une pathologie cancéreuse, consacré par la loi du 26 janvier 2016 et étendu à des pathologies non cancéreuses (CSP, art. L. 1141-5). Lors de la souscription d'un contrat assurance emprunteur, elles ne sont plus obligées de déclarer leur pathologie après l'écoulement de certains délais fixés d'1 à 10 ans selon le type d'affection et intégrés dans une grille de référence adoptée en février 2016. En l'absence de rechute, la fin du protocole thérapeutique est le point de départ du délai décennal. - Cf. de Fallois M., Assurance et « droit à l'oubli « en matière de santé, RDSS 2017-1, p. 132. - Bouteille-Brigant M., Les indispensables du droit médical, Ellipses, 2016, p. 98.

du délai décennal. Regrettablement, les assureurs demeurent libres de refuser de garantir des personnes présentant un risque aggravé de santé candidates à des prêts immobiliers et professionnels. La convention AERAS ne leur garantit aucun accès au crédit.

Par ailleurs, les assureurs sont susceptibles d'utiliser de nouvelles technologies, comme la *blockchain*, dans sa forme de registre sécurisé par exemple, laquelle ne permettrait pas d'effacer les données personnelles. L'assureur peut ainsi trouver un fort intérêt à connaître l'historique d'un contrat (sa reconduction, ses avenants, pour l'application de la garantie dans le temps) et l'assuré à savoir si une clause, abusive par exemple, a bien été éradiquée de la police. Le problème surgit en matière de données protégées, pêle-mêle par la confidentialité, le secret professionnel, le secret médical, ou en matière de données sacrifiées sur l'autel de la transparence par le droit à l'oubli. Deux formes récentes de l'oubli ont été érigées en droit subjectif par le législateur : la convention AERAS pour les assurances des emprunteurs ayant eu des maladies graves et encore l'appréciation par le procureur de la République de l'opportunité de l'effacement dans le fichier de traitement d'antécédents judiciaires pour des personnes ayant eu un tel passif. Le risque est donc celui d'une violation ineffaçable dans la *blockchain*, au point qu'elle puisse devenir perpétuelle. Reportée sur l'analyse du risque par l'assureur, cette impossible suppression de l'information dans la *blockchain* est susceptible de construire un système d'entrave anticipée à la réalisation du droit à l'oubli.

Question à l'actuaire :

L'actuaire est-il déjà amené à utiliser des blockchains dans l'assurance ? Le cas échéant, ces registres dématérialisés posent-ils des difficultés de collecte et de traitement des données à l'actuaire eu égard à certaines informations sensibles, éventuellement protégées par la confidentialité ou le secret, et susceptibles d'influer sur la nature du risque ?

En matière de santé concrètement, le croisement et la connaissance de données passées ne permettent-ils pas de contourner le droit à l'oubli et de refuser, en toute connaissance du risque, un assuré qui devrait être considéré comme vierge par suite du droit qui lui est reconnu de taire sa pathologie ?

L'actuaire peut-il aussi identifier des données protégées par exemple par le droit à l'oubli et les mettre à l'écart pour ne pas discriminer ni à l'entrée ni à la tarification ?

AC : Les *blockchains* sont aujourd'hui utilisées en assurance pour éviter de passer par des intermédiaires coûteux, et n'apportant pas grand-chose dans la chaîne de valeur. Certains assureurs proposent déjà des contrats pour des retards relatifs à des voyages (avion ou train). Historiquement, l'assuré devait contacter son assureur afin de déclarer un retard, avec des justificatifs (parfois difficiles à obtenir). L'assureur devait ensuite vérifier l'information, puis procéder à l'indemnisation. Ces contrats sont simples, car l'indemnité est directement liée à une information qu'il est possible d'avoir par ailleurs, de manière sécurisée (il existe des registres attestant des heures de décollages et d'atterrissages). L'idée des contrats de type *blockchain* est de proposer une assurance indicielle ou paramétrique qui ne nécessite plus de demande de la part de l'assuré et de validation par l'assureur. Le processus peut être automatisé et sécurisé. On peut imaginer des contrats indiciels agricoles basés sur la même technique, avec le versement (automatique) d'une indemnité s'il n'a pas plu pendant trente jours consécutifs. Pour l'instant, les *blockchains* ne posent pas de soucis quant aux données utilisées, car elles sont souvent publiques (heures d'arrivée d'avion, indice de température). Mais la question se poserait pour des contrats dont le sous-jacent serait une donnée personnelle.

Pour le second point, je n'ai pas beaucoup d'expérience en données de santé. Néanmoins, prenons le cas de l'assurance automobile. Quand on parle ici d'une utilisation de données passées, on parle de personnes déjà présentes depuis plusieurs années dans le portefeuille, souhaitant un renouvellement. Dans les exemples mentionnés, on parle plus précisément d'informations relatives à des sinistres : s'il a eu une condamnation pour excès de vitesse, l'assureur ne le sait pas, sauf s'il y a eu un accident. Or le droit des assurances donne déjà un pouvoir discrétionnaire à l'assureur d'exclure certains assurés suite à un sinistre, donc je ne suis pas sûr qu'il y ait quelque chose de réellement nouveau. La difficulté se pose quand l'information que l'assureur veut utiliser n'est pas une information relative à la triche (ou une fraude) avérée d'un assuré, mais sur la suspicion de fraude. Supposons qu'un gestionnaire de

sinistre ait la possibilité d'indiquer sur certains dossiers « suspicion de fraude » (et que cela engage ensuite l'envoi d'un expert). Pourrait-on utiliser cette information même plusieurs années après, ou peut-on imaginer un droit à l'effacement ? Dans ce cas, les techniques statistiques viennent sauver les assurés. En effet, si tous les sinistres étaient contrôlés par des experts, il n'y aurait plus de « suspicion » de fraude, mais juste une variable « a fraudé » / « n'a pas fraudé ». Mais c'est plus complexe, car sur le cas de la fraude, l'actuaire dispose juste d'un échantillon, d'une sous-population sur laquelle un expert s'est prononcé sur la fraude. Si l'envoi d'un expert est purement aléatoire, on aura un sondage sur une population représentative. Mais ce n'est souvent pas le cas : l'expert est souvent envoyé suite à une suspicion. La sous-population n'est pas représentative, et il est alors très difficile d'utiliser la variable fraude. Cette variable est dite manquante, car on ne sait pas si la personne a fraudé ou pas, on sait juste que la personne n'a pas été jugée suspecte. Ce biais rend l'utilisation de ces données très délicates. C'est en fait pareil pour l'assurance santé dont on parlait : que signifie le fait qu'aucune maladie n'ait été déclarée ? Qu'il n'y a pas eu de maladie, ou bien qu'elle n'a pas été mentionnée ? Travailler sur des données dites manquantes rend l'exercice délicat, car l'interprétation peut être fallacieuse.

3) Des données dont la pertinence est sujette à évolution

DCS : L'on imagine volontiers que le travail d'actuariat évolue, selon les transformations sociales, environnementales, les techniques disponibles... Si l'âge, le lieu de résidence ou l'activité professionnelle sont des facteurs de discrimination tarifaire notoirement connus, ils relèvent d'une modélisation classique, liée à une époque où notamment les sources et les méthodes de traitement des données étaient moins développées qu'aujourd'hui...

Question à l'actuaire :

Y a-t-il une limite aux types de données dont vous êtes susceptible de découvrir la pertinence pour mesurer le risque en assurance de masse (automobile, multirisque habitation, santé) ? L'actuariat va-t-il dégager de nouveaux critères, s'ils ne le sont déjà, notamment dans un contexte de croissance du big data ?

AC : Historiquement, ces variables tarifaires étaient utilisées, car elles étaient faciles à avoir. Il y en a qui seraient intéressantes, mais plus difficiles à avoir. Par exemple a-t-on un gros conducteur ou un conducteur occasionnel ? Le kilométrage est une variable très liée à la sinistralité. Mais elle est inconnue à la souscription. Une astuce a longtemps été de demander à ce que l'assuré s'engage à faire moins de 7000 km par an (par exemple). Autre information longtemps utilisée, le genre. Là encore, c'était une variable facile à obtenir, et corrélée avec la sinistralité. Les études récentes sur données télématiques ont montré que le genre était utilisé comme le « proxy » d'une information difficile à avoir, sur le type de trajets effectués. En particulier, en utilisant des informations sur l'heure à laquelle les trajets sont effectués, le nombre de kilomètres parcourus, etc., le genre n'apportait aucune information supplémentaire intéressante[13]. En santé, on pouvait demander si la personne fumait ou pas. Mais ça reste déclaratif, et difficilement vérifiable. On pourrait imaginer avoir des informations plus précises par des objets connectés. Ou sur la pratique sportive d'une personne (nombre de pas par jour avec des bracelets connectés).

B. Le cas des données recueillies via des objets connectés

DCS : Vous venez d'évoquer les objets connectés, et l'on voit précisément à cet égard de plus en plus d'initiatives tendant à lier le contrat d'assurance à leur utilisation. Ainsi en matière automobile, les contrats *Youdrive* de Direct Assurance et *Rate my drive* d'Aviva GB, ou en matière de santé le contrat *Vitaly* proposé par Generali Assurance. Ces contrats restent pour l'instant des alternatives aux contrats classiques en raison, semble-t-il, de la méfiance naturelle de la majorité des assurés, soucieux de leur vie privée, et reposent donc sur l'adhésion à ce type de procédé. Ces nouvelles pratiques soulèvent donc au premier chef la question de leur dépendance au consentement de l'assuré (1°). S'y ajoute celle du moment de la collecte des données de l'objet connecté, notamment au regard de sa finalité (2°).

13 - Résultat établi par R. Verbelen, K. Antonio et G. Claeskens dans *Unraveling the Predictive Power of Telematics Data in Car Insurance Pricing* (http://bit.ly/2DBNMto).

1) La question du consentement de l'assuré

À l'heure actuelle, l'assuré consent à l'utilisation d'objets connectés afin de bénéficier d'un tarif mieux ajusté (tarif bon conducteur), voire d'avantages en nature (assurance santé). À côté du potentiel de prévention que vous évoquiez précédemment, l'on pressent certainement aussi la possibilité d'analyser plus finement le risque grâce aux nouvelles données collectées par l'objet. Or l'on a rappelé le lien existant entre l'entrée d'une donnée dans le champ de l'évaluation du risque et l'obligation pour le candidat à l'assurance de la livrer. Et si cette pratique ne semble être fondée à l'heure actuelle que sur le consentement de l'assuré (a), il n'est pas interdit de se demander ce qu'il en serait dans le cas où la pression concurrentielle conduirait à généraliser ce type de contrats (b).

a) Une pratique supposant le consentement de l'assuré

Le recours à l'objet connecté, qu'il s'agisse de prévenir ou d'évaluer le risque, est aujourd'hui fondé sur l'adhésion de l'assuré et son utilisation doit donc être *consentie*. Mais à défaut d'une information précise sur le type d'informations collectées, il est difficile de considérer que le consentement à l'utilisation du dispositif (boitier sur véhicule, indicateur d'activité physique pour santé) emporte *ipso facto* consentement au traitement de toute donnée collectée par son biais. Un tel raccourci serait contraire à l'exigence d'un consentement *spécialement donné* que le Règlement consacre[14] lorsque le traitement repose sur ce fondement. Par ailleurs, le droit à l'autodétermination informationnelle[15] permet à la personne concernée de retirer celui-ci (art. 7.3 RGPD). Techniquement cela devrait au moins se traduire par une maitrise directe de l'assuré sur

14 - On rappellera ici que l'exigence du consentement a été considérablement renforcée dans le texte européen. Ainsi notamment, l'article 7.2 dispose-t-il que « *si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples* ». Le consentement au traitement des données doit donc être spécialement donné.

15 - Introduit matériellement en droit français par loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, qui a ajouté à l'article premier de la loi I&L un nouvel alinéa selon lequel « *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* ».

l'ensemble du flux de données (ex. V. le nouveau « Pack Assurance » de la CNIL qui envisage le cas du véhicule connecté transmettant les données – V. spéc. le scenario *in-out*– et suggère de prévoir des réglages par défaut sans transmission, ou des dispositifs simples de coupure du flux). Cependant, pour que le droit d'autodétermination informationnel soit effectif, ou simplement même pour que l'on puisse parler de consentement au traitement, cela suppose que l'assuré soit conscient de la nature des données que l'objet collecte, et plus avant, de celles que leur croisement est susceptible de fournir à l'assureur. En d'autres termes, analyser la portée du consentement donné par l'assuré à l'usage de l'objet connecté dans le cadre de son contrat d'assurance suppose de se pencher plus avant sur le type de données dont l'objet connecté sera la source et sur l'usage que peut en faire l'assureur.

Questions à l'actuaire :

Pouvez-vous nous donner une idée du champ de données que ce type d'objets (boitier véhicule, bracelet porté par l'assuré) est techniquement en mesure de fournir à l'assureur ? Au-delà des données brutes (géolocalisation par ex.), quelles autres informations (et donc nouvelles données) l'assureur est-il susceptible de recueillir à partir de leur croisement ?

AC: Pour les données télématiques, les données fines permettent d'avoir des scores de freinage, d'accélération, qui donnent des informations sur le type de conduite. Techniquement, ils permettent de savoir aussi *qui* conduit (voiture conduite par monsieur et madame, voire le grand enfant dans le cas de la conduite accompagnée). On peut aussi savoir quel type de route est utilisé, quelle distance est parcourue par jour, etc. Mais il est aussi possible d'avoir des informations plus agrégées, comme le pourcentage de temps de conduite la nuit. La difficulté rejoint une précédente question : les données collectées dépendent du type de boitier utilisé, mais pour savoir ce qui serait utile, il faut avoir collecté les données. Les assureurs font généralement toutes sortes de tests, afin de savoir ce qu'ils exploiteraient réellement, et à quelle fin. Et voir s'ils veulent les données en temps réel, ou juste à des fins statistiques, en fin de semaine ou de mois. Un assureur pourrait être intéressé par ces données en temps réel pour proposer une application liée à la prévention du risque, par exemple offrir un café sur une aire

d'autoroute si le conducteur a déjà conduit deux heures d'affilée, et qu'il s'engage à faire une pause de trente minutes.

b) L'hypothèse d'une collecte imposée

DCS : Si la pratique actuelle des objets connectés dans les contrats d'assurance repose sur le consentement de l'assuré, les raisons en sont néanmoins pour l'instant essentiellement commerciales. En effet, les assurés ne sont pas prêts à admettre si facilement les potentielles intrusions des objets connectés dans leur vie privée. La question se pose néanmoins de savoir si ce consentement est, du point de vue juridique, un rempart absolu contre ces pratiques. Ainsi qu'on l'a vu, l'assuré ne peut refuser, au sens du Code des assurances, de livrer « *les circonstances qui sont de nature à faire apprécier par l'assureur les risques qu'il prend en charge* » (C. ass., art. L. 113-2). Pour l'instant cette obligation est, de fait, circonscrite au cas où l'information est sollicitée via le questionnaire d'assurance, mais elle n'est pas, en droit, expressément limitée à cette forme de collecte[16]. Or, il n'est pas interdit d'imaginer qu'une information, que seuls ces objets peuvent livrer (ex. données fines de trajet) puisse un jour être tenue pour une circonstance « *de nature à faire apprécier le risque par l'assureur* ». Dans un tel cas, l'obligation de livrer l'information qui va de pair avec cette qualification pourrait se transformer en une obligation d'accepter l'usage de l'objet connecté pour celui qui veut s'assurer. Et, du point de vue, plus général, adopté par le Règlement, l'assureur serait fondé à récupérer cette donnée dès lors que cela est nécessaire à l'exécution du contrat, autrement dit sans avoir à recueillir le consentement de la personne concernée (soit qu'elle conditionne la souscription, soit qu'elle soit faite éventuellement à son insu).

Question à l'actuaire :

Pensez-vous disposer un jour de suffisamment de ces « nouvelles données », issues d'objets connectés, pour que la modélisation du risque repose dessus, au point que l'assureur qui aura construit son modèle tarifaire sur ces variables ne veuille – voire ne puisse - plus s'en passer pour l'ensemble des assurés ?

16 - V. la rédaction de l'article L. 113-2 qui évoque les questions posées à l'assuré « *notamment dans le questionnaire d'assurance* ».

La conséquence n'en serait-elle pas, à terme, une généralisation de la pratique des assurances liées à des objets connectés du fait de leur intégration dans le modèle tarifaire (art. L. 113-2, 2°) ?

AC : Un tarif qui utiliserait ces « nouvelles données » pose la question importante de l'absence d'information : que faire si une personne refuse qu'un boitier GPS soit installé en permanence ? Il existe plusieurs solutions. La première est d'imposer le boitier, mais de permettre qu'une désactivation soit possible. Les assureurs qui ont essayé se sont rendu compte qu'il y avait alors un biais important dans les données collectées (trop peu utilisaient leur voiture du vendredi après-midi au dimanche matin, au vu des données). Une seconde est de faire deux contrats, un pour les utilisateurs de boitiers, un pour les non-utilisateurs. À l'heure actuelle, les assureurs cherchent à avoir des données, le plus possible, afin de mieux comprendre quelles informations sont réellement pertinentes dans un modèle prédictif. Il y a une tendance à offrir un « bonus » aux personnes qui acceptent de fournir leurs données. Mais si l'installation de boitier n'a pas d'impact sur la sinistralité, c'est un jeu à somme nulle (au sens où le montant des sinistres à payer est inchangé) : un « bonus » pour une sous-population signifie un « malus » pour l'autre. Autrement dit, il y aura une pénalisation pour les personnes qui ne souhaitent pas céder ces données personnelles. Cela n'est pas sans poser des problèmes à l'actuaire, car ce refus est une variable intéressante, importante, dont les liens avec la sinistralité sont difficiles à appréhender.

Il convient peut-être de rappeler ici qu'il existe deux tarifications relativement différentes. La première est une tarification dite « a priori », qui concerne les nouveaux clients ; la seconde est une tarification dite « a posteriori » (on parlera parfois d'« experience rating »), qui concerne les renouvellements des contrats. Dans les cas évoqués ici, l'information est alors connue une fois le contrat souscrit et on ne peut pas utiliser ces données en tarification (à moins de changer la forme des contrats. Par exemple en offrant des contrats d'assurance automobile non plus à l'année, mais pour un nombre de kilomètres prédéterminés). En revanche, il serait possible d'utiliser cette information lors d'un renouvellement. Par exemple on pourrait dire que l'an passé, le conducteur a fait partie des 10% des plus gros conducteurs (en termes de nombre de kilomètres parcourus) et qu'une majoration de prime s'impose.

2) La question du moment de la collecte

RB : En définitive, un décalage temporel apparaît entre le moment où les données sont mises à disposition et celui de la conclusion du contrat d'assurance. Les objets connectés accouplés à des *smart contracts* seraient parfois susceptibles de surmonter ce décalage. Il subsiste un problème intermédiaire, celui du déclenchement de la garantie (d'une assurance automobile) en fonction d'un objet connecté relié à un *smart contract*. On peut imaginer deux modes de consentement : une souscription à l'assurance en amont dont le *smart contract* est une condition liée à une prise d'information en temps réel (condition suspensive de mise en œuvre de la couverture liée au démarrage du véhicule) ou une souscription à l'assurance *in situ*, à chaque évaluation du risque par l'objet connecté. Outre les problèmes du consentement indispensable en principe pour la formation du contrat, la prise de données de l'assuré et des biens qu'il assure en permanence par l'assureur peut éventuellement lui permettre de les utiliser ultérieurement à son encontre, c'est-à-dire à d'autres fins que l'objet et l'obligation pour lesquels et dans le cadre desquels l'assuré a consenti à l'installation de l'objet connecté.

§2 : L'exploitation des données de l'assuré par l'assureur

DCS : Une fois collectées, les données d'assurés sont susceptibles d'être exploitées de différentes manières par l'assureur. Au premier chef, bien sûr, lors de la souscription du contrat, s'agissant d'accepter ou non le risque, et le cas échéant, de le tarifer (A). Au cours de l'exécution du contrat, la question de l'usage qui est fait des données de l'assuré ressurgit dans le cadre de la lutte contre la fraude (B). Le cycle des données personnelles d'un assuré ne s'achève cependant pas avec l'exécution du contrat, car elles sont encore susceptibles d'être exploitées parfois bien au-delà du terme du contrat, du fait qu'elles ont vocation à intégrer les statistiques actuarielles de l'assureur (C).

A. Décision de prise en charge et tarification du risque

En raison des spécificités de l'opération d'assurance, l'exploitation des données d'assuré pour déterminer la prise en charge du risque ou sa tarification est en premier lieu confrontée à l'appréhension par le droit de certains types de discriminations, soit qu'il les interdise, soit qu'il

cherche simplement à les réguler (1°). S'agissant plus précisément de la tarification, les techniques mises en œuvre dans ce cadre invitent à se pencher plus spécialement sur la question du profilage (2°).

1) Discrimination prohibée ou limitée

a) Discrimination tarifaire prohibée

Depuis le 1er mars 2011, date de l'arrêt *Test Achat* rendu par la CJUE (Affaire C-236/09) sur le fondement de la Directive 2004/113 du 13 décembre 2004 *mettant en œuvre le principe de l'égalité de traitement entre les femmes et les hommes dans la fourniture de biens et services*, la discrimination fondée sur le sexe de l'assuré est clairement condamnée. Or ce critère faisait partie des facteurs actuariels historiquement utilisés par les assureurs pour prendre la mesure des risques (différenciation de la longévité, du risque automobile...). L'assureur, dont on rappelle qu'il cherche à limiter les effets de l'antisélection, doit donc se fonder sur d'autres facteurs. Peut-être est-il alors tenté d'en chercher de nouveaux. Sachant que l'on peut *a priori* déduire des sympathies politiques du simple croisement de données sur les préférences musicales, il n'est pas interdit de penser que le sexe puisse être déduit du croisement d'autres données, et de s'interroger sur le caractère très platonique de telles interdictions à l'ère du *big data*.

Question à l'actuaire :

Comment les assureurs ont-ils intégré la disparition d'un facteur discriminant majeur de leurs modèles d'évaluation du risque après 2011 ? Techniquement, le fait de disposer de multiples données périphériques ne permet-il pas de déduire la donnée discriminante « interdite » et donc de masquer le réel critère de discrimination tarifaire ? Est-il possible que l'assureur, même sans chercher délibérément à « reconstruire » la donnée « interdite » (sexe dans notre exemple), retrouve la même granularité dans l'analyse du risque à partir des nouvelles données ?

AC: Comme nous l'avons évoqué, il convient de repenser de manière historique comment les tarifs ont été construits. Si l'âge était utilisé en assurance automobile, c'est que cette variable est facile à obtenir,

et qu'elle est corrélée à la sinistralité. Certains évoquent aujourd'hui l'idée de « *spurious correlation* » dans le sens où aucune relation causale ne peut être établie, et elle serait un proxy d'une variable plus difficile, historiquement, à observer. Beaucoup évoquent l'idée que l'âge devrait aussi être exclu, tout comme le genre. En assurance automobile, l'expérience est un facteur clé. Une parade serait d'utiliser l'ancienneté du permis, qui est en fait, bien souvent, une variable plus informative que l'âge (même s'il existe des particularités pour les personnes d'âge très avancé). Il faut garder à l'esprit la différence entre « avoir accès à certaines données » et « pouvoir avoir accès ». Sur le genre, on peut imaginer que l'actuaire puisse prédire (avec un faible taux d'erreur) le genre du conducteur. Mais pour ce faire, il utilisera probablement des données plus intéressantes pour la tarification. Chercher à recréer la variable de genre serait alors un travail coûteux, et inutile.

b) Discrimination limitée

RB : S'agissant de l'exploitation des données sensibles de l'assuré par l'assureur, de santé tout d'abord, ce dernier a la faculté de questionner le futur assuré sur sa santé et sélectionner le risque sans encourir le grief de discrimination et sans violer l'interdiction du traitement de telles données telle que formalisée par l'article 9 du RGPD (art. 8 Loi Informatique et Libertés de 1978). En France, les tests génétiques demeurent interdits néanmoins. L'assuré est ainsi amené à délivrer des informations que l'on peut qualifier, souvent, de données très personnelles, sensibles même. L'objectif est d'offrir un tarif adapté, au plus grand nombre, comme offre d'assurance en contrepartie. Le droit à l'assurance peut alors ne pas être en totale adéquation avec l'obligation d'assurance. La situation paraît plus encore difficultueuse en présence de risques aggravés de santé. Certes, la convention AERAS, s'assurer et emprunter avec un risque aggravé de santé, et ses avenants, ont pour objet de prendre en compte ces risques spécifiques, avec un aménagement spécial des questions de discrimination. Il s'agit donc d'affiner la sélection du risque particulier pour offrir une couverture assurantielle dans certaines limites, grâce à l'amélioration du profil du risque particulier d'une part et de la connaissance des pathologies en général d'autre part. Il ne semble pas être recherché la capacité à l'assurabilité de tout le monde indifféremment.

Question à l'actuaire :

Comment l'actuaire prend-il en compte le nouveau dispositif AERAS dans sa modélisation actuarielle ?

AC : le but d'un modèle actuariel (qu'il s'agisse d'une étude statistique afin de mieux comprendre le risque, ou de la constitution d'un tarif) est de trouver des variables qui pourraient être corrélées à la survenance d'un risque, ou son coût. Dans le dispositif AERAS, un assuré a le droit de ne pas déclarer un cancer passé, dont le protocole thérapeutique est terminé depuis 10 ans, sans rechute. C'est ce que dit la loi. La question importante est de comprendre *comment* cette loi a été élaborée, et en particulier *pourquoi* cette clause a été proposée. Si elle est motivée par des études épidémiologiques, qui montrent que ces personnes ont le même risque de redévelopper un cancer qu'une personne n'ayant jamais eu de cancer diagnostiqué, alors l'actuaire n'a pas de motivation pour essayer de retrouver cette information, car elle n'apporte rien. En statistique, c'est la notion d'indépendance entre des variables (la non-corrélation est une version un peu plus simple) : les évènements A et B sont indépendants si le fait de savoir B n'apporte aucune information sur A. Savoir qu'il pleut à Tokyo ne m'apporte aucune information sur le fait qu'il pleuve à Paris, donc si je fais un modèle météo, je n'ai aucun intérêt à avoir accès à cette information. Ici aussi, si le fait d'avoir eu un cancer il y a 10 ans (et d'avoir survécu, sans rechute) n'influence pas la probabilité d'avoir un cancer aujourd'hui, il n'y a aucune raison de chercher à avoir cette information. Il faut garder en mémoire que les actuaires et les statisticiens qui font de l'épidémiologie ont été souvent formés ensemble, utilisent les mêmes modèles (voire les mêmes logiciels). La situation serait toutefois différente si cette loi avait été votée sur d'autres bases. Si pour des raisons politiques (électoralistes ou éthiques, peu importe – du point de vue du statisticien) il a été décidé de rajouter cette clause, alors que le risque est inchangé, ce n'est pas la même chose. On revient ici sur un problème bien connu en économie d'asymétrie d'information (entre l'assureur et l'assuré), où la solution est de faire révéler l'information (par un moyen détourné) à l'agent le plus informé.

2) L'automatisation des processus décisionnels (profilage)

DCS : Il a été rappelé que le domaine des assurances est intrinsèquement associé à la segmentation tarifaire au sein de la mutualité. Qui dit segmentation dit classement des risques pris en charge en fonctions de critères prédéfinis. Ce mécanisme est par essence de ceux qui bénéficient du développement des procédés modernes d'automatisation des traitements. On parle alors de profilage. Le RGPD évoque sous ce terme « ***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* ».

Dès lors que la conclusion du contrat d'assurance est automatisée (ce qui devrait être de plus en plus fréquent, si l'on pense notamment au développement des assurances en ligne), le rattachement de l'assuré à l'une des catégories tarifaires de l'assureur en fonction de son niveau de risque ne peut mieux répondre à une telle définition. Il semble bien s'agir du profilage visé tant par le Règlement que, avant lui, par la loi Informatique et libertés de 1978. Mais encore faut-il que le *scoring* conduise à une *décision* « *produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* » (élément définitoire du « profilage »), ce qui, si l'automatisation permet d'accepter (ou de refuser) et de tarifer la couverture proposée, ne saurait faire de doute.

Le profilage est interdit en matière de données dites sensibles[17] et le Règlement rappelle le droit des personnes concernées de « *ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé*», mais il en va en revanche autrement dès lors que « *la décision [...] est nécessaire à la conclusion [...] d'un contrat* » (art. 22.2, a). Si bien que celui qui demande à être assuré ne saurait *a priori* s'opposer au profilage qui serait pratiqué par l'assureur à

17 - Sauf consentement de l'intéressé et motif d'intérêt public, validé par le droit d'un État membre (art. 22.4 renvoyant aux exceptions de l'art. 9.2, a ou g)

la souscription. L'assuré se voit néanmoins conférer deux droits spécifiquement associés à une telle hypothèse. L'un concerne le droit d'être informé sur l'existence et la logique sous-jacente du profilage (b). L'autre, auquel nous nous intéresserons en premier lieu, serait celui de pouvoir réintroduire une intervention humaine dans le processus décisionnel (a).

a) La question du droit à une intervention humaine

En cas de décision automatisée sur la conclusion du contrat, le responsable du traitement, ici l'assureur, devra mettre en œuvre certaines mesures, et au moins, respecter le droit de la personne concernée « *d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision* »[18], en bref, dire adieu au traitement automatisé de la décision...

Question à l'actuaire :

L'actuaire dispose-t-il des moyens d'intégrer cette éventualité dans les modèles d'évaluation du risque ? Autrement dit, est-il possible d'élaborer un modèle laissant place le cas échéant à une intervention humaine ?

Quels pourraient être les critères auxquels aurait recours l'intervenant humain et qui n'auraient pas déjà été intégrés dans le processus décisionnel par l'actuaire ? Peut-on selon vous réellement distinguer, dans la pratique assurantielle, des décisions automatisées et des décisions impliquant une « intervention humaine » ?

Enfin, est-il envisageable que le « point de vue » d'un assuré qui contesterait la décision tarifaire (ou d'exclusion de la couverture) puisse changer la décision qui sera prise à son égard par l'assureur ?

AC : Pour l'instant, les modèles sont très artisanaux, dans le sens parfois entendu où l'actuariat est à la fois un art et une science.

18 - RGPD, art. 22.3

L'actuaire choisit quelle variable utiliser, quelle technique permettra de lisser le zonier, quelles interactions sont pertinentes, etc. Mais le « *machine learning* » (et plus généralement toutes les techniques liées à l'intelligence artificielle) propose aujourd'hui des techniques (facilement programmables) qui permettent de ne faire (presque) aucun choix. Historiquement, on avait des modèles très simples, avec des classes de risques très clairement identifiées : une prime de base, un rabais de 15% pour les femmes, une hausse de tarif de 20% pour les personnes habitant en banlieue, et de 30% pour les jeunes conducteurs, puis on rajoute une majoration de 15% pour un véhicule diesel, etc. Puis les modèles sont devenus plus complexes, avec la prise en compte de variables « continues » (l'âge et non plus la classe d'âge, ce qui permet de lisser une baisse ou une hausse tarifaire), mais aussi des croisements de variables (avec une pénalisation pour une classe d'âge spécifique, une zone géographique et un type de véhicule précis, par exemple). Si les modèles étaient plus complexes, les actuaires maitrisaient toujours leur construction. Plus récemment, les actuaires ont découvert l'enrichissement de données, qui implique de lier les données possédées par l'assureur à des bases plus importantes (données sur les caractéristiques du véhicule, sur les caractéristiques du logement, des statistiques sur le quartier où réside la personne, sur les garages à proximité, etc.), il devient impossible de tester la pertinence de *toutes* les variables. Ce problème de grande dimension a été en partie résolu par les techniques de « machine learning » qui proposent une sélection automatique des variables. Il n'est pas étonnant de voir Google ou Amazon intéressés pour entrer sur le marché de l'assurance. Les techniques actuelles sont proches de celles qu'ils développent.

Au-delà du modèle, le tarif repose surtout fondamentalement sur les données. Le même modèle (même le plus simpliste) donnera des primes différentes sur des populations différentes. Le même modèle sur le portefeuille d'assurés d'AXA ou la mutualité de sociétaires de la MAIF donneront des primes (ou des cotisations) très différentes. Contester un prix signifierait qu'il pourrait exister « un prix » à un risque donné. Or rien n'est plus faux. Un risque en assurance ne peut être vu qu'au sein d'un groupe qui cherche à mutualiser le risque, au sein d'une compagnie. La valorisation en assurance n'est pas celle des marchés financiers, où le principe de réplication prévaut. En mathématique financière, deux actifs qui rapportent la même chose

dans tous les états de la nature ont forcément le même prix (sinon via la vente à découvert, il serait possible de gagner de l'argent sans prendre de risque, et de réaliser un « arbitrage »). En assurance c'est impossible. Et il est tout à fait possible d'être vu comme un « bon » risque pour tel assureur, et comme un « mauvais » pour tel autre.

Cela dit, les actuaires proposent un calcul d'une prime dite technique. C'est la prime qu'il conviendrait de demander pour avoir un portefeuille équilibré, et concurrentiel. Mais c'est rarement la prime réellement payée par l'assuré, car il convient d'intégrer une stratégie commerciale, mais aussi le fait que l'activité d'assurance fait intervenir bon nombre d'intermédiaires (entre les agents et les courtiers).

b) La question du droit à l'information sur la logique du profilage

DCS : Le second droit que le RGPD confère à l'occasion de la mise en œuvre d'un profilage, relève plutôt de l'idée de transparence. Ainsi l'article 13 prévoit-il que le droit à l'information de la personne concernée porte notamment sur « *l'existence d'une prise de décision automatisée, y compris un profilage [...] et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée* » (art. 13.2, f).

De fait, cela confère potentiellement à tout assuré le droit de connaitre, et à tout assureur l'obligation de notifier, les critères utilisés par le second pour placer le premier dans telle ou telle catégorie tarifaire, voire si l'on se réfère à la notion de « logique sous-jacente » peut-être même à l'algorithme utilisé pour évaluer son risque.

Question à l'actuaire :

Comment l'assureur pourrait-il satisfaire en pratique à une telle obligation d'information ? Les algorithmes utilisés pour les décisions de tarification ne sont-ils pas des secrets commerciaux ? Et si l'on ne révèle pas l'algorithme, que pourraient être ces « informations utiles concernant la logique sous-jacente » du profilage ? Autrement dit, les algorithmes utilisés comme supports du contrat d'assurance sont-ils susceptibles d'être « résumés » ou vulgarisés ?

AC : Le problème est compliqué. La fonction de l'actuaire est de faire du profilage. C'est aujourd'hui la base de l'assurance. Les algorithmes sont des « secrets commerciaux », mais peut-être moins que les données. En réalité, tous utilisent les mêmes outils, les mêmes techniques. Mais comme ils ont des portefeuilles différents, ils ont des paramètres différents. Par exemple des mutuelles comme la MATMUT ou la MAIF, qui historiquement assurent des fonctionnaires, avaient des portefeuilles très différents d'assureurs privés. Même en construisant le même modèle, les primes demandées sont très différentes. Techniquement, si tous les assureurs expliquaient quelles variables ils utilisent, ça ne changerait pas grand-chose. Fondamentalement, les assureurs connaissent structurellement leur modèle de tarif. Une autre difficulté est de comprendre ce que veut dire « utiliser une variable ». Oui, un assureur va utiliser le modèle du véhicule, parce qu'il peut ensuite obtenir sa côte à l'argus, parce qu'il va en déduire son poids, sa vitesse maximale, sa puissance. Avec le croisement des données, il est complexe d'expliquer lors de la signature du contrat *comment* une information est utilisée, et si elle l'est. De plus, cet enrichissement de données peut donner lieu à de très légers changements, insignifiants, infinitésimaux, mais significatifs. Et qui mis bout à bout ont des conséquences importantes.

Cela dit, la règle peut avoir des conséquences intéressantes : elle permettrait que l'assuré puisse agir sur les variables qui le classent comme un « risque élevé » en demandant une prime plus importante que la moyenne. C'est intéressant, car cela permet de mettre en place de la prévention. Si l'assuré sait que sa prime d'assurance multirisques habitation est élevée, c'est parce qu'il n'a qu'un verrou sur sa porte d'entrée, il a la possibilité d'installer un second verrou, ce qui baissera la prime, mais aussi le risque. En revanche, s'il sait que sa prime d'assurance automobile dépend de la puissance de son véhicule ou du type de carburant, il ne va pas revendre son véhicule pour un acheter un autre. Et souvent, ces variables sont croisées avec d'autres : le carburant ne joue plus via un simple coefficient majorateur (par exemple +20% pour un véhicule diesel), mais le carburant peut-être croisé avec l'âge du véhicule, et le lieu d'habitation. Donc avoir cette information ne servirait pas à grand-chose en pratique.

B. La lutte contre la fraude

DCS : Le fondement d'un traitement de données personnelles dans le cadre de la lutte contre la fraude à l'assurance ne pose pas de problème particulier. Il relève à n'en pas douter de l'intérêt légitime de l'assureur, au sens de l'article 6.1.f du RGPD qui confirme en substance le régime antérieur du droit français[19]. La « prévention de la fraude » est d'ailleurs visée au premier chef dans le considérant 47 comme illustrant un intérêt légitime du responsable de traitement. À ce titre, seront licites tant l'exploitation des données initialement collectées pour une autre fin (par ex. pour l'appréciation du risque dans le questionnaire d'assurance) que les nouvelles collectes de données susceptibles d'établir la fraude (ex. activités de l'assuré depuis le sinistre).

Si le traitement est donc *a priori* licite, la recherche des cas de fraudes est néanmoins susceptible de générer des pratiques qu'il convient de confronter au droit spécial des données personnelles, voire à d'autres règlementations intimement liées à la protection de la vie privée. Ainsi, après le processus de sélection et de tarification des risques, la question du profilage se pose de nouveau en matière de détection de la fraude (1°). On retrouve par ailleurs naturellement certaines difficultés liées à la question de la loyauté de la preuve (2°).

1) La question du profilage des fraudeurs

Les analyses prédictives ne se cantonnent pas au domaine du risque et se retrouvent parfois également dans le cadre de la lutte antifraude. Ainsi *Aviva Assurances* a démarré un projet de croisement numérique de ses dossiers internes de fraudes afin de créer des modèles par corrélation de cas avérés et compte ainsi détecter les 4/5e du potentiel de cas qui échapperaient encore à

19 - V. spéc. sur ce point l'autorisation unique (AU) élaborée par la CNIL : Délibération n° 2014-312 du 17 juillet 2014 portant autorisation unique de traitements de données à caractère personnel ayant pour finalité la lutte contre la fraude à l'assurance mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurance (AU 039)

sa cellule antifraude[20]. L'utilisation de scores prédictifs (*scoring* de suspicion des sinistres) permettrait ainsi de décupler les potentialités en matière de traque à la tricherie. Si ce type de profilage (au sens commun du terme) semble pour l'instant à un stade expérimental, il n'en relève pas moins du droit de la protection des données sur lesquelles il s'appuie.

Or, la question ne peut être envisagée ici de la même manière qu'à la conclusion du contrat. En effet, contrairement à ce qui se passe lors de l'évaluation du risque, il ne devrait pas y avoir par hypothèse de *décisions* basées sur un traitement automatisé, ce qui définit le profilage au sens du RGPD. Si l'assureur peut s'appuyer sur des logiques prédictives et des processus automatisés pour déceler plus facilement les cas de fraude, il ne saurait *a priori* refuser d'indemniser un assuré sur ce seul fondement. En effet, le droit des assurances et les règles du droit civil commun ne permettront à l'assureur de se dégager de son obligation de garantie qu'en cas de fraude avérée. Or, l'on voit mal comment il pourrait se contenter pour cette démonstration du seul traitement automatisé du dossier de l'assuré[21].

Le directeur sinistre de Groupama évoquait un outil en phase test qui permettrait de mettre en évidence une anomalie. Et de conclure : « *soit la manœuvre frauduleuse est immédiatement révélée*[22]*, soit des investigations complémentaires d'enquêteurs certifiés sont nécessaires* ». À en croire les termes de cette déclaration, le refus d'indemniser serait susceptible de résulter en pratique d'un processus automatisé de traitement des données. S'il ne s'agit que d'un lapsus, il pourrait du moins révéler le souhait d'éviter à terme certains coûteux processus d'enquêtes. Les conditions dans lesquelles le RGPD admet le profilage permettent pourtant de douter de cette possibilité puisque dans ce cas, le traitement « humain » et la logique contradictoire devront être réintroduits sur demande

20 - L'argus de l'assurance.com, Dossier spécial « Fraude », 4 / 8, *Le big data sera-t-il la nouvelle arme antifraude ?*, Eloïse Legoff - Publié le 03 septembre 2015 - , consulté le 22.11.17.

21 - L AU n° 39 en matière traitement de données ayant pour finalité la lutte contre la fraude, indiquait déjà que « les requêtes ou alertes détectées automatiquement doivent donner lieu à une analyse non automatisée par le personnel habilité de l'organisme [...] , le cas échéant des investigations complémentaires pourront être diligentées ».

22 - Surligné par nous.

de l'intéressé[23]. Il reste précisément intéressant de comprendre dans quelle mesure un traitement automatisé de données serait techniquement capable de justifier le refus d'indemniser, et d'alimenter éventuellement un dossier probatoire.

Question à l'actuaire :

Que pouvez-vous nous dire des analyses prédictives en matière fraude ? De quelles données ont-elles besoin ? Autrement dit, les modèles peuvent-ils être construits sur les seules données communiquées lors de la déclaration du risque et du sinistre, ou nécessitent-elles un apport complémentaire de données, et si oui lesquelles ?

L'idée d'un algorithme établissant un dossier complet d'éléments prouvant la fraude dans un cas particulier est-elle réellement envisageable ? Autrement dit, pensez-vous qu'il soit possible de se passer d'une analyse* in concreto *de la situation de l'assuré, impliquant une intervention humaine d'enquêteurs ou d'analystes spécialisés ?

AC : On peut imaginer des données collectées en ligne. Par exemple voir sur Facebook qu'une personne est au ski, alors qu'elle est supposée être en arrêt maladie. Récemment, un assureur a refusé d'indemniser un assuré, en congé maladie pour neuf mois par suite de blessures aux cervicales, mais qui annonçait, quelques semaines après le début du congé, sa fierté d'avoir fini 7e à une course de 10 km (et sa prochaine participation à un semi-marathon) sur Twitter.

Les données GPS, utilisées pour l'instant dans un objectif de compréhension du risque, ne sont pas encore utilisées lors des accidents. Les marges d'erreur des boitiers sont importantes. Certains assureurs utilisent de l'analyse textuelle, en repérant des phrases ou des mots utilisés majoritairement par des fraudeurs. Il est aussi possible de croiser des données d'un grand nombre d'assurés pour repérer des garagistes qui surfacturent. Mais c'est toujours fait

23 - V. le droit de s'opposer au profilage en dehors du cas où il conditionne la conclusion du contrat, celui d'exiger une intervention humaine et d'avoir sur ce point un débat contradictoire (article 22).

en complément, ou pour créer un score, un profilage, qui ensuite déclenchera ou pas une action (envoi d'un expert par exemple). L'an passé[24], François Nédey, directeur technique assurance de biens d'Allianz France, affirmait « *Si nous soupçonnons de la connivence, nous allons manuellement regarder les données rendues publiques par l'utilisateur. Si nous confirmons un lien sur les réseaux sociaux, nous procédons alors à une enquête pour prouver la fraude* ». Il s'agit de créer des scores, un outil d'aide à la décision, avec de l'analyse automatique de photos à la suite d'un sinistre, une extraction d'information dans un constat amiable, mais aussi de toutes sortes d'information, qui conditionneront l'envoi d'un expert ensuite.

DCS : On en conclura en conséquence qu'il n'y a pas finalement, dans les pratiques actuelles du moins, de « profilage » au sens du Règlement européen, c'est-à-dire de décision prise sur le seul fondement d'un traitement automatisé, dès lors que le *scoring* n'est qu'une alerte destinée à déclencher des investigations complémentaires. Il reste à savoir comment les assureurs gèreront la question de la conservation d'un assuré dans le fichier des fraudeurs potentiels ou confirmés. C'est en effet à eux, en vertu du principe d'*accountability*, que revient maintenant la charge d'apprécier le temps (strictement nécessaire) de la conservation de telles données[25].

2) Lutte contre la fraude et loyauté de la preuve

RB : s'agissant de la fraude, avec les nouvelles technologies et les objets connectés en particulier, le double usage par l'assureur de la donnée personnelle (*primo* pour un suivi de la tarification, *secundo* pour la détection d'une fraude) semble facilité. Il en va de même avec le problème de la lutte contre le blanchiment d'argent sale.

L'Agence pour la lutte contre la fraude à l'assurance (Alfa) a pu indiquer qu'en 2015, les cas de fraude en assurances de dommages ont représenté un coût d'environ 2,5 milliards d'euros, soit 5 % des primes, avec une prédominance en coût pour les dommages

24 - Dans un article de l'Est Républicain daté de septembre 2016 (http://bit.ly/2G4rE9x)

25 - Question que l'AU n°39 de la CNIL réglait en proposant un mécanisme de conservation de la donnée « suspicion » en deux temps : 6 mois, d'une part, le temps de la qualifier (confirmer ou infirmer), puis 5 ans, d'autre part, une fois confirmée.

corporels, car bien que représentant que 2 % des cas, la fraude liée à ces dommages correspond à 47 % de ces 2,5 milliards d'euros. Une source majoritaire de ces dommages corporels provient des accidents de la circulation.

En partageant entre assureurs les informations concernant les conducteurs et les véhicules sur la *blockchain* par exemple, une détection des tentatives de fraude multiassurance pourrait être effectuée, allant même jusqu'au partage d'une note d'évaluation du conducteur qui le suivrait dans le temps pour que les assureurs puissent disposer d'un historique de son profil de conducteur, de son accidentologie ou de ses tentatives de fraudes.

D'un point de vue juridique, deux choses sont à concilier. D'un côté, la jurisprudence retient que la collecte de la preuve doit être loyale[26], à plus forte raison que l'assuré est présumé, en principe, de bonne foi par le Code des assurances. En outre, elle a condamné à plusieurs reprises des opérations de surveillance et de filature, jusqu'à l'intérieur du domicile, menées par les enquêteurs mandatés par l'assureur[27]. D'un autre côté, l'enquête privée devient de plus en plus intrusive et permanente, sans intervention humaine, mais à l'aide d'objets connectés (boîtiers, caméras, capteurs, accouplés ou non à des *smart contracts*) où l'assureur et son personnel non qualifié se substituent directement à la profession d'enquêteurs privés. Or la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure *(JO 19 mars 2003)* a rendu la formation obligatoire des professions d'enquêteurs privés, sauf pour ceux travaillant de façon interne dans une société (d'assurance) pour le seul compte de leur employeur. Le personnel de l'assureur n'est donc pas soumis aux obligations de qualification.

Questions à l'actuaire :

L'évolution rapide de certaines de ces technologies ne laisse-t-elle pas apparaître un risque d'aggravation d'un usage

26 - Cass. ass. plén., 7 janv. 2011, n°s 09-14.316 et 09-14.667, Bull. civ. ass. plén., n° 1.

27 - Cass. 1re civ., 22 sept. 2016, n°15-24.015, Bull. civ. I ; *adde* Schulz R., *Investigations portant atteinte à la vie privée : droit au respect de la vie privée et droit à un procès équitable*, sous CEDH, 3 sect., 18 oct. 2016, n°61838/10, RGDA 2016, n°12, p. 624 et s.

déloyal, voire illicite, de la preuve et/ou de l'enquête privée « digitalisée «, impliquant une collecte cachée de données personnelles à d'autres fins que le déclenchement de la garantie, par exemple pour la lutte contre le blanchiment et/ou contre la fraude à l'assurance ?

L'actuaire peut-il ainsi tenter de limiter certaines pratiques ?

AC : De nombreuses technologies peuvent être intéressantes. Au Brésil, les services fiscaux utilisent des images satellites pour détecter la fraude de déclaration d'agriculteurs en extrapolant les quantités produites et donc les revenus. Un article récent[28] évoquait l'idée que les autorités fiscales pourraient utiliser les drones pour contrôler les propriétés. Mais cette utilisation de drones est vue «comme une ingérence dans la vie privée». Notons toutefois que certains assureurs commencent à utiliser Google Maps (et Street View) pour avoir des informations sur le logement d'une personne. Ces méthodes relèvent toutefois de pratiques de gestionnaires de sinistres (pour vérifier les dégâts d'une tempête par exemple) ou de souscripteurs (pour voir la présence d'un garage) sur lesquels l'actuaire n'a pas la main. En effet, dans une compagnie d'assurance, l'actuaire cherchera à utiliser toutes les données accessibles, pour une mission dont il a la charge, comme proposer un nouveau tarif, proposer un indicateur de risque de fraude potentielle (de fraude à l'assurance). Une fois construit l'indicateur, c'est aux gestionnaires de sinistres de les utiliser : sur la base de suspicions (mauvais score donné par le modèle), le gestionnaire de sinistre pourra chercher des preuves d'une éventuelle fraude. Mais ça ne relève pas de la mission de l'actuaire.

C. Statistiques et recherche actuarielles

DCS : Pour finir sur cet aperçu du cycle de la donnée personnelle en assurance, venons-en au cœur même de l'activité actuarielle. Les informations personnelles d'un assuré ont en pratique vocation à alimenter les bases de données statistiques de l'actuaire chargé des modèles tarifaires d'une mutualité, voire de recherches actuarielles

28 - « Le fisc interdit de drone pour contrôler les propriétés des contribuables » dans Le Figaro du 18 janvier 2018 (http://bit.ly/2Dz19KZ).

de dimension plus large, et ce souvent donc bien après le terme de la relation contractuelle qui a conduit l'assureur à les recueillir. Or, l'on entend ci et là, depuis l'annonce de l'entrée en vigueur prochaine du Règlement européen, que les compagnies d'assurance entendraient se défaire de leurs anciennes données plutôt que de risquer des sanctions pour non-conformité du traitement, ce qui risquerait d'affecter les bases de données actuarielles. Il semble opportun de clarifier un peu la situation sur ce point.

La protection des données personnelles conduit à interroger leur exploitation en dehors du strict cadre de la relation d'assurance à plusieurs égards. Il s'agit d'abord d'élucider le fondement d'un tel traitement (1°), de la question des garanties susceptibles d'être mises en place pour les personnes concernées, ensuite (2°) et enfin de s'interroger sur la portée du « nouveau » droit à l'effacement (ou droit à oubli) consacré par le RGPD (3°).

1) Le fondement du traitement ultérieur des données d'assurés

En principe, les données personnelles dont dispose l'assureur auront été collectées, soit au titre de la déclaration obligatoire des risques (C.ass., art. L. 113-2, 2°), soit, pour les données « sinistre », au titre de l'obligation de déclaration conditionnant le versement de la garantie (C. ass., art. L. 113-2, 4°). Il est admis que l'obligation légale vient sur ce point remédier à une asymétrie d'information incompatible avec la nécessité pour l'assureur d'évaluer le risque qu'on lui demande de prendre en charge et d'exécuter ses engagements. Si donc un droit lui est conféré sur les *données* d'un assuré, c'est dans le cadre du rapport bilatéral né du contrat qu'il passe avec celui-ci (risque individuel), ce qui ne préjuge en principe pas de ses prérogatives en matière de gestion de sa mutualité (risque collectif). L'analyse n'est pas vraiment différente si l'on se place du point de vue du Règlement. La collecte des données « risque » ou « sinistre » relèvera *a priori* d'un traitement « *nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles* ». De là à douter de la possibilité pour l'assureur de procéder ultérieurement à une exploitation actuarielle des données d'assurés, du moins sans consentement spécifique, il n'y a qu'un pas : parce que, d'une part, les prérogatives conférées à l'assureur par le Code des assurances ne se justifient que dans la mesure où il

s'agit de gérer le lien contractuel avec l'assuré, et parce que, d'autre part, le Règlement soumet le traitement des données au principe de limitation des finalités (art. 5.1, b).

L'assureur devrait néanmoins pouvoir invoquer son intérêt légitime (à équilibrer économiquement sa mutualité) pour fonder une exploitation des données au-delà du contrat (RGPD, art. 6.1, f). Les intérêts et droits fondamentaux des assurés pourraient prévaloir sur l'intérêt de l'assureur s'ils « ne s'attendent raisonnablement pas à ce traitement ultérieur »[29]. Cela étant, ils devront en tout état de cause être informés de ce traitement[30] et notamment du fait qu'ils disposent dans cette hypothèse (fondement sur l'intérêt légitime) d'un droit d'opposition (art. 21).

Plus directement, le Règlement autorise un traitement à des fins différentes du moment que celles-ci sont *compatibles* avec les finalités initiales (art. 5.1, b). Cette compatibilité s'apprécie au regard de plusieurs critères[31], dont le premier cité est le lien entre les finalités successives, ce qui s'agissant d'apprécier un risque individuel et le risque collectif de la mutualité dans lequel il s'est inséré ne semble pas faire de doute. Ce lien sera cependant insuffisant à lui seul pour justifier la *compatibilité,* et devra s'accompagner d'autres circonstances, notamment l'existence de garanties appropriées, « *dont le chiffrement ou la pseudonymisation* ».

Par ailleurs, le Règlement reprend la solution de la Directive de 1995[32] selon laquelle le traitement ultérieur à des fins statistiques, historiques ou scientifiques est réputé compatible avec les finalités initiales du traitement (art. 5.1, b, *in fine*). Pour l'instant, le droit français n'envisage à ce titre que les études et bases de données d'intérêt public. Or, si l'on en croit le considérant 159 dudit

29 - Considérant 47

30 - Art. 13 et 14 du RGPD et art. 32, I de la loi Informatique et Libertés.

31 - Énoncés par l'article 6.4 qui en dénombre cinq : lien entre les finalités initiales et ultérieures, contexte de la collecte, nature des données, conséquences pour l'intéressé et enfin garanties appropriées.

32 - Article 6.

Règlement[33], il n'est pas totalement exclu que cette hypothèse puisse recouvrir les études et statistiques actuarielles réalisées pour le compte des assureurs puisque, nous dit-on, le terme de *recherche*« *devrait être interprété au sens large et couvrir, par exemple [...] la recherche appliquée et celle financée par le secteur privé* ». La question d'une telle assimilation devra être discutée, mais si elle était admise, le travail actuariel resterait en tout état de cause soumis à l'exigence de mesures techniques et organisationnelles garantissant les droits et libertés de la personne concernée. C'est ce que rappelle l'article 89.1 *in fine*, tout en ajoutant que « *chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière* ».

2) L'existence de garanties appropriées, dont la pseudonymisation

En définitive, pour pouvoir être exploitée ultérieurement, la donnée d'assuré aurait donc au premier chef vocation à être « modifiée » pour perdre en tout ou partie son caractère *identifiant* (anonymisation ou pseudonymisation).

S'agissant de la donnée anonyme, celle-ci est par hypothèse exclue du champ de la protection des données dites « personnelles ». Ce tout simplement parce que les deux termes sont antinomiques, la donnée personnelle supposant la faculté d'identification. En anonymisant les données d'assuré, l'assureur devrait pouvoir les soumettre sans difficulté au travail actuariel. Cependant, compte tenu de ce qui a pu être démontré sur le pouvoir du croisement d'informations, l'anonymisation de données « risque » ou « sinistre » parait difficilement praticable. La technique de la « pseudonymisation », quant à elle, n'enlève pas son caractère personnel à la donnée, mais permet d'en alléger le régime. Le terme désigne une sorte d'anonymisation réalisée *a minima*, en ce qu'elle n'est pas définitive. Le Règlement définit la pseudonymisation comme le « *traitement de données à caractère personnel de telle façon que celles-ci ne*

33 - Il y est notamment dit qu'« Aux fins du présent règlement, le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large et couvrir, par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé »

puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (art. 4.5).

Il convient néanmoins d'observer que, dans le cas particulier des études ou bases de données d'intérêt public, il est précisé que la contrainte liée à l'identification des personnes concernées n'existe que « *dans la mesure où ces finalités peuvent être atteintes de cette manière* ». Si donc le traitement actuariel bénéficiait de cette qualification, il pourrait être dispensé de l'anonymisation ou de même de pseudonymisation chaque fois que ladite technique viendrait à l'entraver.

Mais en définitive, que la nécessité de faire perdre aux données leur caractère identifiant soit absolue ou relative, cela soulève la question de la compatibilité de cette exigence avec l'exploitation actuarielle des données d'assurés.

Question à l'actuaire :

Les méthodes de travail de l'actuariat d'assurance sont-elles ou peuvent-elles être construites à partir de données anonymisées ? Ou de données simplement pseudonymisées ? Sinon, quels sont les avantages de disposer de données permettant l'identification directe ou indirecte de la personne de l'assuré ?

AC : Encore une fois, le but n'est jamais d'identifier les gens. Latanya Sweeney a étudié[34] un exemple resté fameux (et relatif à des problèmes d'assurance), à savoir les déclarations annuelles obligatoires de *Group Insurance Commission* (GIC) au Massachusetts, aux États-Unis. Cette institution semi-publique a pour mandat d'offrir des contrats d'assurance santé aux employés de l'État du Massachusetts (135 000 personnes), mais avait obligation de fournir des statistiques

34 - L. Sweeney, 2002, k-anonymity: a model for protecting privacy (http://bit.ly/2DqTbQA)

agrégées sur son portefeuille. Par date de naissance, genre et code postal, l'assureur devait fournir des informations sur les visites et les remboursements médicaux. En utilisant les données électorales de la ville de Cambridge, six personnes partageaient la date de naissance du Gouverneur William Weld, trois seulement étaient des hommes, et il a été aisé de retrouver son code postal. Instantanément, il a été possible d'identifier sans erreur aucune le Gouverneur, et d'avoir des informations non publiques sur son état de santé.

Pseudonymiser les données est un exercice complexe. En particulier en assurance habitation où il est nécessaire de connaître le lieu de résidence précis. En assurance automobile, à partir de l'âge, du code

postal et du modèle de véhicule, plus de la moitié du portefeuille serait identifié avec certitude dans une ville de taille raisonnable. Il n'y a aucun avantage, aucun intérêt à le faire. Mais le fait est que les actuaires peuvent très souvent identifier les données sur lesquelles ils travaillent. Des travaux théoriques sont en cours sur l'utilisation de techniques d'encryptage pour la construction de modèles prédictifs. Mais l'exercice est complexe (et trop technique) pour la discussion que nous avons ici.

3) Le droit à l'effacement

DCS : Il reste en tout état de cause une autre difficulté. En effet, protéger les données en les encryptant ou en les dépouillant de tout ou partie de leur caractère identifiant suppose de les avoir conservées, du moins d'avoir été en mesure de le faire. Or, la question du « nouveau »[35] droit à l'effacement consacré par le Règlement européen est de nature à affecter les bases de données d'assurance s'il devait être exercé massivement dans une mutualité. Comme Pascal l'a montré il y a déjà longtemps avec la loi des grands nombres, la fiabilité de la prédiction suppose de pouvoir se fonder sur un nombre élevé de données d'expérience. Les conditions d'exercice

35 - En France, le droit n'est en effet que « formellement » nouveau dès lors que la possibilité de demander la suppression de ses données existe « substantiellement » depuis la Loi Informatique et Libertés de 1978 : il s'exerce alors dans le cadre de la mise en œuvre d'un droit plus large incluent le droit de rectification (LIL, art. 40). V. également, le droit au déréférencement consacré dans l'arrêt Google Spain rendu par la CJUE le 13 mai 2014 (affaire C-131/12) sur le fondement de la Directive de 1995.

du droit à l'effacement (RGPD, art. 17) permettent cependant de nuancer l'observation.

D'abord, parce que le droit est exclu si l'on se trouve face à un traitement relevant de fins statistiques ou de recherche scientifique (RGPD, art. 89) dont l'effacement « *est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs* ». La question de la qualification de l'actuariat d'assurance ressurgit ici. Si l'on admet que cette activité est couverte par l'article 89, l'assureur n'a pas à redouter le droit à l'effacement. Le droit ne pourrait jouer que si cela ne constitue pas un véritable obstacle à ses études actuarielles. Il restera peut-être à s'entendre sur l'appréciation de la gravité de l'entrave...

Ensuite même si le droit à l'effacement n'était pas exclu (actuariat ne relevant pas de l'article 89), la menace que ce droit constitue doit être relativisée parce qu'il suppose en substance que le traitement ne soit pas ou plus fondé. C'est le cas lorsque ses finalités sont épuisées, ou lorsque l'intéressé a exercé son droit d'opposition sans que le responsable du traitement ait de motifs impérieux de s'y opposer. Or, l'exploitation actuarielle des données d'anciens assurés n'est pas, *a priori,* une finalité qui a vocation à s'épuiser rapidement. Il faudrait pouvoir imaginer un risque que l'on aurait plus de raison légitime d'observer, parce qu'il aurait disparu, ou parce que la mutualité aurait radicalement changé de composition... En bref, l'assuré qui voudrait exercer son droit à l'effacement devrait donc justifier au préalable d'un droit d'opposition à l'exploitation ultérieure de ses données (art. 21).

La vigueur du droit d'opposition de l'assuré dépendra alors du fondement que l'on reconnaitra au traitement actuariel. De deux choses l'une. Soit l'on retient l'« *intérêt légitime* » de l'assureur à alimenter les statistiques de sa mutualité, et alors le droit d'opposition suppose non seulement d'invoquer des « *raisons tenant à sa situation particulière* », raisons qui devront encore être confrontées aux « *motifs légitimes et impérieux* » de l'assureur (art. 21.1). Soit l'on considère que l'actuariat d'assurance relève de l'article 89, et le droit d'opposition supposera toujours que l'assuré puisse justifier de « *raisons tenant à sa situation particulière* », sous réserve cette fois que le traitement ne soit pas « *nécessaire à l'exécution d'une mission*

d'intérêt public ». Or, si l'on admet l'application de l'article 89 aux études actuarielles et aux statistiques assurantielles, c'est qu'on leur aura déjà en principe reconnu un certain intérêt public.

On le voit la marge de manœuvre en matière de traitement post-contractuel des données d'assurés suppose de trancher deux questions. L'une est de déterminer si le fait d'accorder à l'assuré un droit à l'effacement de ses données après le terme du contrat (et l'écoulement des délais de prescription) compromettrait « gravement » les études actuarielles. L'autre est de se demander dans quelle mesure il est légitime d'assimiler ces études à la recherche scientifique, voire à des missions d'intérêt public, et partant de leur accorder un statut dérogatoire au regard des droits des personnes concernées[36].

Question à l'actuaire :

Quel regard portez-vous sur ce droit à l'effacement (ou à l'oubli) et la menace qu'il représente pour l'actuariat d'assurance ?

Pensez-vous qu'il serait légitime d'assimiler le travail que l'actuaire effectue sur les données d'assurés à la notion de « recherche scientifique » ou de « fins statistiques » visée par le RGPD, afin de limiter les droits des assurés sur leurs données ? Dans quelle mesure peut-on considérer que les études utiles aux assureurs, personnes privées, sont assimilables à celles faites dans l'intérêt public ?

AC : Pour illustrer le débat, on peut regarder les pratiques de certains assureurs. La MAIF par exemple propose une « charte numérique »[37],

36 - À l'heure où ce « dialogue » est en voie de publication, le projet de loi français d'adaptation de la loi de 1978 au RGPD (AN, n°490, 15e législature) ne semble pas aller dans cette voie. L'article 12 du projet prévoit en effet que « *les conditions et garanties appropriées prévues à l'article 89 du règlement (UE) 2016/679 sont déterminées par le code du patrimoine et les autres dispositions législatives et réglementaires applicables aux archives publiques. Elles sont également assurées par le respect des normes conformes à l'état de l'art en matière d'archivage électronique* », ce qui indique une vision plus restrictive des hypothèses de l'article 89 qui se limiteraient plutôt aux activités des personnes ou services publics.

37 - Charte Numérique de la MAIF, en ligne le 2 février 2018 (http://bit.ly/2AhVOpv)

avec un premier volet sur la « protection de données personnelles ». On y parle de « respecter », d'« être transparent », de « sécuriser » et surtout d'« oublier ». Pour être plus précis, le dernier point est énoncé de la manière suivante « Dans une société de la mémoire, le droit à l'oubli devient un droit fondamental. Chacun peut nous demander à tout instant la suppression des données qui le concernent, dans le respect de nos obligations de conservation ». Cette déclaration peut sembler généreuse, dans l'esprit des directives récentes, mais si on pousse le raisonnement jusqu'au bout, que faire si tout le monde utilise ce droit ? Comment les actuaires vont-ils pouvoir tarifer si tout le monde exerce ce droit, et qu'il n'existe plus de données pour faire des calculs statistiques ? Il est toutefois mentionné une « obligation de conservation ». Il existe effectivement quelques obligations : dans le code des assurances, des délais de prescriptions sont mentionnés. Par exemple, l'article L.114-1 dit que « *toutes actions dérivant d'un contrat d'assurance sont prescrites par deux ans à compter de l'événement qui y donne naissance* ». Autrement dit, il y a une obligation de conserver pendant deux ans. Ce délai de deux ans fait l'objet de deux exceptions : « *la prescription est portée à dix ans dans les contrats d'assurance sur la vie lorsque le bénéficiaire est une personne distincte du souscripteur et, dans les contrats d'assurance contre les accidents atteignant les personnes, lorsque les bénéficiaires sont les ayants droit de l'assuré décédé* » (alinéa 4) et « *pour les contrats d'assurance sur la vie... les actions du bénéficiaire sont prescrites au plus tard trente ans à compter du décès de l'assuré* » (alinéa 5). Il existe donc en effet des obligations pour conserver des données.

Mais au-delà de cette « obligation » de conservation, l'article 89 du RGPD mentionne surtout un « droit de conservation » correspondant à un « traitement à des fins archivistiques », en lien avec un « intérêt public ». Ce point est important et essentiel pour les actuaires, mais pas seulement. Certains mécanismes d'assurance ont été mis en place dans un « intérêt public », comme l'assurance contre les catastrophes naturelles (loi du 13 juillet 1983). Pour améliorer le système de couverture et d'indemnisation, il pourrait être dans l'intérêt public de faire des études sur certaines catastrophes récentes. Or pour étudier ces risques rares, il convient d'utiliser des sinistres sur une longue période temporelle. Pour comprendre le risque centenaire, utiliser deux ans d'historique n'aidera pas beaucoup. Or combien d'assureurs ont encore des données personnelles relatives aux tempêtes de 1999 (vieilles de

moins de 20 ans) ? En 2005[38], la CNIL avait introduit le concept de « données définitives » (présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction). Ne faudrait-il pas imaginer un système permettant d'archiver, au niveau national, certaines de ces données, à des fins de recherche ? S'il existe une distinction entre les données détenues par des personnes « privées » et des personnes « publiques », comme traiter le cas des catastrophes naturelles, qui fonctionne sur un mécanisme d'acteurs privés, mais dont la prime est fixée par décret gouvernemental ?

Avril 2018

38 - Délibération n°2005-213 du 11 octobre 2005

RECHERCHE EN SANTÉ ET PROTECTION DES DONNÉES PERSONNELLES À L'HEURE DU RGPD

Frédérique Lesaulnier
Docteur en Droit,
Déléguée à la protection des données de l'INSERM

Les données personnelles de santé sont un enjeu de premier plan pour la recherche dans le domaine de la santé. Elles sont le matériau de recherche de base pour les scientifiques et ces données représentent un fort potentiel de contribution à la santé individuelle et collective. C'est pourquoi leur exploitation représente une opportunité de première importance. Cela suppose que ces données sensibles soient exploitées avec la plus grande rigueur, l'expertise et l'esprit critique nécessaires et dans le respect du cadre éthique et réglementaire.

Or, le contexte normatif dans lequel s'inscrivent les activités de recherche est en plein bouleversement. La réglementation relative à la protection des données personnelles est emblématique des « turbulences normatives » tant au plan européen que national.

Le Règlement européen 2016/679 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 (ci-après RGPD[1]) est devenu le texte de référence dans l'ensemble des États membres de l'Union européenne (UE) depuis le 25 mai 2018. Grâce à la disposition relative au « ciblage », les acteurs situés en dehors de l'UE ne pourront pas s'affranchir de ces règles dès lors qu'ils traitent des données relatives aux résidents européens.

Ce règlement est applicable directement sans transposition nationale. Toutefois, il laisse d'importantes marges de manœuvre aux États membres pour maintenir ou adopter des spécificités nationales pour certains types de traitements parmi lesquels les traitements qui portent sur les données de santé, les données génétiques, le numéro d'identification national et les traitements à

1 - « Règlement général sur la protection des données »

des fins de recherche scientifique (art.9.4). Le législateur français a usé de ce pouvoir de subsidiarité et la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles qui a modifié la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés consacre un nouveau chapitre IX aux traitements de données à caractère personnel dans le domaine de la santé applicable aux recherche, études et évaluations dans ce domaine. La bonne compréhension du cadre juridique suppose donc d'articuler le RGPD et le droit national, ce qui en fait un règlement sui generis à mi-chemin entre un règlement et une directive. La technique retenue aboutit à un résultat peu satisfaisant en termes de lisibilité du droit pour les acteurs. C'est pourquoi le Gouvernement a été autorisé à effectuer par voie d'ordonnance ultérieure n° 2018-1125 du 12 décembre 2018, une mise en cohérence de l'ensemble de la législation applicable en matière de protection des données personnelles.

En outre, en matière de recherche dans le domaine de la santé, la nouvelle loi « Informatique et Libertés » modifiée doit elle-même être articulée avec le cadre national applicable à la recherche en santé et, notamment, l'ensemble des dispositions du code de la santé publique applicables issues de la loi du 26 janvier 2016 de modernisation de notre système de santé qui crée le Système National des Données de Santé (SNDS) et de la réglementation applicable aux recherches impliquant la personne humaine (RIPH) issue de la loi n°2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine et de l'ordonnance n° 2016-800 du 16 juin 2016 relative aux recherches impliquant la personne humaine.
L'application du RGPD devra aussi se faire dans le cadre plus global du mouvement de la «science ouverte»afin de promouvoir une ouverture des données de la recherche nécessaire à l'amélioration des connaissances et des soins pour les patients, respectueuse de la protection des données personnelles.

Il en résulte un cadre juridique relatif à la protection des données personnelle applicable à la recherche complexe et difficile à appréhender auquel les communautés de recherche accompagnées des institutions dont ils relèvent doivent se conformer.

§1 : Le RGPD et la place que les activités de recherche scientifique y occupent

A. Vers une responsabilisation accrue des acteurs

Le RGPD est un acte normatif de portée générale qui n'est propre ni à la santé ni à la recherche.

Ce texte modifie l'approche de la protection des données personnelles en s'invitant au cœur de la stratégie, de la gouvernance et de l'organisation des acteurs. Alors que le régime de protection des données antérieur reposait en grande partie sur l'existence de formalités préalables, le RGPD repose sur une logique de conformité et de responsabilité. Il ne s'agit plus seulement pour les acteurs d'effectuer des demandes d'autorisation auprès de la CNIL, ils doivent aussi s'assurer, au moment du montage d'un projet qui implique un traitement de données personnelles, puis tout au long de la vie du projet, en pleine responsabilité, du respect des principes de protection des données et, surtout, ils doivent à tout moment être en mesure de le démontrer en cas de contrôle de la CNIL. Cela suppose le développement de politiques de conformité dites d'«accountability» placées sous le pilotage du délégué à la protection des données qui devront se traduire concrètement par un travail documentaire, la mise en œuvre et la formalisation de procédures, l'utilisation d'outils et la réalisation d'audits permettant d'attester du niveau de conformité.

La sécurité des données personnelles qui est une composante majeure de la conformité des traitements à la législation de protection des données est érigée par le RGPD en condition de licéité des traitements et le renforcement des règles en la matière accentue fortement cette dimension (obligation de mener des analyses d'impact sur la vie privée et les libertés (PIA) pour les traitements qui présentent un risque élevé pour les droits et libertés des personnes ; Privacy by design, privacy by default).

Le développement d'architectures mutualisées permettant de maîtriser la diffusion des données auprès d'acteurs variés (recours aux API (information programming interface), tout en proposant un ensemble de fonctionnalités et présentant des garanties de

conformité technique et réglementaire certifiées est indispensable, mais suppose un changement de paradigme et d'importants moyens.

B. Une évolution plus qu'une révolution dans la régulation

Pourtant, il faut voir dans le RGPD une évolution bien plus qu'une révolution. Il existe un cadre juridique riche et ancien qui définit les conditions d'utilisation d'accès et d'utilisation des données personnelles de santé et qui traduit le caractère sensible de ces données.

Ce cadre général de la protection des données repose en Europe sur le principe selon lequel la protection des données à caractère personnel est un droit fondamental inscrit dans la loi (Charte des droits fondamentaux de l'Union européenne, art.8§1).

L'application de ce cadre juridique est subordonnée à l'existence d'un traitement de données à caractère personnel, c'est à dire susceptibles de permettre la possibilité d'identifier la personne, que cette identification soit directe ou indirecte par référence à un identifiant ou tout élément qui lui soit propre et qui, seul ou avec d'autres (un faisceau de données), permet de remonter à son identité.
Sur la pseudonymisation dont il donne une définition, le Règlement est très clair : les données pseudonymisées sont des données à caractère personnel indirectement identifiantes (considérant 26). Par conséquent, la pseudonymisation des données (qui n'est pas une anonymisation) ne conduit pas à soustraire ces données à l'application du règlement (considérant 28).

Les données sont dites pseudonymes lorsque l'attribution à une personne concernée nécessite le recours à des informations supplémentaires.
Le RGPD précise que les clés de réidentification doivent être « conservées séparément et soumises à des mesures techniques et organisationnelles » afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique (RGPD, art. 4.5).

Cette définition couvre différentes techniques couramment utilisées en matière de recherche en santé :
- le recours à une table de correspondance entre le jeu de données

pseudonymes (codées) et les données d'identité conservées séparément, classiquement utilisée dans les essais cliniques;
- les fonctions de hachage utilisées avec un secret qui permettent de chaîner des données relatives à un individu et de suivre son parcours dans le temps sans permettre de l'identifier (Déclaration obligatoire des maladies, PMSI, SNIIRAM...).
Dans la mesure où les données pseudonymisées restent rattachées à la personne concernée par un identifiant (par exemple une clé ou un code de cryptage), ce sont des données à caractère personnel indirectement identifiantes. Elles restent soumises à l'application de cette réglementation, à la différence des données anonymisées pour lesquelles les clés de ré-identification ne sont plus disponibles.

Le Règlement favorise la pseudonymisation des données en matière de recherche car elle permet de limiter la gravité des impacts potentiels pour les droits et libertés des participants à la recherche, notamment en cas d'atteinte à la confidentialité des données.
Elle est présentée comme une garantie appropriée inhérente au traitement de données à caractère personnel à des fins de recherche scientifique dès lors qu'elle est compatible avec la finalité du traitement (art. 89).

Les données de santé, parce qu'elles relèvent de l'intimité de la vie privée des personnes, sont des données qui doivent faire l'objet d'une protection particulière. À ce titre, le droit leur reconnaît un statut particulier et impose le respect de règles ayant pour objet de garantir leur confidentialité. Elles sont ainsi soumises à un principe d'interdiction de traitement, sauf pour un certain nombre d'exceptions qui permettent ce traitement, prévues par la loi et assorties de garanties (de fond et de procédure) au respect desquelles une autorité administrative indépendante disposant de pouvoirs de sanction accrus veille.

Ces principes de fond sont les suivants : une finalité de traitement déterminée, explicite et légitime, un fondement de licéité du traitement précis, des données adéquates, pertinentes et proportionnées au regard de l'objectif poursuivi (principe de minimisation des données), une durée de conservation déterminée à l'avance et dont la pertinence est appréciée au regard de cette finalité (droit à l'oubli), le respect du droit des personnes qui passe en premier lieu par le principe de loyauté et de transparence des

traitements et enfin, la mise en place de mesures de sécurité de nature à garantir la confidentialité des données.

Les principes posés demeurent pour l'essentiel inchangés dans le RGPD. À noter toutefois que le RGPD accentue fortement les exigences en matière de sécurité (art. 5.1.f). C'est une composante majeure de la conformité des traitements à la législation de protection des données s'agissant du traitement de données de santé dont la CNIL a toujours fait une priorité renforcée.

Les données de santé figurent toujours dans la liste des «catégories particulières de données» et les données génétiques, qui étaient considérées par la CNIL comme des données sensibles, y sont désormais expressément mentionnées. La nouveauté est que l'on y trouve désormais une définition à l'échelle européenne de la donnée de santé, une définition large et englobante. Les « données concernant la santé » sont ainsi définies comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne » (RGPD, article 4 éclairé par le considérant 35). Celles-ci ne concernent plus seulement les données qui permettent d'indiquer la pathologie dont peut être atteint un individu (données de santé « par nature »), mais sont étendues à toute donnée sur l'état de santé physique et mentale, présent, passé ou futur de la personne, toute information sur l'identification du patient dans le système de soins, toutes les prestations de services de santé, toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source (données de santé « par destination »). Les données génétiques sont également définies comme « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question » (art. 4.13).

C. Place des activités de recherche dans le RGPD

Plusieurs dispositions du RGPD témoignent d'une prise en considération des intérêts de la recherche scientifique qu'elles favorisent.

Le considérant 159 donne une définition très large de ce que recouvre la notion de « recherche scientifique » : «Aux fins du présent règlement, le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large et couvrir, par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé. Il devrait, en outre, tenir compte de l'objectif de l'Union mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, consistant à réaliser un espace européen de la recherche. Par fins de recherche scientifique », il convient également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique».

1) Une dérogation au principe d'interdiction de traiter des catégories particulières de données

Le RGPD reprend le principe d'interdiction de traitement des données « sensibles » ainsi que les dérogations à ce principe (prévues à l'article 9.2) parmi lesquelles on retrouve les motifs d'intérêt public, y compris dans les domaines de la santé publique, de la recherche scientifique et des statistiques, moyennant un certain nombre de garanties (art. 9-II-j).

Le RGPD souligne explicitement l'importance et l'intérêt pour la société des traitements effectués à des fins de recherche scientifique ou historique (considérants 156 et 157) et le texte insiste sur la légitimité des activités de recherche, à condition qu'elles respectent les garanties appropriées prévues dans le droit de l'Union ou le droit des États membres.

2) Une présomption de compatibilité de la finalité de recherche scientifique avec une finalité initiale différente et possibilité de conservation à ces fins au-delà de la réalisation de la finalité du traitement

Le RGPD exige que les données soient « collectées pour des finalités déterminées, explicites et légitimes », et ne soient pas « traitées ultérieurement de manière incompatible avec ces finalités ». Toutefois, il pose le principe d'une présomption de compatibilité des traitements ultérieurs à des fins statistiques, de recherche scientifique ou historique qui constituent une base légale suffisante moyennant certaines garanties (RGPD, art. 5 b). La loi «Informatique et Libertés» comportait une disposition similaire (art. 6. 2).

Cette présomption dispense les chercheurs de collecter eux-mêmes les données sur la base du consentement des personnes, ce qui ne les dispense pas d'informer les personnes concernées et d'obtenir une autorisation s'il y a lieu.

De la même manière, la durée de conservation initiale des données peut être prolongée pour répondre aux fins de recherche scientifique.

Le RGPD prévoit à son article 5 que les données ne peuvent être conservées « sous une forme permettant l'identification des personnes concernées » que pendant « une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Néanmoins, une dérogation est admise à ce principe de limitation de la durée de conservation lorsque les traitements sont réalisés à des fins de recherche scientifique sous réserve de la mise en œuvre de mesures techniques et organisationnelles appropriées (art. 5-1-c).

3) Des modalités d'exercice des droits adaptées

Le rôle des patients ou des personnes à l'origine des données est crucial et leurs droits à donner leur accord et à être informés doivent être respectés. C'est l'application d'un principe de transparence et loyauté qui est renforcé par le RGPD (art. 12).

Pourtant, il est indispensable de concevoir des modalités d'exercice des droits susceptibles de garantir une réutilisation de données pour une meilleure compréhension des mécanismes pathologiques, tout en garantissant une meilleure maîtrise par les personnes des données et échantillons biologiques qui les concernent.

Le RGPD permet le recueil d'un consentement « pour une ou plusieurs finalités spécifiques » (art. 6.1.a) ce qui suppose que les finalités aient été déterminées et que la personne concernée en ait été informée. Il résulte de la lecture du considérant 33 du Règlement qu'une finalité spécifique est compatible avec un consentement global. Ce considérant prévoit, en effet, que les personnes concernées devraient pouvoir donner leur consentement « pour ce qui concerne certains domaines de la recherche scientifique dans le respect des normes éthiques reconnues en matière de recherche scientifique ». La personne concernée serait alors en mesure d'accepter que ses données soient utilisées dans le cadre de différents projets de recherche susceptibles d'être menés dans une branche ou un domaine particulier. À noter toutefois que les considérants apportent des précisions qui permettent d'éclairer sur l'esprit du texte mais ne priment pas sur les articles du Règlement.

Ces dispositions doivent être conciliées avec le principe d'une information individuelle et spécifique à chaque projet conforme aux dispositions des articles 13 et 14 qui renforce les obligations de transparence. Cette exigence est difficilement compatible avec les projets reposant sur une réutilisation secondaire de données ou d'échantillons biologiques collectés à cette fin. C'est le cas des cohortes, notamment celles financées par le programme investissement d'avenir, qui ont vocation à mettre leurs données à la disposition de la communauté des chercheurs.

Comme le souligne Georges Dagher au sujet des biobanques, « (...) il est temps de repenser le rôle des personnes-sources plus largement en termes de participation et de contribution à la recherche (...). Le nouveau paradigme développé par l'utilisation des collections biologiques et visant à créer une ressource pour la recherche invite à une évolution du cadre réglementaire et éthique qui régit la question de la participation des patients aux projets de recherche et l'utilisation des données génomiques»[2].

2 - Le Monde paru dans le supplément Sciences & Santé du mercredi 8 juillet 2015

À cet égard, il faut saluer l'évolution de la doctrine de la CNIL sur ce point, illustrée par le projet de méthodologie de référence MR004[3]. Celle-ci admet que l'information puisse être considérée comme valablement délivrée dès lors que les personnes avaient été informées de la réutilisation possible de leurs données et/ou échantillons biologiques lors de la collecte initiale et que l'information initiale renvoie à un dispositif spécifique d'information auquel les personnes pourront se reporter avant la mise en œuvre d'un nouveau traitement (par exemple un site internet). Ce type d'approche apparaît de nature à favoriser l'utilisation des données en recherche tout en préservant l'autonomie des patients qui deviennent de véritables parties prenantes au projet, et par conséquent, à favoriser la confiance indispensable des personnes concernées.

À noter également le maintien de la possibilité de déroger à l'obligation d'information en cas de réutilisation secondaire des données lorsque l'information individuelle se révèle impossible ou exigerait des «efforts disproportionnés», ou dans la mesure où l'obligation d'information est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement sous réserve de garanties appropriées, notamment de pseudonymisation.

Aux termes de l'article 17 du RGPD, et du considérant 65, le «droit à l'effacement» ne s'applique pas et la conservation ultérieure des données à caractère personnel déjà collectées peut être licite dès lors que le traitement des données personnelles est nécessaire à des fins de recherche scientifique, conformément à l'article 89, dès lors que «l'exercice de ce droit risque de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement» (art. 17.3 d).

Cela suppose là encore la mise en œuvre de garanties appropriées pour les droits et libertés des personnes qui peuvent comprendre la pseudonymisation, voire l'anonymisation des données, dans la mesure où les finalités peuvent être atteintes de cette manière et une information des personnes concernées sur ce point au moment où elles donnent leur accord à participer à l'étude.

3 - Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004)

4) La promotion de codes de conduites sectoriels élaborés en lien avec les communautés scientifiques concernées

Le RGPD fait la promotion des codes de conduite sectoriels, construits avec les acteurs de terrain et fondés sur les retours d'expérience. Les organismes de recherche en lien avec les communautés scientifiques ont un rôle majeur à jouer afin de bâtir une corégulation exigeante et efficace qui prenne en compte les évolutions scientifiques et techniques de la recherche et qui soit conforme aux réalités du terrain. En ce sens, la CNIL mène des concertations auprès des acteurs de la recherche sur l'élaboration de projets de méthodologies de référence destinés à encadrer les pratiques. L'INSERM s'est ainsi avec d'autres acteurs de la recherche fortement mobilisé en lien avec les communautés de recherche pour apporter une réponse à la consultation lancée par la CNIL aux projets de méthodologies de référence[4] et s'implique activement dans l'élaboration de codes de conduite.

§2 : L'impact de la loi du 6 janvier 1978 modifiée en 2018 sur la recherche dans le domaine de la santé

La France a pleinement usé des marges de manœuvre laissées aux États membres en prévoyant dans le cadre de la nouvelle loi « Informatique et Libertés » un nouveau chapitre IX intitulé « Traitements de données à caractère personnel dans le domaine de la santé ». Ce nouveau chapitre introduit un régime général applicable à l'ensemble des traitements de données de santé (section 1) ainsi que des dispositions spécifiques additionnelles applicables aux traitements réalisés à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé (Section 2).

Les traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé sont soumis aux dispositions de ces deux sections, sauf dérogations des dispositions spécifiques de la section 2 aux dispositions générales de la section 1.

4 - publiées au JO du 13 juillet 2018

A. Le maintien d'un régime d'autorisation pour les traitements réalisés à des fins de recherche, d'étude oud'évaluation dans le domaine de la santé

Pour les recherches, études et évaluations dans le domaine de la santé, un régime d'autorisation est maintenu, à moins que les traitements ne soient réalisés par des personnels soumis au secret professionnel assurant le suivi médical afin d'effectuer des études destinées à leur usage exclusif.

Le maintien par la loi précitée de cette procédure complexe spécifique à la recherche dans le domaine de la santé qui fait intervenir des organismes distincts selon que la recherche implique ou non la personne humaine (CPP, CEREES et INDS[5] le cas échéant), contraste avec l'esprit d'allègement des formalités porté par le Règlement et à la procédure applicable à d'autres types de recherche telles que les recherches en sciences humaines et sociales (sur l'insertion professionnelle, les discriminations, la diversité ethnique. . .) ou les recherches menées sur internet à partir de données qui ne sont pas sensibles a priori mais qui peuvent le devenir pas recoupement (données prédictives de comportement) qui ne sont pas soumises à un régime d'autorisation. Pour la recherche en santé, la procédure d'autorisation vient en complément de l'autorégulation des pratiques qui incombe désormais aux acteurs et pose, en l'état la question des moyens nécessaires à cette double exigence. Enfin, les procédures sont à nouveau en passe d'être modifiées par le projet de loi relatif à l'organisation et à la transformation du système de santé qui élargit le SNDS et crée le Health Data Hub (Plateforme des Données de Santé), qui sera une évolution de l'INDS actuel.

Toutefois, trois évolutions notables méritent d'être soulignées :

- La possibilité pour la CNIL d'homologuer des référentiels, règlements types et méthodologies de référence en concertation avec les organismes publics et privés représentatifs (et avec l'INDS qui se substitue au CEREES) est maintenue et ces normes deviennent le

5 - Comité de protection des personnes - Comité d'Expertise pour les Recherches, les Études et les Évaluations dans le domaine de la Santé - Institut national des données de santé.

principe. À terme, avec la multiplication des normes de simplification homologuées par la CNIL, les démarches à effectuer auprès d'elle vont diminuer. Il est donc nécessaire de poursuivre l'élaboration de nouvelles normes simplifiées qui s'inscrivent dans l'esprit du RGPD et permettent de construire avec les communautés scientifiques concernées une régulation exigeante, efficace et réactive.

- le silence de la CNIL après deux mois, renouvelables une fois, vaut acceptation à condition toutefois que l'avis ou les avis rendus préalablement soient « expressément favorables ») (art. 54).

- Un comité d'audit du SNDS est mis en place afin d'accroître les contrôles de sécurité pour le SNDS dont la composition et le fonctionnement ont été précisés par le décret d'application de la loi relative à la protection des données du 1er août 1978.

B. Le champ d'application territorial de la loi française

Le législateur a choisi d'instaurer un critère de rattachement territorial particulier pour les spécificités françaises. La loi française d'applique « dès lors que la personne concernée réside en France », et ce « y compris lorsque le responsable de traitement n'est pas établi en France ».

L'article 5-1 vise spécifiquement les règles nationales prises en application du RGPD, dans le cadre des marges de manœuvre laissées par le règlement aux États membres, correspondant notamment aux dispositions du chapitre IX de la LIL.

Ainsi, en application de l'article 5-1 de la LIL, le chapitre IX section 2 a vocation à s'appliquer dès lors qu'une personne concernée par le traitement réside en France, quel que soit le lieu d'établissement du responsable de traitement.

Le RGPD quant à lui s'applique dans deux cas :

- l'existence d'un établissement du responsable du traitement ou du sous-traitant sur le territoire de l'Union que le traitement ait lieu ou non sur le territoire de l'Union;

- le fait que le traitement cible des résidents européens (offre de biens ou de services de personnes dans l'Union ou suivi de leur comportement au sein de l'UE

Le cumul des règles d'application territoriale est source de complexité pour les responsables de traitement établis à l'étranger, hors de l'Union européenne ou dans un autre État membre, qui réalisent des traitements de données relatives à des personnes résidant dans plusieurs États membres, et qui doivent appliquer, en plus des dispositions du RGPD (selon les critères de l'article 3 du RGPD), et autres éventuelles dispositions nationales, les dispositions de la loi française si une personne concernée réside en France.

La recherche en santé se situe de façon croissante dans un contexte collaboratif national et international. Dans ce contexte, les conditions locales de régulation de l'accès aux données constituent un enjeu majeur pour la compétitivité française. Il est donc important qu'une attention particulière soit portée aux lois nationales qui seront applicables aux traitements mis en œuvre à des fins de recherche dans le domaine de la santé dans les autres pays européens afin d'éviter la mise en concurrence des systèmes juridiques au détriment de la recherche française.

DONNÉES PERSONNELLES ET TRANSPARENCE DE LA VIE PUBLIQUE

Charles-Édouard Sénac
Professeur à l'Université de Bordeaux
CERCCLE (EA 7436)
CURAPP ESS (UMR 7319)

« *Je n'ai pas, je n'ai jamais eu de compte à l'étranger, ni maintenant, ni avant* »
Jérôme Cahuzac, le 5 décembre 2012, à l'Assemblée nationale.

« On nous parle souvent de corruption, de fortunes scandaleuses. Pour connaître de quel côté a été la corruption, je demande que chaque député soit tenu de donner l'état détaillé de sa fortune ; que cet état soit imprimé ; et que celui qui aurait fait un faux bilan soit déclaré infâme », s'exclama un membre de la Convention nationale lors de la séance du 14 mai 1793[1]. Aussitôt formulée, la proposition suscita la controverse au sein des révolutionnaires. Pour Cambacérès, la mesure « est sans utilité pour la chose publique ; elle est de plus immorale, et ne tend à rien moins qu'à compromettre la propriété et la sûreté de chacun de nous ». Le girondin Buzot la juge, en l'état, insuffisante. À ses yeux, la chambre doit décréter que « tous les députés à l'Assemblée constituante, à l'Assemblée législative, ou à la Convention, dont la fortune s'est accrue [depuis les débuts de la Révolution], seront tenus de déclarer, dans le délai d'un mois, par quels moyens ils l'ont augmentée, sous peine d'être condamnés à dix années de fers, et d'avoir leurs biens confisqués ». La Convention adoptera finalement, sur la proposition de Barbaroux, une déclaration de principe suivant laquelle « *les représentants du peuple sont à chaque instant comptables à la Nation de l'état de leur fortune* ». Et, deux années plus tard, elle consacrera la position défendue par le défunt Buzot, reprise par un autre girondin, Garrau. Le 4 vendémiaire an IV, elle décrète que « *chaque représentant du peuple sera tenu, dans le délai d'une décade, et dans celui de deux décades pour ceux qui sont négociants ou marchands, de déposer au comité des décrets la déclaration, écrite et signée par*

1 - *Archives parlementaires*, vol. 64, séance du 14 mai 1793, p. 676.

chaque déclarant, de la fortune qu'il avait au commencement de la Révolution et de celle qu'il possède actuellement ; que cette déclaration sera imprimée et envoyée à toutes les communes, pour y être publiée, affichée, et soumise à la censure publique »[2]. Ainsi, la transparence de la vie publique était née.

La postérité de ces décrets révolutionnaires, au demeurant peu appliqués, sera faible, voire nulle[3]. L'idée de soumettre les élus à des obligations de déclaration des éléments de leur patrimoine – ou d'autres données personnelles – dans le but de contrôler leur intégrité et leur probité, tombe rapidement dans l'oubli. Il faut attendre la Cinquième République et la réaction législative à l'un de ses premiers scandales politico-financiers pour que l'exigence juridique de transparence de la vie publique voit véritablement le jour. Le scandale en question est l'affaire de la « Garantie foncière », du nom de la société civile de placement immobilier impliquée dans une vaste affaire d'escroquerie, dans laquelle le député UDR André Rives-Henrÿs, proche de Jacques Chaban-Delmas et ancien directeur de la société, fut inculpé d'escroquerie, d'abus de confiance et d'abus de biens sociaux, puis finalement condamné pour usage irrégulier de son titre de député à des fins publicitaires[4]. La réaction du législateur, initiée par l'Exécutif, consiste dans l'adoption de la loi organique du 24 janvier 1972, dont l'article 3 instaure une double obligation déclarative à la charge des députés et sénateurs[5]. Chaque parlementaire doit, d'une part, dans les huit jours qui suivent son entrée en fonction, « *déclarer au bureau de l'Assemblée à laquelle il appartient toute activité professionnelle qu'il envisage de conserver* » et, d'autre part, « *déclarer toute activité professionnelle nouvelle qu'il*

2 - *Bulletin des lois de la République française*, vol. 6, n° 1132.

3 - Sur l'adoption du décret du 4 vendémiaire et sa mise en œuvre, v. P. Bourin, Démocratie tronquée, Convention transparente. Les Deux Tiers au crible des déclarations individuelles d'état-civil et de patrimoine, Annales historiques de la Révolution française, 2015, n° 381, p. 155-187.

4 - Les dirigeants de la « Garantie foncière » avaient mis en place une escroquerie sur le modèle de la « pyramide de Ponzy » pour attirer plusieurs dizaines de milliers d'investisseurs. Sur cette affaire, v. J. Garrigues, *Les scandales de la République. De Panama à l'affaire Cahuzac*, Nouveau Monde éditions, 2013, coll. « Poche-Documents », p. 273 et s.

5 - La loi renforce également le régime des incompatibilités parlementaires. Sur ce point, v. F. Ancel, *Les incompatibilités parlementaires sous la Vème République*, PUF, coll. « Travaux et recherches de l'Université de droit, d'économie et de sciences sociales de Paris », série « Science politique », n° 4, 1975, p. 77 et s.

envisage d'exercer » au cours de son mandat[6]. Depuis cette date, les déclarations obligatoires intègrent l'arsenal parlementaire de lutte contre les manquements à la probité des élus, à côté d'autres mesures telles que l'établissement d'une commission d'enquête ou le renforcement du régime des incompatibilités. La transparence de la vie publique revient périodiquement dans l'agenda du législateur, le plus souvent lorsqu'un scandale dégrade l'image de la classe politique française et accrédite l'idée d'une perte de confiance des citoyens dans leurs représentants. En 1988, les deux premières lois en matière de transparence financière de la vie politique sont adoptées à la suite des affaires « Luchaire »[7] et « Carrefour du développement »[8]. Elles exigent le dépôt obligatoire d'une déclaration de patrimoine pour un certain nombre de dirigeants publics, ainsi que pour les candidats à l'élection présidentielle, et créent une commission chargée de les contrôler[9]. En 1995, la législation relative aux déclarations de patrimoine des élus est sensiblement renforcée[10] dans un contexte marqué par de nombreux scandales politiques[11]. En 2013, même si

6 - Loi organique n° 72-64 du 24 janvier 1972 modifiant certaines dispositions du titre II de l'ordonnance n° 58-998 du 24 octobre 1958 portant loi organique relative aux conditions d'éligibilité et aux incompatibilités parlementaires.

7 - L'affaire « Luchaire », du nom de la société française accusée d'exportation illégale d'armes à destination de l'Iran entre 1983 et 1986 et soupçonnée de financement illégal du parti socialiste, éclate en 1987. Elle implique plusieurs personnalités politiques, dont le ministre de la Défense de l'époque, Charles Hernu. Sur cette affaire, v. J. Garrigues, *op. cit.*, p. 387 et s.

8 - L'affaire « Carrefour du développement », du nom d'une association créée en 1983 à l'initiative du ministre délégué à la Coopération et au développement, Christian Nucci, éclate en juin 1986 lorsque son successeur, Michel Aurillac, diffuse un rapport de la Cour des comptes dévoilant que plusieurs millions de francs de fonds publics ont été détournés par les responsables de l'association. Sur cette affaire, v. J. Garrigues, *op. cit.*, p. 395 et s.

9 - Loi organique n° 88-226 du 11 mars 1988 et loi n° 88-227 du 11 mars 1988 relatives à la transparence financière de la vie politique.

10 - Loi organique n° 95-63 du 19 janvier 1995 relative à la déclaration de patrimoine des membres du Parlement et aux incompatibilités applicables aux membres du Parlement et à ceux du Conseil constitutionnel ; loi n° 95-126 du 8 février 1995 relative à la déclaration de patrimoine des membres du Gouvernement et des titulaires de certaines fonctions.

11 - Parmi les scandales ayant éclaté en 1994 figurent l'affaire « Dauphiné News », du nom d'un journal grenoblois créé à l'initiative d'Alain Carignon, qui entraîne en juillet sa démission du gouvernement avant sa mise en examen pour recel d'abus de sociaux, et l'affaire des HLM de la Ville de Paris qui provoque la démission du ministre Michel Roussin en novembre à la suite de sa mise en examen pour recel d'abus de biens sociaux. Un autre ministre, Gérard Longuet, démissionne en octobre avant d'être mis en examen dans deux affaires, l'une relative au financement occulte du Parti républicain et l'autre concernant le financement de sa villa tropézienne. Sur ces affaires, v. J. Garrigues, *op. cit.*, p. 476-478, p. 484-486, p. 456-459 ; J. Georgel, A.-M. Thorel, *Dictionnaire des « affaires ». Argent et Politique*, Éditions Apogée, 1997, p. 50-54, p. 134-146, p. 107-109 et 147-154.

les lois relatives à la transparence de la vie publique s'inspirent des travaux des commissions Sauvé et Jospin[12], la cause première de leur adoption est la retentissante affaire « Cahuzac »[13]. Ces lois instituent une Haute autorité pour la transparence de la vie publique (HATVP), à la place de la commission créée en 1988, amplifient les déclarations obligatoires imposées aux gouvernants, imposent la publication de la « réserve parlementaire »[14] et développent l'accès du public à certaines données personnelles[15]. La dernière réforme en date ne dévie pas du *modus operandi* du législateur : les lois du 15 septembre 2017 pour la confiance dans la vie politique sont le contrecoup des révélations, au cours de la campagne précédant l'élection présidentielle de 2017, sur les emplois familiaux de complaisance par François Fillon[16]. Si les mesures les plus emblématiques de ces lois, comme l'interdiction pour certains responsables publics de recruter comme collaborateur un proche parent ou la suppression de la « réserve parlementaire »[17], ne concernent pas la transparence, ces textes apportent néanmoins des changements au régime des déclarations obligatoires[18].

Le développement des exigences législatives en matière de transparence de la vie publique s'est fait au détriment du droit au respect de la vie privée des élus. En effet, dans la mesure où

12 - La Commission de réflexion sur la prévention des conflits d'intérêts dans la vie publique, présidée par Jean-Marc Sauvé, a présenté ses conclusions le 26 janvier 2011. La Commission de rénovation et de déontologie de la vie publique, présidée par Lionel Jospin, a remis son rapport le 9 novembre 2012.

13 - En décembre 2012, Jérôme Cahuzac, ministre délégué chargé du Budget, est accusé par le site d'information en ligne Mediapart d'avoir possédé des fonds non déclarés sur un compte en Suisse. Il démissionne le 19 mars 2013, après l'ouverture d'une information judiciaire contre X pour blanchiment de fraude fiscale, et finit par avouer les faits le 2 avril 2013. Sur cette affaire, J. Garrigues, *op. cit.*, p. 554 et s.

14 - La « réserve parlementaire » est un ensemble de subventions d'État votées et modifiées en lois de finances initiales ou rectificatives permettant aux parlementaires de soutenir financièrement des investissements de proximité décidés par des collectivités locales et des activités menées par des associations.

15 - Loi organique n° 2013-906 et loi n° 2013-907 du 11 octobre 2013 relatives à la transparence de la vie publique.

16 - Loi organique n° 2017-1338 et loi n° 2017-1339 du 15 septembre 2017 pour la confiance dans la vie politique.

17 - La suppression de la « réserve parlementaire » met logiquement fin à sa publication.

18 - Par ex., à propos de l'obligation désormais faite aux candidats à l'élection présidentielle de déposer une déclaration d'intérêts (art. 1er, de la loi organique n° 2017-1338 préc.).

la transparence entraîne la diffusion de données personnelles (patrimoine, activités professionnelles et bénévoles, rémunérations, etc.), les obligations déclaratives portent nécessairement atteinte au droit à la confidentialité de ces données[19]. Or, en France comme ailleurs, le droit au respect de la vie privée est un droit fondamental pour tout individu, quel que soit son emploi ou à sa fonction[20]. En outre, en France plus qu'ailleurs, les médias et la population sont traditionnellement sensibles à la préservation de la vie privée de leurs dirigeants. Toutefois, la vie privée des puissants n'est plus le sanctuaire qu'elle était il y a une quarantaine d'années. D'une part, l'émotion de la population, à la suite de la divulgation de scandales, financiers ou non, a débouché sur une demande populaire de transparence. D'autre part, les élus eux-mêmes reconnaissent que leur vie privée peut intéresser l'opinion publique et font parfois le choix de la porter à la connaissance du public par le moyen des médias ou l'utilisation des réseaux sociaux.

Quoi qu'il en soit, le maintien d'un dispositif attentatoire au droit à la confidentialité des données personnelles n'est légitime que s'il satisfait à deux exigences élémentaires : l'efficacité du dispositif et la proportionnalité de l'atteinte. Concernant l'efficacité des déclarations obligatoires, il est encore trop tôt pour apprécier l'influence d'un dispositif profondément réformé en 2013 et retouché à plusieurs reprises depuis, tant sur l'objectif éthique – garantir la probité et l'intégrité des responsables publics – que sur la finalité politique – rétablir la confiance des gouvernés dans les gouvernants. S'agissant de la proportionnalité de l'atteinte, trois indicateurs sont, à nos yeux, déterminants pour évaluer sa portée. D'abord, il faut prendre en considération le type de données personnelles dont la communication est exigée : celles qui se rattachent à l'intimité de l'être (santé, convictions, orientation sexuelle, etc.) impliquent, selon nous, une protection accrue par rapport aux autres données personnelles. Ensuite, il faut regarder, d'une part, les personnes soumises à l'obligation de déclarer leurs données et, d'autre part,

19 - Ainsi que le rappelle le Conseil constitutionnel (CC, n° 2013-675 DC, 9 octobre 2013, cons. 6 ; CC, n° 2013-676 DC, 9 octobre 2013, cons. 13 ; CC, n° 2016-732 DC, 28 juillet 2016, cons. 48).

20 - Le droit au respect de la vie privée est garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, tel qu'interprété par le Conseil constitutionnel (CC, n° 99-416 DC, 23 juillet 1999, cons. 45), et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

celles qui ont accès aux données d'autrui. Dans les deux cas, plus le nombre de personnes est potentiellement élevé, plus l'atteinte est forte. Pour que chacun puisse évaluer dans quelle mesure le droit à la confidentialité des données personnelles des responsables publics est atteint par les règles de transparence de la vie publique, nous présenterons les personnes assujetties à l'exigence de transparence (I), puis les données personnelles visées par celle-ci (II) et, enfin, les destinataires des données diffusées au nom de la transparence (III).

§1 : Les personnes assujetties à l'exigence de transparence

Depuis 1972, le cercle des individus assujettis à l'exigence de transparence de la vie publique n'a cessé de s'élargir. Initialement limité aux titulaires des plus hautes fonctions électives, ce sont désormais des dizaines de milliers de personnes qui sont soumises aux obligations déclaratives prévues par le droit français. D'une part, le nombre de fonctions publiques ou privées placées sous surveillance a considérablement augmenté au fil des années (A) ; d'autre part, l'exigence de transparence s'étend désormais à l'entourage familial et professionnel de certains titulaires de fonctions publiques (B).

A. Les fonctions ciblées

Au terme – sans doute provisoire – de l'évolution du champ des fonctions visées par l'exigence de transparence de la vie publique, les secteurs concernés par des obligations déclaratives sont au nombre de quatre.

Le premier secteur est celui des responsables politiques, au sens large du terme. Avec les élargissements successifs réalisés par les lois de mars 1988, de février 1995 et d'octobre 2013, ce sont désormais de nombreuses fonctions qui sont soumises à l'obligation de déposer une déclaration de situation patrimoniale et, depuis 2013, une déclaration d'intérêts. Au niveau national sont visés les titulaires des fonctions de député[21], sénateur[22], député européen[23] et membre du gouvernement[24]. Le Chef de l'État est aussi concerné, de même que

21 - Art. LO 135-1 du code électoral.

22 - Les obligations déclaratives imposées aux députés par le code électoral s'appliquent aux sénateurs en vertu de l'article LO 296 du même code.

23 - Art. 11, § I, 1° de la loi n° 2013-907 préc.

24 - Art. 4 de la loi n° 2013-907 préc.

tous ceux qui ont été déclarés candidats à l'élection à la présidence de la République par le Conseil constitutionnel[25]. Les collaborateurs du Président de la République, du Président de l'Assemblée nationale, du Président du Sénat, et les membres des cabinets ministériels doivent également satisfaire à ces obligations déclaratives[26].

Au niveau local, les déclarations obligatoires imposées au nom de la transparence de la vie publique touchent les titulaires des fonctions de président de conseil régional, président de conseil départemental, président d'une assemblée territoriale d'outre-mer, président élu d'un exécutif d'une collectivité d'outre-mer, de maire d'une commune de plus de 20 000 habitants, et celles de président d'autres organes délibérants ou d'autres organes exécutifs locaux[27]. Depuis avril 2016, les directeurs, directeurs adjoints et chefs de cabinet de ces autorités territoriales sont également visés[28]. Qui plus est, l'exigence de transparence touche les conseillers régionaux, les conseillers départementaux, les conseillers à l'assemblée de Guyane et ceux à l'assemblée de Martinique, les conseillers exécutifs de Martinique et ceux de Corse, les adjoints aux maires des communes de plus de 100 000 habitants et certains vice-présidents des établissements publics de coopération intercommunale[29].

25 - Art. 3, § I, de la loi n° 62-1292 du 6 novembre 1962 relative à l'élection du Président de la République au suffrage universel.

26 - Art. 11, § I, 4° et 5° de la loi n° 2013-907 préc.

27 - Art. 11, § I, 2° de la loi n° 2013-907 préc. Les autres fonctions visées sont celles de président de l'Assemblée de Corse, de président du conseil exécutif de Corse, de président de l'assemblée de Guyane, de président de l'assemblée de Martinique, de président du conseil exécutif de Martinique, de président du conseil de la métropole de Lyon, de président élu d'un établissement public de coopération intercommunale à fiscalité propre dont la population excède 20 000 habitants ou dont le montant des recettes totales de fonctionnement figurant au dernier compte administratif est supérieur à 5 millions d'euros ainsi que les présidents des autres établissements publics de coopération intercommunale dont le montant des recettes totales de fonctionnement figurant au dernier compte administratif est supérieur à 5 millions d'euros.

28 - Art. 11, § I, 2° de la loi n° 2013-907 préc., dans sa version issue de la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires.

29 - Art. 11, § I, 3° de la loi n° 2013-907 préc. Les vice-présidents concernés sont ceux des établissements publics de coopération intercommunale à fiscalité propre de plus de 100 000 habitants et du conseil de la métropole de Lyon lorsqu'ils sont titulaires d'une délégation de fonction ou de signature, respectivement, du président du conseil régional, du président du conseil exécutif, du président du conseil départemental, du maire, du président de l'établissement public de coopération intercommunale ou du président du conseil de la métropole de Lyon.

Deuxièmement, l'exigence de transparence s'étend à de nombreuses fonctions au sein du secteur public. Depuis les lois « Cahuzac » de 2013, les membres des collèges et, le cas échéant, les membres des commissions investies de pouvoirs de sanction, ainsi que les directeurs généraux et secrétaires généraux et leurs adjoints, de nombreuses agences publiques sont assujettis à des obligations déclaratives[30]. Sont aussi concernés le déontologue de l'Assemblée nationale[31], les présidents et directeurs généraux de nombreuses sociétés d'économie mixte, d'établissements publics nationaux à caractère industriel et commercial, de certains offices publics de l'habitat[32], ainsi que les présidents des fédérations sportives et des ligues professionnelles, du Comité national olympique et sportif français et du Comité paralympique et sportif français[33]. Plus généralement, toute personne exerçant un emploi ou des fonctions à la décision du Gouvernement pour lesquels elle a été nommée en conseil des ministres est astreinte à des obligations déclaratives[34].

On peut ajouter à cette liste déjà longue de nombreux agents publics depuis que la loi du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires a étendu à certains agents

30 - La listes des agences, qui comprend notamment la HATVP est, fixée à l'art. 11, § I, 6° de la loi n° 2013-907 préc. On peut y ajouter certains médiateurs visés par l'art. 11, § I, 6° bis de la loi n° 2013-907 préc.

31 - Art. 11, § I, 5° bis de la loi n° 2013-907 préc. À la différence du Déontologue de l'Assemblée nationale qui n'est pas un député, les membres du Comité de déontologie parlementaire du Sénat sont déjà soumis aux obligations déclaratives en leur qualité de sénateur.

32 - Sont concernés les présidents et directeurs généraux des sociétés et autres personnes morales dans lesquelles plus de la moitié du capital social est détenue directement par l'État, des établissements publics nationaux à caractère industriel et commercial, des sociétés et autres personnes morales dans lesquelles plus de la moitié du capital social est détenue, directement ou indirectement, séparément ou ensemble, par sociétés d'économie mixte nationales ou des établissements publics nationaux à caractère industriel et commercial, et dont le chiffre d'affaires annuel, au titre du dernier exercice clos avant la date de nomination des intéressés, est supérieur à 10 millions d'euros, des offices publics de l'habitat gérant un parc comprenant plus de 2 000 logements au 31 décembre de l'année précédant celle de la nomination des intéressés, des autres sociétés et personnes morales dont le chiffre d'affaires annuel, au titre du dernier exercice clos avant la date de nomination des intéressés, dépasse 750 000, dans lesquelles les collectivités régies par les titres XII et XIII de la Constitution, leurs groupements, leurs établissements publics industriels et commerciaux, leurs sociétés d'économie mixte possèdent, directement ou indirectement, plus de la moitié du capital social ou sont mentionnés au 1° de l'article L. 1525-1 du code général des collectivités territoriales (art. 11, § III de la loi n° 2013-907 préc.).

33 - Art. 11, § III bis de la loi n° 2013-907 préc.

34 - Art. 11, § I, 7° de la loi n° 2013-907 préc.

publics la quête de transparence[35]. Avant cette loi, certains d'entre eux étaient certes déjà assujettis à des déclarations obligatoires. À ceux entrant dans le champ d'application de la législation d'octobre 2013, s'ajoutaient certains agents travaillant dans le domaine de la santé publique et soumis, depuis la réaction législative au scandale du Médiator, à des obligations déclaratives[36]. En 2016, le législateur a manifesté son intention d'élargir encore plus le champ des agents publics placés sous surveillance. Il a habilité le pouvoir réglementaire à fixer les listes des emplois et fonctions dont le niveau hiérarchique ou la nature justifie que le fonctionnaire, l'agent contractuel ou le militaire l'occupant ou en voie de l'occuper soit soumis à des déclarations obligatoires[37]. Les emplois et fonctions concernés sont détaillés dans deux décrets du 28 décembre 2016 pour la fonction publique[38] et un décret du 2 février 2018 pour le personnel militaire[39]. Conformément à ce qu'avait souhaité le législateur, le

35 - Loi n° 2016-483 préc.

36 - Le Mediator est un médicament, mis au point et commercialisé par les Laboratoires Servier en 1976, qui se compose d'une molécule, le benfluroex, laquelle peut être à l'origine de graves troubles cardiaques. En dépit de plusieurs mises en garde, son autorisation de mise sur le marché ne sera suspendue que le 25 novembre 2009 par l'Agence française de sécurité sanitaire des produits de santé, puis retirée le 20 juillet 2010. Un rapport de l'Inspection Générale des Affaires Sociales dénoncera plus tard le comportement des laboratoires Servier « qui, pendant 35 ans, sont intervenus sans relâche auprès des acteurs de la chaîne du médicament pour pouvoir poursuivre la commercialisation du Mediator », ainsi que « l'incompréhensible tolérance de l'Agence à l'égard du Mediator » et « les graves défaillances du système de pharmacovigilance » (IGAS, 15 janvier 2011, « Enquête sur le Mediator », n° RM2011-001P). S'inspirant du *Physician Sunshine Act* voté en 2010 aux États-Unis, la loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé oblige les professionnels de santé et décideurs publics à déclarer leurs liens d'intérêt et elle contraint à divulguer les avantages consentis par les entreprises du secteur à tous les professionnels de santé, ainsi qu'à leurs associations, fondations, sociétés, etc.

37 - Art. 25 ter et 25 quinquies de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ; art. L. 4122-6 et L. 4122-8 du code de la défense ; art. 6 de la loi n° 2016-483 préc.

38 - Décret n° 2016-1967 du 28 décembre 2016 relatif à l'obligation de transmission d'une déclaration d'intérêts prévue à l'article 25 ter de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et décret n° 2016-1968 du 28 décembre 2016 relatif à l'obligation de transmission d'une déclaration de situation patrimoniale prévue à l'article 25 quinquies de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

39 - Décret n° 2018-63 du 2 février 2018 relatif aux obligations de transmission de déclarations d'intérêts et de situation patrimoniale prévues aux articles L. 4122-6 et L. 4122-8 du code de la défense. Initialement, les décrets n° 2017-38 du 16 janvier 2017 et n° 2017-39 du 16 janvier 2017 se bornaient à renvoyer aux listes établies par les décrets du 28 décembre 2016 préc.

périmètre des agents astreints à déclarer leur patrimoine est plus restreint que celui des agents soumis à déclaration de leurs intérêts.

Le troisième secteur auquel ont été étendues les exigences de la transparence est celui de la justice. La loi du 20 avril 2016 a imposé des déclarations de données personnelles aux membres du Conseil d'État[40], conseillers des tribunaux administratifs et des cours administratives d'appel[41], membres et personnels de la Cour des comptes[42], magistrats du siège des chambres régionales des comptes, procureurs financiers et aux personnes mises à disposition pour exercer les fonctions de rapporteur auprès des chambres régionales des comptes[43]. Tous doivent fournir une déclaration d'intérêts, mais seuls le vice-président et les présidents de section du Conseil d'État, les présidents des tribunaux administratifs et des cours administratives d'appel, le premier président, le procureur général et les présidents de chambre de la Cour des comptes, les présidents de chambre régionale des comptes et les procureurs financiers sont soumis à l'obligation de déposer une déclaration de situation patrimoniale[44]. Le législateur organique a souhaité transposer ce système aux magistrats judiciaires et aux membres du Conseil supérieur de la magistrature (CSM). Initialement, la déclaration d'intérêts devait être remplie par tous, et la déclaration de patrimoine par les seuls membres du CSM, premier président et présidents de chambre de la Cour de cassation, procureur général et premiers avocats généraux près la Cour de cassation, premiers présidents des cours d'appel et procureurs généraux près les cours d'appel, présidents des tribunaux de première instance et procureurs de la République près les tribunaux de première instance. Toutefois, le Conseil constitutionnel, au titre de son contrôle obligatoire des lois organiques avant leur promulgation, a jugé contraire au principe d'égalité devant la loi la discrimination établie entre ces magistrats judiciaires et les autres[45], ce qui laisse planer un doute sérieux sur

40 - Art. L. 131-7 du code de justice administrative.

41 - Art. L. 231-4-1 du code de justice administrative.

42 - Art. L. 120-9 du code des juridictions financières.

43 - Art. L. 220-6 du code des juridictions financières.

44 - Art. L. 131-10 du code de justice administrative ; art. L. 120-12 du code des juridictions financières.

45 - CC, n° 2016-732 DC, 28 juillet 2016, cons. 45 et s.

la constitutionnalité des dispositions similaires du code de justice administrative et du code des juridictions financières. En tout état de cause, la censure de la loi organique sur ce point a conduit à supprimer l'obligation de déclaration de situation patrimoniale pour tous les magistrats judiciaires[46]. Désormais, seuls les membres du CSM y sont assujettis ; tous sont en revanche soumis à l'obligation de déclarer leurs intérêts et activités[47].

Enfin, le quatrième secteur visé par l'exigence de transparence de la vie publique ne concerne pas des responsables publics, mais certains de leurs interlocuteurs : les représentants d'intérêts (ou « lobbyistes »), que la loi du 9 décembre 2016 dite « Sapin 2 » définit comme les personnes morales de droit privé, les établissements publics ou groupements publics exerçant une activité industrielle et commerciale, les chambres de commerce et de l'industrie et les chambres des métiers et de l'artisanat, dont un dirigeant, un employé ou un membre a pour activité principale ou régulière d'influer sur la décision publique ou bien comme les personnes physiques qui exercent à titre individuel une activité professionnelle ayant cette finalité[48]. Cette même loi instaure à la charge de ces représentants une obligation de se déclarer auprès de la HATVP et, notamment, de communiquer certaines données relatives à leur personnel[49]. L'identité du représentant d'intérêt ainsi que l'ensemble des données transmises sont mises à la disposition du public grâce à un registre

46 - Le Conseil a également censuré la disposition visant à contraindre ses membres à déclarer leur situation patrimoniale et leurs intérêts au motif que l'amendement parlementaire à son origine était un « cavalier organique », c'est-à-dire une disposition ne présentent pas de lien, même indirect, avec celles qui figuraient dans le projet de loi organique (*ibid.*, cons. 101). Sur ce point, v. J. Benetti, Continuité jurisprudentielle ou (nouveau) revirement ? À propos de la censure de cavaliers organiques par la décision du Conseil constitutionnel du 28 juillet 2016, Constitutions, 2016, p. 396 et s.

47 - Art. 7-2 et 7-3 de l'ordonnance n° 58-1270 du 22 décembre 1958 portant loi organique relative au statut de la magistrature et art. 10-1-1 et 10-1-2 de la loi organique n° 94-100 du 5 février 1994 sur le Conseil supérieur de la magistrature, créés par la loi organique n° 2016-1090 du 8 août 2016 relative aux garanties statutaires, aux obligations déontologiques et au recrutement des magistrats ainsi qu'au Conseil supérieur de la magistrature.

48 - Art. 18-2 de la loi n° 2013-907 préc., dans sa rédaction issue de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

49 - Art. 18-3 de la loi n° 2013-907 préc.

numérique des représentants d'intérêts tenu par la Haute autorité[50]. Ce faisant, la loi prend le relais de pratiques mises en place à partir de 2009 par les chambres pour encadrer l'activité de lobbying auprès des parlementaires[51], en posant des règles contraignantes, comme l'avait suggéré le président de la HATVP dans un rapport remis au Chef de l'État en janvier 2015[52]. Au demeurant, les obligations déclaratives imposées aux représentants d'intérêts sont bien moins intrusives que celles applicables aux responsables publics : aucune déclaration de patrimoine ou déclaration d'intérêts n'est exigée d'eux.

B. Les entourages touchés

La recherche de l'efficacité des mécanismes de déclarations obligatoires destinés à promouvoir l'exemplarité des responsables publics a conduit le législateur à étendre à leurs entourages les effets de la transparence. Sur ce sujet, comme d'autres, l'élargissement de la perspective est l'œuvre des lois d'octobre 2013. Ces dernières ont, comme on l'a vu, contraint les collaborateurs des plus hauts dirigeants politiques à remplir eux-mêmes des déclarations comprenant des données personnelles. Mais elles ont également astreint certains responsables publics à déclarer des informations relatives à leur entourage professionnel ou familial, et donc à divulguer des données personnelles de tiers. Concernant l'entourage professionnel, seuls les parlementaires sont tenus de communiquer des informations personnelles d'autrui : ils doivent indiquer sur leurs déclarations d'activités et d'intérêts « *les noms des collaborateurs parlementaires ainsi que les autres activités professionnelles déclarées par eux* »[53]. En revanche, l'entourage familial de l'ensemble des personnes assujetties aux déclarations obligatoires est touché par les exigences de la transparence de la vie publique. En premier lieu, s'inspirant de l'adage selon lequel « la femme de César doit être au-dessus de tout soupçon », les pouvoirs publics ont décidé que les déclarations d'intérêts et d'activités des responsables publics doivent mentionner

50 - Le répertoire est consultable à l'adresse suivante : http://www.hatvp.fr/le-repertoire. Au 8 février 2017, 958 représentants d'intérêts se sont inscrits.

51 - Sur ces pratiques, v. P. Jan, Le droit parlementaire à l'épreuve du lobbying, Petites Aff., 11 avril 2013, n° 73, p. 4 et s.

52 - J.-L. Nadal, *Renouer la confiance publique*, rapport au Président de la République sur l'exemplarité des responsables publics, 2015 p. 68 et s.

53 - Art. LO 135-1, § III 10°, du code électoral.

les activités professionnelles exercées à la date de la nomination ou de l'élection par leur conjoint, leur partenaire lié par un pacte civil de solidarité ou leur concubin[54]. À l'origine, les déclarations devaient également inclure les activités professionnelles des enfants et des parents, mais le Conseil constitutionnel a jugé que, pour ces proches, l'atteinte au droit au respect de la vie privée était disproportionnée et, partant, s'y est opposé[55]. En second lieu, la déclaration de situation patrimoniale doit préciser à chaque fois si le bien déclaré est un bien propre, un bien de la communauté ou un bien indivis[56]. Dans ces deux derniers cas, la déclaration de patrimoine du responsable public dévoile, le cas échéant, des informations patrimoniales d'autrui.

§2 : Les données personnelles visées par l'exigence de transparence

La détermination du type de données personnelles soumis à communication dépend de la finalité de la transparence. S'il s'agit de lutter contre l'enrichissement frauduleux des dirigeants publics ou, plus généralement, l'utilisation détournée des fonds publics, les données patrimoniales sont la cible principale, voire exclusive, des obligations déclaratives. À partir du moment où la transparence s'est imposée, plus largement, comme un instrument de lutte contre les conflits d'intérêts, définis par les lois de 2013 comme « *toute situation d'interférence entre un intérêt public et des intérêts publics ou privés qui est de nature à influencer ou paraître influencer l'exercice indépendant, impartial et objectif d'une fonction* », le champ des données dont la communication paraît légitime croît sensiblement. Aux données patrimoniales qui font l'objet d'une déclaration spécifique (A) se sont ajoutées diverses informations qui sont regroupées dans une déclaration d'intérêts (B).

54 - Art. LO 135-1, § III 6°, du code électoral ; art. 4, § III, 6°, et art. 11, §I, de la loi n° 2013-907 préc. ; annexe 3, 6°, du décret n° 2013-1212 du 23 décembre 2013 relatif aux déclarations de situation patrimoniale et déclarations d'intérêts adressées à la Haute Autorité pour la transparence de la vie publique ; art. 7, 6° du décret n° 2016-1967 préc. ; art. R. 131-4, 6° et R. 231-4, 6° du code de justice administrative ; art. R. 120-1 et R. 220-1 du code des juridictions financières ; art. 3 du décret n° 93-21 du 7 janvier 1993 pris pour l'application de l'ordonnance n° 58-1270 du 22 décembre 1958 modifiée portant loi organique relative au statut de la magistrature ; art. R. 4122-37, 6° du code de la défense.

55 - CC, n° 2013-675 DC préc., cons. 29 et 41 ; n° 2013-676 DC préc., cons. 15.

56 - Art. 4, § II, de la loi n° 2013-907 préc.

A. Les données contenues dans la déclaration de situation patrimoniale

Les lois de mars 1988 relatives à la transparence financière de la vie politique constituent la base du système de déclaration obligatoire de la situation patrimoniale des gouvernants. Elles prévoyaient que chaque responsable public concerné dépose une déclaration « *de sa situation patrimoniale concernant notamment la totalité de ses biens propres ainsi que, éventuellement, ceux de la communauté ou les biens réputés indivis* » au moment de son entrée en fonction et une seconde déclaration du même type à la sortie de fonction[57]. Si les lois exigèrent une double déclaration, permettant de contrôler la variation du patrimoine du décideur public et ainsi de s'assurer qu'il n'a pas mis à profit sa fonction pour s'enrichir indument, elles ne détaillèrent pas leur contenu. Les lois de janvier et février de 1995 ne précisèrent pas les éléments devant intégrer les déclarations, mais ajoutèrent l'obligation, pour les déclarants, de communiquer « *toutes les modifications substantielles de leur patrimoine, chaque fois qu'ils le jugent utile* » et exonérèrent les déclarants de l'obligation de déposer une déclaration de sortie dans le cas où ils auraient établi depuis moins de six mois leur déclaration de situation patrimoniale[58].

En 2013, les pouvoirs publics profitent de la profonde refonte du droit de la transparence pour détailler le contenu des deux déclarations de patrimoine dans la loi et le règlement[59]. D'une part, les lois « Cahuzac » précisent que la déclaration initiale doit porter sur les dix éléments suivants : « *les immeubles bâtis et non bâtis* », « *les valeurs mobilières* », « *les assurances vie* », « *les comptes bancaires courants ou d'épargne, les livrets et les autres produits d'épargne* », « *les biens mobiliers divers d'une valeur supérieure à un montant fixé par voie réglementaire* », « *les véhicules terrestres à moteur, bateaux et avions* », « *les fonds de commerce ou clientèles et les charges et offices* », « *les biens mobiliers, immobiliers et les comptes*

57 - Les candidats à l'élection présidentielle n'ayant pas remporté l'élection doivent seulement déposer la déclaration initiale.

58 - Art. 1er de la loi organique n° 95-63 préc. ; art. 1er de la loi n° 95-126 préc.

59 - Avant 2013, la Commission pour la transparence financière de la vie politique avait élaboré un modèle de déclaration de patrimoine qui détaillait son contenu, mais il n'avait pas valeur contraignante. Le modèle en question, ainsi que les rapports de la Commission, sont consultables sur www.legifrance.gouv.fr.

détenus à l'étranger », « *les autres biens* » et les éléments du « *passif* »[60]. La déclaration finale doit mentionner les mêmes éléments, auxquels s'ajoute une présentation des événements majeurs ayant affecté la composition du patrimoine depuis la précédente déclaration, présentation qui n'exonère pas de l'obligation de déclarer, dans un délai de deux mois, toute modification substantielle de la situation patrimoniale. Pour les deux déclarations, les lois d'octobre 2013 exigent que la déclaration de situation patrimoniale indique, pour chaque élément mentionné, s'il s'agit de biens propres, de biens de la communauté ou de biens indivis. D'autre part, un décret du 23 décembre 2013 complète le dispositif législatif en fixant à 10 000 euros le seuil au-dessus duquel un bien doit être déclaré et en déterminant minutieusement les informations devant figurer dans les déclarations patrimoniales[61]. Par exemple, s'agissant de la déclaration de compte bancaire, le déclarant doit indiquer le nom du titulaire du compte, l'établissement teneur du compte, la nature et le numéro de compte, le solde du compte à la date du fait générateur de la déclaration. Pour les immeubles bâtis et non bâtis, il doit mentionner l'adresse, la nature et la superficie du bien, son mode, sa date et son prix d'acquisition, sa nature juridique (bien propre, commun ou indivis), la quote-part du bien détenue par le déclarant ou, le cas échéant, par la communauté, le droit réel exercé sur le bien par le déclarant ou, le cas échéant, par la communauté (pleine propriété, usufruit ou nue-propriété), le montant des travaux effectués, le cas échéant, depuis l'acquisition, la valeur vénale, à la date du fait générateur de la déclaration, de la quote-part du bien détenue par le déclarant ou, le cas échéant, par la communauté.

B. Les données présentes dans la déclaration d'intérêts

Suivant les recommandations de la Commission Sauvé formulées en 2011, reprises par la Commission Jospin en 2012, les lois « Cahuzac » ont consacré dans le domaine de vie publique les dispositifs de déclaration obligatoire d'intérêts. Ainsi que le soulignent les travaux de la Commission Sauvé, ces dispositifs « ont surtout vocation à

60 - Art. 4, § II, de la loi n° 2013-907 préc. ; art. LO 135-1, § II, du code électoral.

61 - Annexes 1 et 2 du décret n° 2013-1212 du 23 décembre 2013 préc. Le décret étend aux « autres biens » visés par les lois de 2013 le seuil de dix mille euros en dessous duquel la déclaration n'est pas obligatoire. En outre il donne un exemple de biens concernés : les comptes courants de société ou les stock-options.

prévenir des situations de conflit d'intérêts ponctuelles et à imposer l'abstention en cas de risque d'un tel conflit. Ils assurent une certaine transparence d'intérêts qui, sans nécessairement justifier immédiatement une mesure contraignante (comme l'obligation de s'en défaire), imposent une certaine vigilance »[62]. La déclaration vise donc à identifier les intérêts qu'un responsable public détient en relation avec les fonctions exercées ou susceptibles de l'être, qui pourraient susciter un doute raisonnable sur son impartialité et son objectivité. De la même manière que pour les déclarations de situation patrimoniale, le législateur et le pouvoir réglementaire ont défini avec précision le contenu des déclarations d'intérêts et d'activités[63]. Plusieurs éléments sont communs à toutes les déclarations ; d'autres diffèrent selon le type de déclarants.

Les informations dont la déclaration est exigée pour tous les responsables publics sont au nombre de six. D'abord, doivent être mentionnées les activités professionnelles donnant lieu à rémunération ou gratification et les activités de consultant exercées à la date de l'élection ou de la nomination et au cours des cinq dernières années précédant la déclaration, la participation aux organes dirigeants d'un organisme public ou privé ou d'une société à la date de l'élection ou de la nomination et au cours des cinq années précédant la date de la déclaration. Pour chacune de ces trois entrées, le déclarant doit préciser l'identification de l'employeur, la description de l'activité exercée, sa période d'exercice et la rémunération ou la gratification perçue annuellement pour chaque activité. La déclaration doit également faire état des participations financières directes dans le capital d'une société à la date de l'élection ou de la nomination, en détaillant le nom de la société, le nombre de parts détenues dans la société et, lorsqu'il est connu, le pourcentage du capital social détenu, l'évaluation de la participation financière, et la rémunération ou la gratification perçue pendant l'année précédant l'élection ou la nomination. En outre, les déclarants doivent mentionner, le cas échéant, les fonctions et mandats électifs exercés à la date de l'élection ou de la

62 - *Pour une nouvelle déontologie de la vie publique*, rapport de la Commission de réflexion pour la prévention des conflits d'intérêts dans la vie publique, remis au Président de la République le 26 janvier 2011, p. 55.

63 - Art. 4, § III, de la loi n° 2013-907 préc. ; art. LO 135-1, § III, du code électoral ; annexes 3 et 4 du décret n° 2013-1212 préc.

nomination, en présentant la nature des fonctions et des mandats exercés, la date de début et de fin de fonction ou de mandat et les rémunérations, indemnités ou gratifications perçues annuellement pour chaque fonction ou mandat. Enfin, obligation est faite aux déclarants, comme on l'a vu, d'indiquer les activités professionnelles exercées à la date de l'élection ou de la nomination par le conjoint, le partenaire lié par un pacte civil de solidarité ou le concubin. Sur ce dernier point, l'étendue des obligations est plus limitée : le déclarant précise l'identité de son conjoint, partenaire, ou concubin et de son employeur et indique l'activité professionnelle exercée, mais non le montant de la rémunération ou la période d'exercice de l'activité.

Une septième information est présente dans certaines déclarations d'intérêts et selon une portée qui diffère : les fonctions bénévoles susceptibles de faire naître un conflit d'intérêts. L'exigence de préciser le nom et l'objet social de la structure dans laquelle ces fonctions sont exercées et la nature de ces activités vaut pour tous les responsables publics, à l'exception des fonctionnaires, agents publics contractuels et militaires exerçant les fonctions ou emplois visés par la loi du 20 avril 2016[64]. De plus, certains déclarants sont contraints de mentionner, non seulement leurs fonctions bénévoles susceptibles de faire naître un conflit d'intérêts, mais également celles de leur conjoint, partenaire, ou concubin. Cette exigence supplémentaire, absente des lois « Cahuzac », s'applique aux juges administratifs et aux juges financiers, mais pas aux magistrats judiciaires[65].

Au sein des responsables publics, certains sont astreints à des obligations déclaratives supplémentaires. La déclaration d'intérêts des députés et sénateurs doit indiquer, comme on l'a vu, les noms de leurs collaborateurs et les autres activités professionnelles déclarées par ces derniers. En outre, la déclaration des parlementaires, ainsi que

64 - Le décret n° 2016-1967 préc. et le décret n° 2018-63 préc., portant application de la loi d'avril 2016, ne comportent pas cette obligation déclarative.

65 - Art. R. 120-1 et R. 220-1 du code des juridictions financières (dans leur rédaction issue du décret n° 2016-1921 du 28 décembre 2016 relatif à l'obligation de transmission de la déclaration d'intérêts mentionnée aux articles L. 120-9 et L. 220-6 du code des juridictions financières ; art. R. 131-4 et R. 231-4 du code de justice administrative (dans leur rédaction issue du décret n° 2017-12 du 5 janvier 2017 relatif à l'obligation de transmission de la déclaration d'intérêts mentionnée aux articles L. 131-7 et L. 231-4-1 du code de justice administrative).

celles qui seront remplies par les candidats à la prochaine élection présidentielle, doivent mentionner les activités professionnelles ou d'intérêt général, même non rémunérées, que l'élu ou le candidat envisage de conserver durant l'exercice de son mandat[66]. Enfin, les lois du 15 septembre 2017 pour la confiance dans la vie politique ont ajouté une rubrique supplémentaire aux déclarations d'intérêts des parlementaires, applicables aux candidats à l'Élysée et aux députés européens[67]. Ces déclarants doivent mentionner les participations directes ou indirectes détenues à la date de leur entrée en fonction qui leur confèrent le contrôle d'une société dont l'activité consiste principalement dans la fourniture de prestations de conseil[68]. À côté de ces règles législatives, les textes internes aux chambres sont également sources d'obligations déontologiques pour les députés et les sénateurs. En effet, l'article 7 du code de déontologie de l'Assemblée nationale oblige les députés à déclarer au déontologue de la chambre « *tout don, invitation à un événement sportif ou culturel ou avantage d'une valeur qu'ils estiment supérieure à 150 euros dont ils ont bénéficié en lien avec leur mandat* » et « *toute acceptation d'une invitation de voyage émanant d'une personne morale ou physique* ». De son côté, l'article 20 bis de l'Instruction générale du Bureau du Sénat prévoit que les sénateurs déclarent « *les invitations à des déplacements financées par des organismes extérieurs au Sénat* [à l'exception de ceux effectués à l'invitation des autorités étatiques françaises ou dans le cadre d'un mandat local], *ainsi que les cadeaux, dons et avantages en nature - à l'exception des invitations à des manifestations culturelles ou sportives en métropole et des cadeaux d'usage - qu'ils pourraient être amenés à recevoir, dès lors que la valeur de ces invitations, cadeaux, dons ou avantages excède un montant de 150 euros* ».

§3 : Les destinataires des données personnelles

La transparence implique une mise à disposition d'informations à destination d'autrui, en d'autres termes un dévoilement. Le cercle des

66 - Art. LO 135-1, § III, 11° du code électoral.

67 - Les représentants français au Parlement européen sont également soumis aux règles déontologiques prévues par le droit parlementaire européen.

68 - Art. LO 135-1, § III, 5° du code électoral (dans sa rédaction issue de l'art. 6 de la loi n° 2017-1338 du 15 septembre 2017).

personnes destinataires des informations dévoilées peut être plus ou moins large. Schématiquement, on peut distinguer deux systèmes de transparence. Le premier met en place une transparence sans publicité, autrement dit une transparence qui préserve en grande partie la confidentialité des données transmises. Le destinataire de la transparence n'est pas le public, mais une (ou plusieurs) autorité habilitée, chargée de contrôler les informations et, *in fine*, de veiller à la probité des décideurs publics. Ce système implique que l'autorité concernée maintienne la confidentialité pour que le public n'ait pas accès aux informations communiquées. Le second système embrasse pleinement la philosophie de Jeremy Bentham selon laquelle « l'œil du public rend l'homme d'État vertueux »[69]. Il instaure une transparence avec publicité des données dévoilées : la population est le destinataire des informations et chacun peut, s'il le souhaite, les consulter. En France, la transparence sans publicité a pendant longtemps été la règle et la transparence avec publicité l'exception. Les lois d'octobre 2013 ont cependant réalisé une avancée majeure dans ce domaine : le public devient – enfin – le destinataire d'informations dont la connaissance est supposée rétablir sa confiance dans ses représentants. Si le droit positif met donc en œuvre les deux types de transparence, le champ de la transparence sans publicité (A) demeure plus vaste que celui de la transparence avec publicité (B).

A. La transparence sans publicité

Aussi paradoxal que cela puisse paraître, la transparence peut exister sans publicité. En effet, le droit peut instaurer une obligation de dévoiler des informations sans pour autant permettre à toute personne d'y accéder. Dans ce cas, une autorité est habilitée pour recevoir ces informations, en contrôler le contenu et veiller au respect de leur confidentialité. Telle a été la particularité du droit français applicable aux responsables publics jusqu'en 2013. Depuis, si certaines déclarations sont rendues publiques, il existe encore des déclarations qui demeurent confidentielles et dont le contrôle impartit exclusivement aux gardiens de la déontologie publique.

69 - J. Bentham, *The Works of Jeremy Bentham*, édité par J. Bowring, William Tait, vol. XIX, 1842, p. 145 ("the eye of the public makes the statesman virtuous").

Le droit français de la transparence de la vie publique est traditionnellement un droit protecteur de la confidentialité des données personnelles. En effet, les lois de mars 1988 ont mis en place un dispositif largement dominé par l'objectif de préserver la vie privée des déclarants. En premier lieu, une seule autorité était, en principe, habilitée à recevoir les déclarations et à en contrôler le contenu : le Bureau de la chambre à laquelle appartient le parlementaire déclarant[70] et la Commission instaurée par la loi pour les déclarations des membres du Gouvernement et des plus hautes autorités locales[71]. Toutefois, pour ces dernières, si le déclarant est aussi parlementaire, le Bureau de la chambre concernée était également destinataire de la déclaration[72]. En outre, les déclarations des candidats à l'élection présidentielle étaient déposées sous pli scellé auprès du seul Conseil constitutionnel qui ne pouvait ouvrir que celle du candidat finalement proclamé élu, en vue de sa publication[73]. En second lieu, les lois de 1988 s'opposent à la publicité des informations contenues dans les déclarations : l'autorité destinataire n'a le droit de les communiquer à autrui qu'avec l'autorisation expresse du déclarant ou de ses ayants droit ou bien sur demande des autorités judiciaires à la condition que cette communication soit nécessaire à la solution du litige ou utile pour la découverte de la vérité. Les lois de 1995 ont réformé partiellement ce système en consacrant le principe d'un gardien unique des déclarations de situation patrimoniale. La Commission pour la transparence financière de la vie politique est alors le destinataire exclusif de ces déclarations, y compris celles des députés et sénateurs[74], à l'exception toutefois de celles des candidats à l'élection présidentielle. Les lois d'octobre 2013, en remplaçant

70 - Art. 5 de la loi organique n° 88-226 préc. Le bureau est la plus haute autorité collégiale de la chambre ; il se compose de son président et de ses vice-présidents, ainsi que de ses questeurs et secrétaires (soit 22 membres pour l'Assemblée nationale et 26 pour le Sénat).

71 - Art. 1er et 2 de la loi n° 88-227 préc. La commission se composait du vice-président du Conseil d'État et des premiers présidents de la Cour des comptes et de la Cour de cassation.

72 - Art. 2 de la loi n° 88-227 préc.

73 - Art. 1er de la loi organique n° 88-226 préc. V. *infra.*

74 - Art. 1er de la loi organique n° 95-63 préc.

la Commission par la HATVP[75], ont maintenu la règle selon laquelle toute déclaration de situation patrimoniale doit être transmise au nouveau gardien de la déontologie de la vie publique, en l'élargissant aux candidats à l'élection présidentielle. Elles font également de la Haute autorité le destinataire systématique, mais pas exclusif, des nouvelles déclarations d'intérêts. Si l'une des innovations majeures des lois « Cahuzac » consiste, comme on le verra, à mettre un terme au caractère secret de certaines informations contenues dans ces déclarations, un grand nombre de données personnelles demeure protégé par le droit au respect de la vie privée. À cet égard, le nouveau dispositif prévoit que la publication d'informations dont la diffusion n'est pas autorisée est passible des peines prévues à l'article 226-1 du Code pénal, soit un an d'emprisonnement et 45 000 euros d'amende[76].

Depuis la loi du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires, la Haute autorité présidée par Jean-Louis Nadal n'est plus l'unique destinataire des déclarations qui demeurent confidentielles. Face à l'augmentation massive du nombre de décideurs publics soumis aux exigences de la transparence, le législateur n'a pas souhaité alourdir outre mesure la charge de travail de la Haute autorité[77]. Seules les déclarations de situation patrimoniale remplies par les fonctionnaires et agents contractuels, militaires, juges administratifs et financiers, magistrats judiciaires et membres du CSM sont communiquées à la Haute autorité qui veille au maintien de leur confidentialité[78]. Les déclarations d'intérêts ne lui sont pas transmises, mais adressées à différentes autorités selon le type de déclarant. Par exemple, le fonctionnaire

75 - La HATVP est une autorité administrative indépendante, dont le président est nommé par décret du président de la République et qui comprend, en outre, 2 conseillers d'État élus par l'assemblée générale du Conseil d'État, 2 conseillers à la Cour de cassation élus par l'ensemble des magistrats du siège hors hiérarchie de la cour, 2 conseillers-maîtres à la Cour des comptes élus par la chambre du conseil ; 2 personnalités qualifiées nommées, l'une par le président de l'Assemblée nationale, l'autre par le Président du Sénat, après avis conforme de la commission des lois de la chambre concernée.

76 - Art. 26 de la loi n° 2013-907 préc.

77 - À ce jour, plus de 15 000 responsables publics déclarent leur patrimoine et leurs intérêts auprès de la HATVP.

78 - Art. 25 quinquies de la loi n° 83-634 préc. ; art. 6, 14, § III et IV, 19, § III et IV, de la loi n° 2016-483 préc. ; art. L. 131-10 et L. 231-4-4 du code de justice administrative ; art. L. 120-12 et L. 220-9 du code des juridictions financières ; art. L. 4122-8 du code de la défense ; art. 7-3 de l'ordonnance n° 58-1270 préc.

qui va être nommé dans l'un des emplois assujettis à l'obligation de déclaration d'intérêts doit préalablement transmettre sa déclaration à l'autorité investie du pouvoir de nomination, laquelle sera chargée, après la nomination, de transmettre ladite déclaration à l'autorité hiérarchique dont relèvera le fonctionnaire dans l'exercice de ses nouvelles fonctions[79]. Le magistrat d'un tribunal administratif ou d'une cour administrative d'appel remet une déclaration de ses intérêts au chef de la juridiction à laquelle il a été affecté et au vice-président du Conseil d'État ; le chef de l'une de ces juridictions transmet sa déclaration au président de la mission d'inspection des juridictions administratives et au vice-président du Conseil d'État[80]. La Haute autorité n'est pourtant pas totalement absente du dispositif de contrôle des déclarations d'intérêts. Les statuts de la fonction publique prévoient que l'autorité destinataire de la déclaration peut, en cas de difficulté pour apprécier si l'agent public déclarant est dans un cas de conflit d'intérêts, transmettre sa déclaration à la HATVP qui, après examen de l'affaire, adressera, le cas échéant, une recommandation en vue de faire cesser le conflit d'intérêts[81]. En tout état de cause, l'ensemble des déclarations dont le dépôt est rendu obligatoire par la loi du 20 avril 2016, ainsi que par la loi organique du 8 août 2016 pour les magistrats judiciaires et membres du CSM, doivent demeurer confidentielles. Les textes prévoient à cet égard que les déclarations de situation patrimoniale et d'intérêts ne sont ni versées au dossier de l'intéressé, ni communicables aux tiers. Sur ce point, leur régime est radicalement différent de celui prévu par les lois d'octobre 2013 pour certaines déclarations.

B. La transparence avec publicité

Pendant longtemps, la population a été tenue à l'écart de la transparence de la vie publique. À la différence de l'Allemagne et du Royaume-Uni, la publicité des déclarations des gouvernants était exclue[82], sauf pour une fonction publique. La loi organique de mars

79 - Art. 25 ter, § I, de la loi n° 83-634 préc.

80 - Art. L. 231-4-1 du code de justice administrative.

81 - Art. 25 ter, § II et III, de la loi n° 83-634 préc.

82 - À propos des déclarations obligatoires des députés, v. C. de Nantois, *Le député : une étude comparative, France, Royaume-Uni, Allemagne*, LGDJ - Lextenso éditions, coll. « Bibliothèque constitutionnelle et de science politique », 2010, t. 136, p. 150 et s.

1988 prévoyait la publication au Journal officiel de la République française, d'une part, de la déclaration de situation patrimoniale du candidat élu Président de la République et, d'autre part, de la déclaration de situation patrimoniale du Président à la fin de son mandat[83]. Les déclarations de patrimoine des autres responsables publics demeuraient confidentielles et les révélations de la presse d'investigation étaient la seule source d'information disponible pour la population. Les lois « Cahuzac » ont ébranlé le système français de la transparence-opaque en organisant la diffusion des déclarations de patrimoine et, dans une plus large mesure, des déclarations d'intérêts. Pour ce faire, deux mécanismes de publicité ont été mis en œuvre : la mise en ligne, sous la forme de données ouvertes, et la consultation en préfecture.

Une donnée ouverte (ou *open data*) est une information qui est librement accessible et réutilisable par tous. Si ce mode de publicité, indissociable de l'essor des nouvelles technologies de l'information et de la communication, est principalement utilisé pour faciliter la consultation d'informations administratives[84], il s'applique à certaines données personnelles des gouvernants depuis 2013. Concernant les déclarations de situation patrimoniale, les lois « Cahuzac » ont instauré une publication en ligne des informations déclarées par les membres du gouvernement, les membres de la HATVP et les candidats à l'élection présidentielle, sous quelques réserves destinées à protéger la vie privée des déclarants, de leur entourage familial ou d'autres personnes. Les déclarations des membres du gouvernement et de la Haute autorité sont mises en ligne par la HATVP dans un délai maximal de quatre mois environ à la suite de leur transmission[85]. Celles des candidats à la présidence de la République sont rendues publiques par la HATVP au moins quinze jours avant le premier tour de scrutin[86]. Dans les deux cas, la

83 - Art. 1er de la loi organique n° 88-226 préc.

84 - La plateforme ouverte des données publiques françaises est accessible à l'adresse https://www.data.gouv.fr/fr.

85 - Art. 5, § I, et 19, § IV, de la loi n° 2013-907 préc. Plus précisément, la HATVP transmet la déclaration à l'administration fiscale qui fournit en retour, dans les 30 jours suivant cette transmission, tous les éléments lui permettant d'apprécier l'exhaustivité, l'exactitude et la sincérité de la déclaration de situation patrimoniale. Puis, la HATVP rend publiques la déclaration dans un délai de 3 mois suivant la réception des éléments.

86 - Art. 3, § I, de la loi n° 92-1292 préc.

loi interdit que soient rendus publics les éléments suivants : l'adresse personnelle du déclarant, les noms du conjoint, du partenaire lié par un pacte civil de solidarité ou du concubin et des autres membres de la famille, les indications, autres que le nom du département, relatives à la localisation des biens, ainsi que les noms des personnes qui possédaient auparavant les biens mentionnés dans la déclaration et, le cas échéant, les noms des autres propriétaires indivis, les noms des usufruitiers, les noms des nus-propriétaires.

Le champ des déclarations d'intérêts mis en ligne sur le site *www.hatvp.fr*, qui accueille également le répertoire numérique sur les relations entre les représentants d'intérêts et les pouvoirs publics, est amplement plus vaste que celui des déclarations de patrimoine. En plus des membres du gouvernement et des candidats à l'élection présidentielle – la publication est alors réalisée dans les mêmes conditions que celles applicables aux déclarations de patrimoine – toutes les fonctions visées par l'article 11 de la loi du 11 octobre 2013 sont touchées. Les responsables politiques, et les agents du secteur public, à l'exception de ceux relevant des régimes de déclarations obligatoires instaurés par la loi du 20 avril 2016, voient leur déclaration d'intérêts accessible en ligne. Ceci étant, certaines informations nominatives ne sont pas publiées par la HATVP pour préserver la vie privée des personnes concernées. Ainsi, il est interdit de divulguer l'adresse personnelle du déclarant, les noms du conjoint, du partenaire lié par un pacte civil de solidarité ou du concubin et des autres membres de la famille et, s'agissant des instruments financiers, les adresses des établissements financiers et les numéros des comptes. On notera, par ailleurs, que la diffusion en ligne des déclarations d'intérêts n'empêche pas leur transmission préalable à d'autres autorités que la HATVP. Par exemple, le bureau de la chambre est destinataire des déclarations d'intérêts des députés et sénateurs[87] et le Premier ministre est destinataire des déclarations d'intérêts des membres du Gouvernement[88].

La mise en ligne des déclarations des responsables publics constitue une avancée majeure pour la transparence démocratique qui, pourtant, ne s'applique pas intégralement aux premiers représentants

87 - Art. LO 135-1, § I, du code électoral.

88 - Art. 4, § I, al. 2, de la loi n° 2013-907 préc.

de la Nation que sont les députés et les sénateurs. Dans le but de limiter la publicité de leurs déclarations de patrimoine par rapport à celles des ministres, les parlementaires ont opté pour une modalité de consultation qui paraît archaïque. Elles ne sont pas publiées sous la forme de données ouvertes, mais tenues à la disposition des personnes inscrites sur les listes électorales qui peuvent les consulter en préfecture, mais non les reproduire ou les réutiliser[89]. En revanche, les mêmes omissions d'informations nominatives sont faites que pour les déclarations de situation patrimoniale des membres du gouvernement. Bien que ce mode de publicité tronquée ait été critiqué, notamment, par l'organe anticorruption du Conseil de l'Europe[90], le législateur français n'a pas souhaité le modifier. Malgré cette résistance des parlementaires, la diffusion en ligne des données des responsables publics paraît s'imposer dans l'avenir comme le mode de publicité privilégié pour satisfaire les objectifs de transparence, en particulier le rétablissement de la confiance de la population dans ses dirigeants. Le droit au respect de la vie privée des gouvernants se trouve désormais confronté à la montée en puissance d'un droit de savoir et d'un pouvoir d'influence des gouvernés qu'ils veulent exercer pleinement[91]. Plus de deux siècles après son inscription à l'article 15 de la Déclaration des droits de l'homme et du citoyen, le droit de la société « *de demander compte à tout agent public de son administration* » semble enfin prendre vie.

89 - Art. 135-2, § I, du code électoral.

90 - Le rapport d'évaluation de la France par le Groupe d'États contre la corruption du Conseil de l'Europe (GRECO) sur le thème « Prévention de la corruption des parlementaires, juges et procureurs », adopté en mars 2016, est accessible à l'adresse : https://rm.coe.int/16806c5dfc.

91 - B. Nabli, Fondements de la « moralisation-juridicisation » de la vie politique, Pouvoirs, n° 154, 2015, p. 151-161, p. 160.

TABLE DES MATIÈRES

Liste des contributions 3

Introduction : le modèle européen de protection des données personnelles à l'heure de la gloire et des périls
par Emmanuel Netter 5
§ 1 : Le droit européen des données menacé en dedans 13
A. Le manque de lisibilité 14
B. Le manque d'effectivité 18
1) Du point de vue des personnes concernées 19
2 – Du point de vue des responsables de traitement et sous-traitants 23
§ 2 : Le droit européen des données menacé au-dehors 24
A. Le difficile dialogue des modèles : le transfert des données hors de l'Union 25
B. L'affrontement des modèles : un choc des souverainetés 28

PREMIERE PARTIE : APPROCHE TRANSVERSALE

La protection des données personnelles et la mort
par Céline Béguin-Faynel 35
Section I – Les mesures ante mortem organisées par la personne 44
§ 1 : Proroger les droits des personnes sur leurs données *après la mort* 44
A. Mesures préexistantes relatives aux données de santé *post-mortem* 45
1) Limitation du traitement à fins de recherche des données de santé *post-mortem* 45
2) Limitation des expertises génétiques *post-mortem* 47
B.Mesures conventionnelles de protection des données personnelles *post-mortem* 52
1) Coexistence entre directives générales et particulières 52
2) Nature contractuelle des directives du défunt 56
C. Rénovation de l'analyse du droit sur les données après la mort 58
1) Réaffirmation du droit d'opposition et du droit à l'information 58

2) Consécration de l'analyse personnaliste et relativisation de l'analyse patrimoniale 60
§ 2 : Administrer les données et l'identité numérique après la mort 64
A. Diversité des pratiques numériques face à la mort..... 64
B. Difficulté à préparer sa mort numérique 67
C. Flexibilité des outils d'organisation numérique de sa mort 70
Section II - Section II - Les mesures post mortem ouvertes aux héritiers 73
§ 1 : Articulation éprouvée entre droits du mort et des vivants ...74
A. Respect dû au mort et vie privée des héritiers..... 75
B. Actions en réparation intentées par les héritiers..... 78
1) Préservation des intérêts patrimoniaux des héritiers.... 78
2) Levée du secret médical du mort dans l'intérêt des héritiers..... 82
C. Accès aux origines tenues secrètes après le décès des père et mèrede naissance..... 84
§2 : Articulation rénovée des droits du mort et des vivants sur les données..... 87
A. Les missions définies par la loi : protection et accès aux données *a minima*..... 88
1) Promouvoir la prise en compte du décès par le responsable de traitement 89
2) Favoriser l'organisation et le règlement de la succession pour les héritiers 90
a) Accès préexistant des héritiers aux données concernant les avoirs financiers du défunt 91
b) Nouvelles mesures habilitant les héritiers du défunt..... 93
c) Recevoir communication des biens numériques et données apparentées aux souvenirs de famille 98
3) Régler les conflits entre héritiers devant le tribunal de grande instance 104
B. Les directives du défunt : préservation de l'identité numérique du défunt *a maxima*..... 106
1) Administration des comptes du mort sur les réseaux sociaux numériques..... 107
2) Exploitation de l'image du mort..... 109
3) Résurrection numérique du mort par un avatar ou un hologramme..... 111

Le règlement 2016/679/eu à la lumière du droit américain : à la recherche d'un fonds commun entre l'union européenne et les états-unis
par Céline Castets-Renard 117
§ 1 : À la recherche d'un fonds commun dans le choix des instruments normatifs 125
§ 2 : À la recherche d'un fonds commun dans le choix des règles applicables 131
§ 3 : À la recherche d'un fonds commun au travers des parties prenantes 134

Tous responsables de traitement de données personnelles ?
par Mélanie Clément-Fontaine 139
§ 1 : Des critères accueillants 141
§ 2 : L'exclusion des activités strictement personnelles ou domestiques 148

Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence
par Jean-Marc Deltorn 153
Section I – Le traitement algorithmique des données personnelles : un nouvel enjeu juridique 155
§ 1 : Apprendre des données : les algorithmes prédictifs et les données personnelles 155
A. L'émergence d'un nouvel objet technique 155
B. Les algorithmes d'apprentissage face aux droits fondamentaux .. 159
§ 2 : Les recours juridiques en réponse au traitement algorithmique des données personnelles 164
A. Un accès (limité) à la logique des algorithmes 164
B. Les conditions d'application du droit d'accès à la logique des algorithmes 169
Section II – Le principe de transparence à l'épreuve des modèles prédictifs 172
§ 1 : L'opacité des modèles prédictifs : interpréter l'ininterprétable ? 172
A. La « logique sous-jacente » aux procédés algorithmiques, une notion en construction 172
B. Un accès à la logique en bute face aux modèles prédictifs 177
§ 2 : Le secret des modèles prédictifs, source d'opacité 183

A. Les modèles prédictifs et le recours au secret 183
B. Entre secret des affaires et droit d'accès aux modèles, quelle articulation ? 188
Section III – Au delà du principe de transparence, vers un principe de responsabilité 194
§1 : Face à la volatilité des développements techniques, le recours au droit souple 194
§2 : Quelques considérations pratiques de mise en oeuvre du principe de responsabilité algorithmique 201
Conclusion et perspectives 204

Le règlement général sur la protection des données à caractère personnel appliqué aux états tiers : une appréciation de son caractère extraterritorial
par Élodie Weil 207
§1 : La licéité de l'extraterritorialité 214
A. L'extraterritorialité de la réglementation européenne fondée sur une conception extensive du rattachement territorial 216
1. L'inadéquation partielle de la conception territoriale objective . comme fondement à la réglementation européenne 217
2. L'affinement de la conception objective du rattachement territorial : la technique du *targeting* 222
B. L'absence de contestation du caractère extraterritorial de la réglementation 225
§2 : L'efficacité de la réglementation extraterritoriale 228
A. L'obstacle du conflit de valeurs 229
B. De l'effet de persuasion à l'exportation du modèle européen en matière de protection des données 235

DEUXIEME PARTIE : APPROCHE SECTORIELLE

La gouvernance des données personnelles dans la banque
par Aurélie Banck 243
§1 : Le Délégué à la protection des données 245
§2 : L'adhésion au mécanisme du one *stop shop* 249
§3 : La répartition des responsabilités au sein des groupes 253
Conclusion 257

La protection des données personnelles en assurance : dialogue du juriste avec l'actuaire
par Arthur Charpentier, Delphine Cocteau-Senn et Rodolphe Bigot 259
Introduction : Les données, instruments de mesure du risque .. 259
A. De la donnée à la donnée « à caractère personnel » 259
B. De la donnée personnelle à la « donnée sensible » 263
§ 1 : La collecte des données personnelles de l'assuré 265
A. Données recueillies via la proposition d'assurance 266
1) Des données pertinentes au regard du risque à évaluer 266
2) Des données « juridiquement disponibles » 270
3) Des données dont la pertinence est sujette à évolution 273
B. Le cas des données recueillies via des objets connectés 274
1) La question du consentement de l'assuré 275
a) Une pratique supposant le consentement de l'assuré 275
b) L'hypothèse d'une collecte imposée 277
2) La question du moment de la collecte 279
§ 2 : L'exploitation des données de l'assuré par l'assureur 279
A. Décision de prise en charge et tarification du risque 279
1) Discrimination prohibée ou limitée 280
a) Discrimination tarifaire prohibée 280
b) Discrimination limitée 281
2) L'automatisation des processus décisionnels (profilage) .. 283
a) La question du droit à une intervention humaine 284
b) La question du droit à l'information sur la logique du profilage 286
B. La lutte contre la fraude 288
1) La question du profilage des fraudeurs 288
2) Lutte contre la fraude et loyauté de la preuve 291
C. Statistiques et recherche actuarielles 293
1) Le fondement du traitement ultérieur des données d'assurés 294
2) L'existence de garanties appropriées, dont la pseudonymisation 296
3) Le droit à l'effacement 298

Recherche en santé et protection des données personnelles à l'heure du RGPD
par Frédérique Lesaulnier 303

§1 : Le RGPD et la place que les activités de recherche scientifique y occupent 305
A. Vers une responsabilisation accrue des acteurs 305
B. Une évolution plus qu'une révolution dans la régulation .. 306
C. Place des activités de recherche dans le RGPD 309
1) Une dérogation au principe d'interdiction de traiter des catégories particulières de données 309
2) Une présomption de compatibilité de la finalité de recherche scientifique avec une finalité initiale différente et possibilité de conservation à ces fins au-delà de la réalisation de la finalité du traitement 309
3) Des modalités d'exercice des droits adaptées 310
4) La promotion de codes de conduites sectoriels élaborés en lienavec les communautés scientifiques concernées 313
A. Le maintien d'un régime d'autorisation pour les traitements réalisés à des fins de recherche, d'étude oud'évaluation dans .... le domaine de la santé 314
B. Le champ d'application territorial de la loi française 315

Données personnelles et transparence de la vie publique par Charles-Édouard Sénac 317
§1 : Les personnes assujetties à l'exigence de transparence 322
A. Les fonctions ciblées 322
B. Les entourages touchés 328
§2 : Les données personnelles visées par l'exigence de transparence 329
A. Les données contenues dans la déclaration de situation patrimoniale 330
B. Les données présentes dans la déclaration d'intérêts 331
§3 : Les destinataires des données personnelles 334
A. La transparence sans publicité 335
B. La transparence avec publicité 338

Table des matières 343