L'émergence d'un droit sur l'identité numérique

Bettina Bordure

▶ **To cite this version:**

Bettina Bordure. L'émergence d'un droit sur l'identité numérique. Sciences de l'Homme et Société. 2020. dumas-02559566

HAL Id: dumas-02559566

https://dumas.ccsd.cnrs.fr/dumas-02559566v1

Submitted on 30 Apr 2020

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.

Institut de Recherche et d'Études en Droit de l'Information et de la Communication

Master 2 Droit des Médias et des Télécommunications

Année universitaire 2017 – 2018

L'émergence d'un droit sur l'identité numérique

Mémoire présenté par Bettina BORDURE

Sous la direction de Monsieur Philippe MOURON, Maître de conférences à la Faculté de Droit et de Science Politique d'Aix-Marseille Université

Institut de Recherche et d'Études en Droit de l'Information et de la Communication

Master 2 Droit des Médias et des Télécommunications

Année universitaire 2017 – 2018

L'émergence d'un droit sur l'identité numérique

Mémoire présenté par Bettina BORDURE

Sous la direction de Monsieur Philippe MOURON, Maître de conférences à la Faculté de Droit et de Science Politique d'Aix-Marseille Université

A B R É V I A T I O N S

Actu. : Actualisation

AFP : Agence France Presse

ANSES : Agence nationale de sécurité sanitaire

APC : Chambre syndicale des producteurs et exportateurs de films français

BDEI : Bulletin du Droit de l'Environnement Industriel

CA : Cour d'Appel

CC : Conseil Constitutionnel

C. Cass : Cour de Cassation

CE : Conseil d'État

CEDH : Cour Européenne des Droits de l'Homme

CJUE : Cour de Justice de l'Union Européenne

CGU : Conditions générales d'utilisation

CMB : Compagnie des machines Bull

CNIL : Commission nationale pour l'informatique et les libertés

Com. : Commentaire

CRISTINA : Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux

DARPA : Defense Advanced Research Projects Agency

Éd. : Éditions

EDVIGE : Exploitation documentaire et valorisation de l'information générale

FBI : Federal Bureau of Investigation

FNDF : Fédération nationale des distributeurs de films

GAFA. : Google, Apple, Facebook, Amazon

GPS : Global Positioning System

IBM : International Business Machines

IP : Internet Protocol

PI : Revue Propriétés intellectuelles

IP/IT : Revue Dalloz Droit de la propriété intellectuelle et du numérique

JCP G : La Semaine Juridique

M.à.j : Mise à jour

MAUSS : Mouvement anti-utilitariste en sciences sociales

MIT : Massachussetts Institute of Technology

N. : Numéro

N. D. Cal : United States District Court for the Northern District of California

NOYD : None of your business

NSA : National Security Agency

OCDE : Organisation de cooperation et de développement économique

ONU : Organisation des Nations Unies

P. : Page

PUF : Presses universitaires de France

PUAM : Presses universitaires d'Aix-Marseilles

QR : Quick Response

Rép. civ. : Répertoire de Droit civil

RFDA : Revue française de droit administratif

RGPD : Règlement européen général à la protection des données

RLDI : Revue Lamy Droit de l'Immatériel

Rub. : Rubrique

SAFARI : Système automatisé pour les fichiers administratifs et le répertoire des individus

Sec. : Section

SEVN : Syndicat de l'édition vidéo

SFR : Société française du radiotéléphone

SNCF : Société nationale des chemins de fer

SPI : Syndicat des producteurs indépendants

T. : Tome

TA : Tribunal administratif

text. : textuellement

UE : Union Européenne

UFC Que Choisir : Union Fédérale des Consommateurs Que Choisir

UNICEF : United Nations Children's Fund (Fonds des Nations unies pour l'enfance)

UPF : Union des producteurs de film

URL : Uniform Resource Locator

Vol. : Volume

S O M M A I R E

INTRODUCTION

Quis custodiet ipsos custodes ?[1]

Pendant de nombreux millénaires, l'espace géographique voyait sa délimitation opérée au regard des éléments physiques du paysage. Traditionnellement apparaissent donc trois strates : l'espace terrestre, l'espace aérien et l'espace maritime. Sur chacune d'entre elles, l'État détient des droits, lui permettant ainsi d'exercer ses prérogatives régaliennes. Cette souveraineté s'explique par le bornage de frontières, acceptées par lui-même et par ses voisins. La défense de ce territoire n'ayant rien de compliqué, chaque conflit territorial se réglait par la force armée. Ces espaces étant matérialisés, aucune difficulté juridique ne semblait apparaître.

Ce ne fut plus le cas avec l'arrivée de l'nternet. Dans les années 1960, l'idée ambitieuse de ce procédé de communication, développé par l'ARPA, une agence américaine pour l'équipement de l'armée, avait pour but de relier entre eux différents ordinateurs afin qu'ils ne soient plus de simples calculateurs, mais de véritables nœuds du réseau. En 1971, quinze postes avaient établi une première liaison.

Le développement de l'ARPANET, tel qu'il fut baptisé initialement, s'accompagnait de la découverte du protocole TC/IP, par Vint Cerf et Robert Kahn, permettant de transmettre des informations utiles au fonctionnement correct des services. Ainsi était née l'idée d'une inter-connectivité entre les machines, qui prévenait en réalité d'une mondialisation de l'internet.[2] Enfin, de la naissance de ces nouveaux outils émergeait le Web, un espace regorgeant de contenus et totalement dématérialisé, sur lequel toute appartenance restait à établir — bien qu'il apparaisse aujourd'hui qu'il soit encore plus fastidieux de la conserver.

Quelle souveraineté envisager pour un espace dont aucune délimitation géographique n'existe, et sur lequel chaque État projette une conception différente, dépendante de sa vision du régime politique et de la conception aléatoire de certains droits fondamentaux ?

La souveraineté étatique est une légitimité de droit instaurée par les hommes dès lors qu'ils ont été désireux de se regrouper en communautés, dirigées par des instances politiques. Elle trouve ses fondements dans une velléité d'organisation de la société en un système fluide et contrôlé, dans lequel les citoyens s'en remettent à leurs dirigeants pour leur protection. Il en va totalement différemment pour le réseau internet, qui est une création technique purement artificielle, dont seules les conséquences sont visibles, et qui ne fonctionne que parce que les individus ont décidé de l'utiliser.

---

[1] Litt. « Qui garde nos gardiens ? ».

[2] CERUZZI (E.), « Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté », *Le temps des médias*, 2012/1, n°18, pp. 15-28.

La puissance de ce réseau a conduit les États à accepter cette forme de souveraineté technique sur laquelle ils n'avaient initialement que très peu de prises. Certains auteurs vont même jusqu'à considérer que le réseau a une force normative, tant il génère automatiquement des codes de conduite, des valeurs et des principes, et des éthiques que les utilisateurs respectent.[3] Bien qu'il n'en ait pas les contours traditionnels, le réseau pourrait même être comparé à un État au regard des éléments matériels de constitution politique : composé d'une population d'utilisateurs plutôt dévoués, son territoire serait certes immatériel mais bien existant. Quant à sa souveraineté, nul n'est besoin d'argument pour prouver qu'il existe une gouvernance du numérique sur les individus.

En outre, la capacité normative du réseau entraîne des heurts entre les réglementations des États, devenues concurrentielles, chacun ayant sa propre ligne de conduite pour encadrer ce nouvel espace — l'exemple le plus marquant en est la dichotomie entre les États-Unis et les pays de l'Union Européenne, respectivement partisans d'une liberté capitaliste ou d'un encadrement individualiste. L'idée d'une règlementation harmonisée mondialement n'ayant pas été envisagée pour le moment, les conflits de territorialité du droit restent réglés casuistiquement, n'arrangeant rien à la complexité de la situation.

Ce nouvel espace qu'est le numérique, avec ses possibilités infinies, est un eldorado regorgeant de multiples pistes de réflexions en droit. L'efficacité et les progrès qu'il permet réfrènent les envies gouvernementales de contrôle, mais force est de constater que les États perdent progressivement leur pouvoir sur leurs propres infrastructures, sur leur économie, sur les droits fondamentaux dont ils sont garants, et à terme, sur leur population.

Face à ces constatations poignantes, il était impensable pour les États de tous horizons de laisser une telle révolution prendre une si grande ampleur et écraser leurs prérogatives de droit — ainsi s'est engagée une véritable croisade de récupération de ce qui tend à devenir une souveraineté numérique. « La souveraineté numérique est justement cette volonté de maîtriser ce nouveau destin, afin qu'il réponde des lois de la République et que cette mutation renforce tout autant nos libertés, nos choix que notre prospérité ».[4]

Tout en tâtonnant dans la réglementation de cet océan numérique, les États se confrontent en outre à une nouvelle évolution sociale, née de l'utilisation de ce réseau : la relation anthropologique entre l'homme et la machine, désormais si proches l'un de l'autre qu'ils en révèlent une nouvelle conception de l'Humain.

« L'humanité est engagée dans une transition vers une nouvelle anthropologie, qu'il est difficile de métaboliser. Comme si l'humanité, qui vivait jusqu'alors protégée par les lois de la nature, avait découvert des espaces dans lesquels le degré de liberté, soudainement atteint, s'avérait immaîtrisable. […] Si les lois de la nature s'effondrent, le vide qu'elles laissent devra être rempli par des lois humaines qui reconstituent artificiellement, principalement via des

[3] ROJINSKY (C.), « Cyberespace et nouvelles régulations technologiques », *D.*, 2001, pp. 844-847.

[4] BELLANGER (P.), « Les données personnelles : une question de souveraineté », *Le Débat*, 2015/1, n°183, pp. 14-25.

interdictions, les contraintes naturelles que la science a fait disparaître. La société attend de la loi d'abord du réconfort, ensuite de la protection. » [5]

Happés par l'attrait commercial des nouvelles technologies, les hommes ont sombré dans un extrême technique que rien ne semble plus arrêter. Ils n'ont en réalité que succombé aux promesses des GAFA — Google, Amazon, Facebook, Apple — et autres entreprises du numérique, qui leur ont fait miroiter des biens et des services exceptionnels, désormais ancrés dans les habitudes de vie quotidienne.

L'Union internationale des télécommunications estimait, en 2016, que 3,385 milliards d'individus dans le monde étaient connectés au réseau internet, connexion qui passe par l'utilisation de ces biens et de ces services, qui ont su ainsi se servir de la popularité du numérique pour se rendre indispensables. Or ce développement massif ne s'est pas effectué sans heurts : de nouveaux phénomènes, tels que la cyberdépendance, le harcèlement en ligne, ou l'usurpation d'identité, voient le jour, inquiétant les spécialistes des sciences de la communication.[6]

Ces nouvelles problématiques ne sont qu'accessoires, en revanche, face au mal du siècle digital qu'ont fait jaillir la mise en réseau et le numérique : la projection de l'identité.

« Notre présent transite de plus en plus par le réseau qui, sans cesse, oriente nos décisions. Notre futur dépend du réseau car les informations collectées sur nous, aujourd'hui, déterminent les choix qui nous seront proposés demain ».[7]

Il était prévisible qu'à force d'intégrer le numérique dans nos habitudes, celui-ci finirait par avoir d'importantes influences anthropologiques. Ainsi, la notion entière d'identité, au prisme du digital, évolue de manière radicale vers quelque chose de totalement inexploré.

Il est deux facettes à la notion d'identité, toutes deux impactées par ce que l'on pourrait qualifier à juste titre de révolution numérique : la fonction d'identification, technique et juridique, et la fonction de détermination de l'individu, plus sociale mais dont les conséquences intéressent également le droit.

S'agissant de l'identification, traditionnellement effectuée par des documents ou des structures gouvernementales authentifiantes, celle-ci voyait ses composantes et ses caractères muter au fur et à mesure de l'écoulement du temps.

De la simple description physique d'un individu s'est effectuée une transition vers une identification complète, aux moyens d'éléments physiques, mais également moraux, sociétaux, idéologiques, et même parfois, comme le montre la captation d'images, visuels. Le

---

[5] RODOTA (S.), « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements,* 2010, n°62, pp. 55-70.

[6] JUNEAU (S.), « La cyberdépendance : un phénomène en construction », *Déviance et Société*, 2014/3, vol n°38, p. 285.

[7] BELLANGER (P.), « Les données personnelles : une question de souveraineté », *Le Débat*, 2015/1, n°183, pp. 14-25.

développement progressif des techniques, qu'il s'agisse de l'écriture, de la reprographie, de la photographie, ou de l'informatique, ont systématiquement permis le perfectionnement de l'identification — plus rapide, plus sécurisée, plus fiable.

La numérisation de ces procédés a entraîné des développements considérables. La reconnaissance faciale, réalisée par de nombreux smartphones aujourd'hui, permet de déverrouiller le support sans même le toucher. L'apposition d'une empreinte sur une touche particulière permet d'authentifier l'individu. Bien plus difficile à usurper, l'identification s'est vue révolutionnée par les techniques digitales, entraînant une multitude de problématiques juridiques non résolues.

S'agissant en revanche de la détermination individuelle, le numérique a engendré des conséquences juridiques, mais en premier lieu sociales. Par le biais des réseaux sociaux et des applications numériques en tout genre, l'homme a pu transposer son identité traditionnelle dans son nouvel océan, en l'enjolivant parfois de caractéristiques supplémentaires, ou en y ajoutant des objets traditionnellement pas pris en compte par les autorités. L'état civil ne fait nullement état des idéologies politiques, des orientations amoureuses ou des couleurs favorites d'un individu — ce qui est désormais possible sur internet.

Le dévoilement de soi est devenue une pratique courante, encouragée par une liberté d'expression quasi-totale en ligne, se manifestant dans la création de blogs personnels, de profils en tout genre sur divers réseaux, du partage de photos intimes, et de la connexion presque permanente aux messageries. Ces possibilités ont permis aux individus de se façonner une identité correspondant peut-être davantage à leur réalité que n'en témoignait l'identité traditionnelle — et quelque part, de se distinguer encore plus du reste du monde. Ce besoin d'externalisation de la personne est satisfait par l'obtention « d'identités narratives » : des identités validées par la communauté numérique, qui renforcent la confiance des individus en eux. Ces comportements sont spécifiques à la vie digitale, tant ils sont inexistants du monde réel.[8]

Mais pour les entreprises du numérique, l'ensemble de ces informations identitaires ne sont pas des objets d'étude comportementale. Elles tendent plutôt à devenir des valeurs commerciales, ramenant ainsi les éléments de l'identité à une simple marchandise, sans aucune distinction les unes entre les autres, et plaçant ainsi les individus sur le même pied d'égalité. Ce paradoxe était déjà souligné en 1977, par Jean Foyer, lors des débats parlementaires sur l'élaboration de la loi pilier de la protection des données : « Tout à la fois, l'informatique dépersonnalise trop et personnalise trop ».

Une partie conséquente de la doctrine critique allègrement cette tendance à la numérisation excessive de l'identité. Une fois numérisée, elle ne définit plus nécessairement une personne par ses simples caractères. Il s'agit plus d'un ensemble de traces numériques, certes rattachés à la personnalité, mais également à son activité — historiques de recherches, préférences commerciales — et dont la visée est plutôt capitaliste. La persistance des données

[8] DENOUËL (J.), et GRANJON (F,) « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie*, vol. 1, n°1, 2010, pp. 25-43.

n’a pas un but scientifique ou historique, elle aide simplement à faire persister le profit économique des entreprises.

« L’homme est devenu un document comme les autres, disposant d’une identité dont il n’est plus "propriétaire", dont il ne contrôle que peu la visibilité, et dont il sous-estime la finalité marchande ». [9]

Voilà le véritable enjeu que dissimule l’apparition d’une identité numérique : l’exploitation des éléments de celle-ci par les acteurs privés. Portant régulièrement atteinte aux droits des personnes, cette pratique est désormais monnaie courante pour tous les géants du numérique, tant elle est rémunératrice. La réalité du terrain est bien moins glorieuse qu’une simple question de souveraineté : l’accès à des services ludiques et bien souvent gratuits dissimule en réalité la commercialisation des éléments de l’identité numérique, et par-là même, des potentialités de litiges multipliées.

Ces agrégats de l’identité sont matérialisés par ce que les textes nomment les données personnelles. Éléments numériques regorgeant d’informations, ces flux sont considérés comme tels dès lors qu’ils permettent une identification directe ou indirecte de la personne.[10]

L’homme s’est laissé doucement bercer par le chant des sirènes digitales, enlacé par la douceur de vie engendrée par les applications mobiles et les réseaux sociaux, et, non content d’y avoir consenti par la délivrance de ses données personnelles, il exige désormais que son État lui garantisse une protection efficace, à laquelle il assène perpétuellement des blessures. À trop se créer des éléments d’identité, voir à les multiplier par l’institution d’avatars ou de pseudonymes, l’individu se perd, et ne sait plus qui il est réellement.[11]

Pourtant, la protection législative n’a pas connu de retard. Dès 1978, l’État français s’est doté d’une loi, d’ailleurs visionnaire en la matière, afin de conserver l’informatique au rang de service à la personne, et non de nouveau diktat. S’attachant essentiellement à la protection des données des individus, dans tout type de fichiers existants, la loi venait poser un cadre plutôt complet quant à l’exploitation des informations individuelles. La directive européenne ne viendra que presque vingt ans plus tard, en 1995, s’inspirant assez largement du cadre posé par la loi française — à tel point que celle-ci n’aura besoin d’être transposée qu’en 2004.

Cette préoccupation n’a pas reculée, puisque la directive sera remplacée par un règlement européen général à la protection des données, communément appelé RGPD, dont la date d’entrée en vigueur est fixée au 25 mai 2018 — et ce afin d’harmoniser le niveau de protection sur l’ensemble du territoire de l’Union.

L’aspect majeur de l’identité numérique est bien représenté dans les données personnelles, et en cela, la volonté constante des États de les protéger est non seulement louable, mais nécessaire. Pour autant, il n’est pas que cette facette de la notion qui importe aujourd’hui,

---

[9] ERTZSCHEID (O.), « L'homme, un document comme les autres », *Hermès, La Revue* 2009/1, n° 53, pp. 33-40.

[10] Art. 2, loi n°78-16 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés.

[11] DENOUËL (J.), et GRANJON (F,) « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie*, vol. 1, n°1, 2010, pp. 25-43.

tant elle est large et tant ses aspects sont mobilisés par le numérique. Il faut finalement prendre du recul pour s'apercevoir que l'identité numérique appelle à d'autres protections.

Les atteintes que portent, entre autres, les GAFA, à l'identité numérique, ne sont pas que de l'ordre de l'exploitation abusive des données personnelles. La surveillance permanente par le biais de la géolocalisation, notamment, peut tout à fait être considérée comme une atteinte au respect de la vie privée. L'identité est intrinsèquement liée à la personne et toute injure qui lui serait portée serait un préjudice. Il semble donc qu'une relation naissante entre l'identité numérique et les droits de la personnalité émerge.

L'Allemagne porte un regard plus contemporain que la France sur ces problématiques. Reconnaissant déjà un droit à l'autodétermination informationnelle aux individus — une liberté de décision quant à la délivrance ou non de certaines données —, elle avait déjà apporté une pierre à l'édifice en 2008, lorsque la Cour constitutionnelle censurait un amendement à la loi sur les renseignements intérieurs. Cet amendement visait à légitimer la surveillance numérique dissimulée. La Cour déclarait la loi non conforme à la loi fondamentale allemande, et consacrait un « droit fondamental à la confidentialité et à l'intégrité des systèmes techniques et des systèmes d'information », en tant qu'un élément des droits de la personne.

« Un continuum est ainsi établi entre la personne et la machine. En le reconnaissant, la loi crée une nouvelle anthropologie, qui impacte les classifications légales et change leur nature ».[12]

Dès lors, un débat de plus large ampleur s'instaurait entre la nécessité d'adapter les droits et les libertés fondamentaux existants, ou de créer un nouveau cadre spécifique à la protection de l'identité numérique. Lorsque les droits créés par le digital sont évoqués, cela peut laisser à penser que le contexte juridique va évoluer pour s'y adapter — mais les droits fondamentaux ne sont pas un cadre instable à vocation de mutation : ils ne peuvent que s'adapter aux évolutions technologiques.

En revanche, de nouvelles prérogatives découvertes, par un spectre de nouvelles possibilités, peuvent être adaptées au droit en vigueur et y être associées. Ces modifications impliquent parfois de redéfinir la personne ou certains de ses aspects, et de poser de nouvelles limites.[13]

Il n'existe pour l'instant aucun droit sur l'identité numérique, ce concept ayant simplement émergé des questionnements gravitant autour de celui-ci. La délimitation même de la notion entraîne déjà des tergiversations au sein des doctrines, quant à la qualification des données personnelles qui la composent.

S'interroger sur la nécessité impérieuse de fonder un droit général français et européen sur l'identité numérique, englobant une définition précise de cette notion et lui intégrant des

---

[12] RODOTA (S.), « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements,* 2010, n°62, pp. 55-70.

[13] RODOTA (S.), *ibid*.

prérogatives de droit pour les individus, est une question primordiale à l'aune d'une société si digitalisée qu'elle en impacte les droits et les libertés les plus fondamentaux.

La pratique démontre que, même en l'absence de consécration textuelle, divers éléments tendent à faire émerger un tel droit. Les vifs débats sur la nature de la donnée personnelle sont la preuve que l'identité numérique interroge quotidiennement les juristes. Les plus anciennes dichotomies du droit sont affectées par la numérisation de la société — la donnée suscite un profond intérêt en ce qu'elle n'est qualifiée ni de bien ni de prérogative personnelle.

Ce débat témoigne d'une difficulté d'adéquation entre la loi et la réalité. Le régime traditionnel de la propriété est incompatible avec la donnée personnelle. Pourtant, dans la pratique, elle est déjà considérée comme une marchandise par les entreprises du numérique, qui l'exploitent allègrement et en dégagent des bénéfices colossaux. Cette théorie soulève donc un engouement pour les fervents partisans des consommateurs, qui souhaiteraient voir ce déséquilibre réajusté en faveur des individus — mais permet également aux opposants de la théorie classique de la propriété d'appuyer leur thèse selon laquelle ce régime est obsolète.

À l'inverse, l'absence de reconnaissance textuelle de droits de la personnalité sur l'identité est paradoxale, tant dans la pratique il existe des moyens de prouver des atteintes à celles-ci, sur des fondements juridiques liés aux individus. Il en va ainsi pour toutes les diffamations et les injures en ligne, intrinsèquement liées à la réputation numérique, sanctionnées par la loi du 29 juillet 1881 sur la liberté de la presse. Il en est de même pour les diffusions illicites de contenus visuels en ligne, sans autorisation, qui sont prohibées par le Code pénal.

Il existe un « halo informationnel » autour de la personne, qui pose des problèmes vis-à-vis des droits de la personnalité. Le droit constitutionnel ne reconnaît pas encore de droit autonome à la protection de celles-ci, mais rattache cette prérogative à la protection de la vie privée. [14]

« Internet a valeur de service public. Des personnes, des communautés, des institutions publiques et des organismes privés s'appuient sur internet pour mener leurs activités et sont en droit d'attendre des services en ligne qu'ils soient accessibles, fournis sans discrimination, abordables, sécurisés, fiables et continus. En outre, la jouissance des droits de l'Homme et des libertés fondamentales des utilisateurs d'internet ne doit être soumise à aucune restriction illégale, inutile ou disproportionnée ».[15]

Il serait donc vain de renier le lien indéfectible qui unit l'identité et les droits de la personnalité, bien que pour le moment, les dispositions permettant de les protéger soient éparses. Le bien-fondé d'un droit sur l'identité numérique trouve sa source dans le paradoxe d'inadéquation du droit et de la réalité — et d'un besoin primordial de définition des concepts

[14] GEFFRAY (E.), « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », *Les nouveaux Cahiers du Conseil Constitutionnel*, 1er juin 2016, n°52, p. 7.

[15] TURGIS (S.), « Le "Guide des droits de l'homme pour les utilisateurs d'Internet" du Comité des ministres du Conseil de l'Europe : Vademecum du droit européen de l'internet », *LPA*, 29 août 2014, n°173, p. 7.

et d'harmonisation de leur protection, tant au niveau des droits fondamentaux qu'au niveau des droits personnels (**Partie 1**).

De plus, là n'est pas le seul intérêt d'un éventuel droit sur l'identité numérique. Au niveau législatif, il reflèterait de nouvelles interrogations sur l'étanchéité du droit à de nouvelles sources normatives. Traditionnellement effectuée de manière verticale, la législation générée par un groupe d'individus spécialisés en la matière tend à se répandre sur l'ensemble de la population, et tout ceci de manière légitime par la validation citoyenne des institutions juridiques.

Le numérique bouleverse cet ordre institué. Le réseau est un ordre virtuel légitimé par les individus, qui n'a pourtant pas été créé par les institutions étatiques. Il est un « objet sur lequel toutes les personnes, dont les données sont maillées, disposent de droits, mais qui ne peut être matériellement divisé entre eux. […]. C'est donc une forme d'indivision qui concerne toute la population ».[16] Les citoyens attendent un certain niveau de protection par leurs gouvernants, mais ils en sont également une partie active. Le réseau n'est pas un domaine sur lequel les individus n'ont pas d'incidence.

Les libertés fondamentales sont protégées en fonction de l'image qu'a l'État de celles-ci, mais rien n'empêche les individus d'invalider sa vision. Cette affirmation explique parfaitement le principe d'autodétermination. Les individus cherchent désormais à éviter l'omniprésence des technologies et à protéger leurs identités — parfois sans l'aide étatique.[17]

Après l'ivresse du numérique, le repos s'est fait désirer, et une conscientisation des individus a émergé. De mieux en mieux informées sur l'utilisation de leurs identités, les populations ont commencé à se mobiliser dans la démocratie digitale, ce qui n'a pas été mis de côté par les gouvernements — en témoigne, en France, la consultation citoyenne effectuée en vue de la loi pour une République numérique.

« L'accompagnement de l'innovation implique en effet de passer d'une logique de réglementation à une logique de régulation, c'est-à-dire à un type d'encadrement et d'accompagnement qui combine la fidélité à des principes fondamentaux et à une règle de droit claire, et des nouveaux modes d'intervention du régulateur, fondés sur le droit souple. »[18]

Une forme de régulation citoyenne a donc émergé afin de protéger directement les identités de tous. Il est indéniable qu'elle est plus efficace dans certains domaines, car elle ne vient pas des États ou d'acteurs extérieurs, mais d'individus qui manient les technologies quotidiennement. Qwant, moteur de recherche français, ambitionne de détrôner Google en

---

[16] BELLANGER (P.), « Les données personnelles : une question de souveraineté », *Le Débat*, 2015/1, n°183, pp. 14-25.

[17] RODOTA (S.), « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements,* 2010, n°62, pp. 55-70.

[18] GEFFRAY (E.), « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », *Les nouveaux Cahiers du Conseil Constitutionnel*, 1er juin 2016, n°52, p. 7.

proposant à ses utilisateurs de ne pas conserver leurs historiques de recherche ou leurs préférences de consommation. Newmanity, messagerie collaborative, permet d'échanger des contenus sans que les données personnelles ne soient collectées. L'association Noyb, créée par Maximilian Schrems, permet aux individus de faire appel à une aide juridique en cas de litige en la matière.

Bien que cela semble remettre en question les équilibres constants du droit, force est d'admettre que le numérique a bouleversé les relations existantes entre les États et les entreprises, entre les entreprises et les individus, et entre les individus et leurs États. Se borner à ne vouloir légiférer sur l'identité numérique et les données personnelles sans prendre en compte les éléments extérieurs serait vain — la législation qui en ressortirait ne serait que partiellement efficace.

Au-delà de l'intérêt juridique de la consécration d'un droit sur l'identité numérique, demeure un intérêt social. La conception du soi ne doit pas être trop bouleversée par les évolutions techniques, tant elle en est déjà atteinte. La mort numérique en est une des conséquences les plus poignantes, tant elle dérange. Ce concept émergent est né de la multiplication des profils de réseaux sociaux laissés inactifs après le décès de leurs propriétaires, parfois dérangeants pour les proches, et qui pose des problèmes de droits sur la délivrance des comptes aux héritiers, mais également des complications parfois psychologiques, tant la rémanence virtuelle d'une personne disparue peut choquer. (**Partie 2**).

Les limites de l'identité numérique sont sans cesse repoussées. L'individu pourrait devenir permanent, là où normalement, ses caractères et son identité s'évanouissent avec lui à sa mort. Il est déjà des projets, certes légèrement fictifs, de fixation de la mémoire dans un support artificiel — mais à l'heure où la technologie est sans cesse plus inventive, estimer une création comme impossible serait une erreur. En outre, il existe déjà des logiciels d'intelligence artificielle permettant le dialogue avec des personnes disparues, sur base de discussions virtuelles préenregistrées auparavant.[19] Tout cela, qui plus est, sans compter les questions relatives à la bioéthique et aux humains améliorés, qui interrogent tant l'éthique médicale que le droit à la santé.

Il paraît donc étonnant que les législateurs français et européens ne se soient pas saisis de l'importance d'une telle notion, tant ses implications juridiques sont variées. À l'heure où un robot acquiert la citoyenneté d'Arabie Saoudite, l'encadrement de l'identité traditionnelle, de l'identité numérique, et de l'identité robotique, permettrait de clarifier la situation actuelle et d'évoluer sereinement vers un futur technologique.[20]

Enfin, d'un point de vue éthique, la délimitation d'une identité numérique, tant par les États que par les individus, témoigne d'une certaine vision de la vie privée et des garanties incessibles malgré l'apparition du numérique. La loi du 6 janvier 1978 rappelait à juste titre qu'aucun asservissement à la technologie ne doit exister. Or, à trop céder ses données personnelles en contrepartie d'un maigre bénéfice au regard des profits que leur exploitation

[19] TURRETTINI (É.), « Des "chatbots" pour parler avec les morts », *Le Temps*, 26 fév. 2017, article en ligne.

[20] MORIN (V.), « Sophia, robot saoudienne et citoyenne », *Le Monde*, 4 nov. 2017, article en ligne.

permet, les individus ont fini par placer les entreprises du numérique en position hégémonique, portant eux-mêmes atteintes à leur vie privée.

Juvénal avait donc raison de se demander, dès le IIème siècle, qui garde nos gardiens. Dans ce cercle vicieux — ou vertueux, selon le point de vue — créé par la numérisation, États et individus tentent progressivement de s'allier contre les détenteurs et exploitants des données personnelles. Malgré ces efforts, pour le moment, les gardiens des bénéfices demeurent les colosses de la Silicon Valley, au-dessus de certaines lois, assis sur la relation de dépendance qu'ils ont instaurée.

Le droit sur l'identité numérique, mélange de collaboration inter-individus et étatique, basée sur une réglementation politique et une régulation citoyenne, impactée par des considérations sociales, économiques et juridiques, serait donc une arme de poids pour réajuster la balance, et faire de nos gardiens, nos obligés.

PREMIÈRE PARTIE. L'IDENTITÉ NUMÉRIQUE, ENTRE LA PERSONNE ET LA CHOSE

La classification stricte en deux parties a depuis longtemps permis aux juristes d'avoir un avis éclairé et global sur les objets du droit. La *suma divisio* entre les personnes et les choses n'y fait pas exception, tant elle est, et demeure encore aujourd'hui, structurante dans l'apprentissage du droit. Ainsi, la législation française distingue catégoriquement les biens, « toutes choses qui pouvant procurer à l'homme une certaine utilité sont susceptibles d'appropriation ».[21], et les personnes, physiques ou morales, êtres humains ou sociétés, et sujets de droits.

Structurant l'ordre juridique, leur fondamentalité les oppose : la personne, dès sa naissance, est un sujet de droit — le bien, inerte, est un objet de droit. Au fil du temps s'est construit une relation primordiale entre eux : le droit de propriété de l'un, sur l'autre. Cette garantie individualiste consacrée par les législateurs permet aux individus de disposer librement et comme ils l'entendent des biens sur lesquels ils ont acquis une propriété.

À l'heure du numérique, cette distinction tend à être affectée par l'apparition de nouveaux objets — ou sujets ? — de droit : les données personnelles. Reliées intrinsèquement à l'identité personnelle, qui, ayant subi un processus digital, se voit désormais numérisée, celles-ci posent de nombreux problèmes de qualification juridique, tant les débats sont agités entre les partisans de l'individualisation ou de la réification de cette identité. Tantôt celle-ci est une partie de l'individu, nécessitant un encadrement par un droit fondamental, et sur lequel l'État doit garantir une protection plus qu'efficace — tantôt celle-ci est un démembrement de son corps sur lequel l'établissement d'une propriété serait envisageable, fustigeant ainsi le principe de non-marchandisation du corps humain.

Les partisans des deux thèses s'affrontent encore pour atteindre la solution la plus adaptée — mais le numérique semble avoir remis en cause certaines stabilités juridiques, car des incohérences apparaissent régulièrement. L'exposition perpétuelle de soi et l'implication des individus dans ce processus ne rend pas la tâche facile, leur consentement (bien que parfois contestable) étant un obstacle majeur à la protection. Si la création d'un tel droit sur l'identité numérique devait aboutir, si louable serait-il, il faudrait encore classer les éléments identitaires dans l'une ou l'autre catégorie juridique — bien que, juridiquement et sociétalement, la doctrine tend plutôt vers l'individualisation de ceux-ci.

---

[21] ATIAS (C.), *Droit civil, Les biens*, 11ème éd., Litec, 2011, p. 1, *in* REBOUL-MAUPIN (N.), *Droit des biens*, 6ème éd., Dalloz, Hypercours, p. 9.

Titre premier – L'individualisation de l'identité numérique

De la naissance, à la compréhension, et à l'appréhension de la notion d'identité par les hommes, des milliers d'années se sont écoulées — plus que passionnante, son histoire révèle en réalité, mais non sans surprise, l'histoire des institutions politiques, des relations humaines, et des évènements historiques. Son utilité première sera pour l'individu de se nommer, lui, puis ses congénères — mais au fil du temps, diverses fonctions lui seront également reconnues. D'intérêt social, elle devient progressivement une aide étatique.

Alliée à des procédés techniques, elle se développe concomitamment aux évolutions matérielles des hommes : la démocratisation de l'écriture et de la lecture permet la création de registres identitaires, la naissance des fiches en accélère les procédés de confection, la photographie et la vidéographie renforcent les moyens policiers — c'est sans étonnement donc que le numérique révolutionne, à son échelle, l'identité et l'identification.

Le perfectionnement des technologies a engendré le dépassement des fonctions initialement étatiques de l'identité. Les entreprises du numérique ayant compris que les données personnelles la composant pouvaient avoir de la valeur, l'identité va devenir un objet de commerce — nécessitant *de facto* une protection, afin de ne pas porter démesurément atteinte aux droits des individus.

Chapitre 1. L'identité personnelle de l'individu et le numérique

Avant l'apparition du digital et d'internet, l'identité personnelle était un simple ensemble de caractéristiques physiques, appréhendables, permettant de reconnaître un individu au milieu d'une foule de citoyens. Il aurait été difficile pour les français du Moyen-Âge d'imaginer que cette identité puisse être dédoublée dans un monde virtuel, voire démembrée, à tel point qu'il faille lui créer une protection spécifique, tant parfois elle dépasse le cadre traditionnel de l'état civil et des descriptions physiques. Il est donc naturel que se soit développée dans un premier temps la notion d'identité personnelle, au fur et à mesure du perfectionnement des techniques de collecte des informations.

Par la suite, les bouleversements juridiques engendrés par la révolution numérique ont conduit à transposer les caractéristiques traditionnelles de l'identité vers un environnement digital, où leur importance et leur sens ont été contraints d'évoluer. Les implications juridiques n'ont pas conduit pour autant le législateur à définir textuellement l'identité, qu'elle soit personnelle ou numérique — aucun texte français n'en fait mention, si ce n'est de manière

détournée, par ses caractéristiques. Cette absence textuelle permet de faire le rapprochement entre l'identité et les droits de la personnalité, ce corpus de prérogatives fondamentales rattachées aux individus, car leur étude démontre un objet de protection similaire.

Section 1. L'apparition de la notion d'identité personnelle

Selon l'UNICEF, 51 millions de naissances par an ne sont pas déclarées, alors que l'identité est pourtant au cœur de problématiques fondamentales.[22] Malgré cela, une absence de définition textuelle persiste. Qu'elle soit nationale, personnelle, collective ou secrète, l'identité demeure pour le moment un mystère juridique. Qui souhaite s'y intéresser devra nécessairement emprunter des sentiers détournés pour l'appréhender — à commencer par les textes de loi y faisant référence. La Convention internationale relative aux droits de l'enfant de 1989 reconnaît, à titre d'exemple, un droit à l'identité en son article 7 : « L'enfant est enregistré aussitôt sa naissance et a dès celle-ci le droit à un nom, le droit d'acquérir une nationalité ».

Effectivement, il semble légitime qu'afin de s'insérer dans sa société, l'enfant doit être à même de se désigner, et de se distinguer de ses congénères. Ainsi, la première approche de l'identité est rendue possible par ses éléments de composition — en France, il s'agit de l'état civil, consacré dans l'article 34 du Code Civil, en tant que « les prénoms, noms, professions et domiciles ».

L'identité serait donc principalement réduite aux informations de base permettant de connaître un individu : sa dénomination, sa fonction sociale et sa localisation géographique. Or la réalité est toute autre. La notion regroupe bien plus de définitions qu'il n'y paraît, et tout autant de fonctions y sont rattachées. L'article 8 de la même Convention impose notamment des obligations positives aux États membres, qui s'engagent à « respecter le droit de l'enfant, de préserver son identité, y compris sa nationalité, son nom et ses relations familiales, tels qu'ils sont reconnus par la loi ».

Il appert qu'un individu est une identité, inséparables l'un de l'autre — la lui reconnaître revient à accepter le sujet de droit qu'il est. Bien plus qu'un simple agglomérat d'informations nominatives, l'identité est un concept juridique à part entière, représentatif des citoyens auxquels elle renvoie — elle a subi des évolutions juridiques liées aux évolutions des techniques d'identification, auxquelles elle est intrinsèquement liée, à commencer par la reconnaissance orale.

[22] Fiche thématique « Les droits de l'enfant : le droit à l'identité », unicef.org.

Paragraphe 1. De l'oralité à l'authentification de l'identité personnelle

La nécessité de s'identifier ainsi que ses congénères est née de l'« encellulement », le regroupement des hommes en communautés et en classes sociales.[23] L'individu isolé ne ressent pas l'utilité d'une dénomination dès lors qu'il ne connaît que sa propre personne. La volonté de s'unir au sein d'un groupe en osmose démontre vite ses limites lorsqu'aucun des hommes n'est distinguable du groupe. Il n'est donc rien de surprenant à ce que les premiers fondateurs de puissantes cités aient parfaitement intégré cette nécessité : c'est en effet les romains qui créèrent un des systèmes juridiques d'identification encore usité.

Le *tria nomina* comportait un prénom, un nom et un surnom : le *praenomen*, le *nomen* et le *cognomen*. Ce système d'identification, déjà inscrit dans ce qui était l'ancêtre d'un registre, permettait de distinguer les citoyens entre eux. Les femmes portaient le nom de leur père ou de leur mari et le port d'un nom complet permettait de reconnaître la citoyenneté d'un homme — ceux qui ne bénéficiaient que d'un prénom n'étaient que des pérégrins destinés à une vie nomade.

Cet exemple permet la démonstration parfaite des trois profits de l'identification. Originellement, elle permet de singulariser un individu. Dès lors que l'homme, sorti de son mutisme, rencontre son homologue, il lui est nécessaire d'obtenir un moyen de se nommer. Ce processus de reconnaissance passe par l'invention de l'outil nominatif. Puis, face à ses congénères, le besoin de se différencier au sein d'une petite communauté s'est fait sentir — cette communauté s'est progressivement transformée en ville, puis en État. L'identité collective est née de l'addition des identités de chacun de ses habitants.

Une fois cette entité politique formée, afin d'en assurer un fonctionnement efficace, il était nécessaire que les institutions puissent à leur tour reconnaître les hommes. Ces trois stades peuvent être retrouvés à toutes les périodes de l'histoire, à l'utilisation de chaque nouvelle technique d'identification, ce qui se vérifie toujours actuellement.[24] L'exemple le plus marquant est celui des réseaux sociaux : l'individu créé une page personnelle par le biais de son nom et de son prénom pour se singulariser, puis se différencie des autres par la publication de messages et de contenus variés propres à son identité, ce qui permet ensuite au reste de sa sphère de l'identifier et de le reconnaître.

En France, les premiers procédés d'identification ont émergé durant le Moyen-Âge. Initialement, il était très difficile de se distinguer, du fait du manque de moyens techniques. Cela n'était d'ailleurs pas sans poser de problèmes juridiques. La nécessité de l'appartenance de la notion d'identité personnelle à un individu précis, de manière inaliénable, prit tout sen sens dans une célèbre affaire jugée à Toulouse en 1560.

---

[23] ABOUT (I.), DENIS (V.), *Histoire de l'identification des personnes*, La Découverte, « Repères », 2010, pp. 8- 31.

[24] ABOUT (I.), DENIS (V.), *ibid.*

Martin Guerre, marié très jeune à son épouse, disparaît brutalement après douze ans de vie commune. Après quelques mois de questionnement, sa famille et son village finissent par admettre sa disparition. Ce n'est qu'après huit ans qu'il revient, et reconnaissant tout l'entourage qu'il a laissé, il reprend sa place chez lui et en société. Pourtant l'histoire révèlera qu'il s'agissait d'un imposteur, Arnauld Du Tilh, mis en cause trois ans après par un soldat en visite dans le village, qui avait fait ses armes avec le véritable Martin Guerre. Le procès qui eut alors lieu s'avéra extrêmement difficile, dans la mesure où l'imposteur connaissait les réponses à chaque question du juge — jusqu'à ce que le véritable Martin Guerre revienne, prouvant son identité. L'escroc fut condamné à mort, mais l'affaire, de par sa complexité, marqua les esprits.[25]

Initialement, l'oralité était donc le seul témoin de l'identité. Passer par les souvenirs des congénères était le seul procédé de reconnaissance, moyen totalement soumis à l'aléa de la mémoire. L'imposteur qui connaissait tous les détails de celui à qui il vole son identité était bien armé pour assurer la véracité de ses propos. Ceci ne serait plus possible de nos jours, par la multiplication constante des données, mais également grâce à l'authenticité des actes permise par l'écriture.

Paragraphe 2. La technicisation du traitement de l'identité personnelle

L'écrit s'imposera naturellement comme une preuve de validité pour les contrats et les documents officiels. C'est au XI^{ème} siècle qu'apparaîtra le sceau, l'un des premiers moyens d'authentification, bague de cire apposée sur des écrits afin de garantir l'identité de son possesseur. Les armoiries lui succèdent, symboles permettant d'obtenir des informations sur la position politique de la famille, ses membres, ou les alliances maritales, en un simple regard. Mais ce n'est qu'au XIII^{ème} siècle que les véritables systèmes de comptabilisation et d'enregistrement des individus voient le jour, initialement sous vocation religieuse. En 1214, le concile de Latran, convoqué par le Pape Innocent III, consigne scrupuleusement dans un registre les présents aux confessions obligatoires. Une première distinction est ainsi faite chez les fidèles — les absents n'auront pas le bénéfice de recevoir la communion de Pâques.

C'est ainsi que se développe les objectifs basiques des premières administrations : recenser les individus, les classer, et en déduire des informations afin de les scinder en diverses catégories. Les premières bases de données personnelles voient le jour au travers de cadastres

[25] ABOTT (B.) *Travelling Law-School and Famous Trials (First Lessons in Government and Law)*, Boston, D. Lothrop, 1884, pp. 50-57.

ou de registres d'enquêtes. Elles deviennent également des preuves d'identification car, après avoir listé la population, l'Église les utilisera pour dénoncer les criminels et les hérétiques.[26]

Les ancêtres de nos papiers d'identité apparaissent progressivement, sous la forme de sauf-conduits et de passeports — cette innovation visionnaire demeure majeure pour nos sociétés contemporaines. Il s'agit dans un premier temps de billets de santé, preuve de non-contamination lors des épidémies de peste. Au XV^{ème} siècle, cette pratique d'enregistrement s'accroit : il faut généraliser et enregistrer le plus d'individus possible, et tout autant d'informations sur eux. À l'instar de l'état civil actuel, cette volonté se manifeste initialement dans la tenue de registres de mariages, de baptêmes et d'enterrements.

C'est aux abords du XVI^{ème} et du XVII^{ème} siècle que les enregistrements identitaires deviennent des outils au service des politiques étatiques — la première d'entre elles sera tout simplement fiscale. L'État français est une nation unie et les registres permettent de déterminer les richesses de chaque famille pour, au nom de l'intérêt général, les taxer. Ce besoin de recensement s'intensifie avec le développement de techniques juridiques. La coopération qui éclot entre les institutions judiciaires pour retrouver les criminels en cavale impose des échanges de livres, contenants tous les avis de recherche.

L'état civil, le premier outil juridique à part entière, et survivant à toutes ces époques, apparaît en 1792 : y sont consignés des actes de naissance, de mariage, de baptêmes et de décès. La vie et la mort prennent désormais une notion plus légale que philosophique dans la mesure où s'y adjoint une personnalité juridique, acquise à la naissance et envolée au décès. Sans une reconnaissance gravée dans le marbre, l'identité de la personne n'est pas reconnue par l'État et celle-ci se retrouve sans droits.

C'est ainsi que, finalement, l'identité se définit en premier lieu par sa juridicité. Il s'agit déjà là d'un premier dédoublement : la personne physique est reconnue pour une personnalité juridique, une sorte d'entité morale lui garantissant des prérogatives, à la condition que son identité matérielle soit reconnue par la loi. L'individu peut exister sans personnalité juridique, mais il serait invisible aux yeux de son État.

Dans cette conception réside la fondamentalité de l'identification : au sein d'un système politique, la simple identité matérielle ne suffit pas à devenir un être de droit. Cette affirmation permettra, à l'avenir, d'appréhender au mieux l'importance de l'identité numérique, et son lien intrinsèque aux données personnelles. L'article 18 du Code Pénal ancien vient étayer notre propos, puisqu'il reconnaissait la mort civile aux condamnés à des peines à vie[27] — c'est-à-dire le retrait de toutes les prérogatives de droit rattachées à un individu. La personnalité juridique basée sur l'identité demeure encore aujourd'hui le fondement de la notion de personne.

Ainsi, l'article 311-4 du Code Civil dispose qu'« aucune action n'est reçue quant à la filiation d'un enfant qui n'est pas né viable », laissant donc la charge aux législateurs de déterminer le moment précis du début et de la fin de vie, problématiques qui sont toutes autant

[26] ABOUT (I.), DENIS (V.), *op.cit.*, pp.32- 55.

[27] GALLMEISTER (I.), « État et capacité des personnes », *Rép. Civ.*, juin 2016, rub. 38-54.

actuelles que complexes. Pour l'obtenir, l'enfant doit être né et viable[28], et être déclaré par ses parents à l'état civil.[29] Cette conception prend sa source dans les pratiques techniques mises en œuvre au fur et à mesure de l'histoire. L'état civil ne sera pas la seule invention qui soutint les procédés d'identification.

En 1801, l'obligation de recensement quinquennale est instaurée, elle qui perdure encore de nos jours. Puis dans les années 1830, le passage du registre — trop lourd et peu maniable — aux fiches, permet de recenser et de classer avec plus de rapidité et d'efficacité. Ce changement de support va améliorer le rendement des administrations. C'est ce qui conduira le XIV^{ème} siècle à connaître le plus de perfectionnements en la matière. Les papiers d'identité, devenus progressivement obligatoires, sont désormais délivrés par l'État qui a le monopole sur leur distribution.

Ils se développement en parallèle de la démocratisation des moyens de transport, et de l'émergence de flux migratoires conséquents — la nécessité de contrôler les entrées et les sorties du territoire apparaît, et les documents identitaires en attestent. Les casiers judiciaires, dans le même souci de protection, voient le jour, à des fins de contrôle des récidives, mais également pour permettre aux magistrats français d'avoir accès aux informations des criminels.[30]

Pendant la Première Guerre Mondiale, l'identité prend une nouvelle dimension, au travers des carnets A, qui recensaient les étrangers résidant en France, aptes à faire le service militaire, et les carnets B, qui pour leur part listaient les antimilitaristes et les déserteurs[31]. Ici encore, les funestes évènements causés par le régime nazi, pendant la Seconde Guerre Mondiale, étayent la thèse selon laquelle la destitution de l'identité entraîne la destitution de l'humanité. C'est la réflexion qu'adoptèrent les armées allemandes en assimilant les populations à des numéros, les privant de leurs identités avant de les exterminer. Les identités personnelles leur furent également un outil, puisque c'est en ayant accès aux registres des hôpitaux qu'elles purent mener à bien leur programme « Aktion T4 » — campagne d'extermination d'adultes handicapés physiques et mentaux.[32]

Trop souvent, et à tort, l'on considère que le passage à l'informatique s'est fait sans aucune transition. Or il est une innovation majeure que l'histoire occulte : la mécanographie. Une fois mises de côté les dérives tragiques causées par l'exploitation belliqueuse des données personnelles, l'évolution de celles-ci comme des outils administratifs s'est poursuivie. En ce sens, la mécanographie a considérablement joué dans la croissance de l'efficacité des

---

[28] Arts. 318 et 725, Code civil.

[29] Art. 55, Code civil.

[30] ABOUT (I.), DENIS (V.), *op. cit.*, pp. 32-55.

[31] FORCADE (O.), « Objets, approches et problématiques d'une histoire française du renseignement : un champ historiographique en construction », *Histoire, économie & société* 2012/2 (31ème année), p. 99-110.

[32] BENSOUSSAN (G.), « Éditorial », *Revue d'Histoire de la Shoah*, 2005, n° 183, pp. 5-15.

traitements de l'identité. Charles Babbage, mathématicien britannique, conceptualise en 1833 une machine capable d'effectuer une suite de calculs, sur l'idée d'un artisan français, Joseph-Marie Jacquard, d'allier à son métier à tisser des feuilles perforées pour les décorer.

Ce traitement mécanographique se matérialise aux États-Unis, sous l'impulsion du Bureau national de Recensement : le système de « carte perforée par machines électriques » était né. Thomas Watson, futur fondateur d'IBM, deviendra célèbre pour les perforatrices qu'il créa pour l'occasion.[33]

À compter de cette technologie, les premières machines informatiques étaient nées. Trois concurrents étaient sur le marché : du côté américain, IBM et Remington Rand — du côté français, la Compagnie des machines Bull. Celle-ci conceptualisera le premier des ordinateurs transistorisés, le Gamma 60. Les premières machines sont en réalité des calculateurs, se bornant à reprendre le principe de fonctionnement de la mécanographie, de manière à accélérer ces procédés.[34]

Quel impact cette technologie a pu avoir sur la notion d'identité ? En réalité, elle a permis que les procédés de collecte de ses éléments deviennent mécaniques, parfois même sans nécessité de supervisation humaine — cette mutation rend les traitements de données et les classifications plus rapides et plus efficientes, mais à contrario leur enlève une certaine confiance de la part des usagers, puisque l'absence de vérification par l'homme est gage d'insécurité. En outre, le développement des nouvelles technologies accessoires, telles que la photographie ou la caméra, ont fait rentrer dans les mœurs une nouvelle habitude : mettre la personne en image.

Ces premières expositions de l'individu conduisent nécessairement à penser aux droits qui en découlent, nés de ces pratiques, notamment le droit à la vie privée, qui par bien des aspects, rejoint les ambitions de la protection de l'identité numérique — car, d'un point de vue extensif, les éléments de la vie privée sont également des éléments identitaires.

---

[33] CHERIF (A.), « Introduction des nouvelles technologies et changements organisationnels au sein du ministère français des Finances : l'exemple de la mécanographie (des années 1930 aux années 1970) », *Entreprises et Histoires*, 2014/2, n° 75, pp. 24-41.

[34] VULBEAU (A.)., « Contrepoint – La Compagnie des machines Bull, de la mécanographie à l'informatique », *Informations sociales*, 2015/3, p. 52.

Section 2. Les droits traditionnels de la personnalité et l'identité numérique

L'étude de l'identité démontre d'insoupçonnées implications juridiques, pourtant logiques une fois exposées. Dès lors que celle-ci a été reconnue, il est devenu nécessaire de la protéger. Par son caractère intrinsèquement lié à la personne, la laisser sans garanties et à la merci de dérives reviendrait à dénier une protection aux individus — or il est impossible pour l'État de ne pas se préoccuper de ses gouvernés. Autour des personnes sont donc nés des droits et des libertés : les droits de la personnalité.

Ces droits plutôt récents ne sont apparus qu'au XX^{ème} siècle, et leur avènement a été permis par l'intérêt que leur a porté la doctrine, réalisant que l'apparition de concepts tels que la vie privée nécessitait un corpus de garanties protectionnistes. D'abord soutenue par les doctrines suisses et allemands, c'est le juriste français Alphonse Boistel qui les évoque initialement par sa théorie du droit, selon laquelle il « existe "des droits que l'homme apporte avec lui en naissant" ».[35] Ensuite reconnue par d'autres juristes, la théorie des droits de la personnalité fut également critiquée — mais sa reconnaissance par la Cour de cassation en 1969 mit un terme au débat.

Les droits autour de l'identité, et notamment le droit à l'image et le droit sur le nom, ont été les premiers reconnus par la doctrine. En ce qui concerne la vie privée, la doctrine l'ayant identifiée avant la loi, c'est le juge qui a permis sa protection. Dès sa consécration en 1970, le juge s'est appuyé sur celle-ci et en a nourri la doctrine, à laquelle se sont ensuite ajoutées des législations supplémentaires sur les droits de la personnalité, tels que la loi de 1978 relative à l'information, aux fichiers et aux libertés, ou la loi de 1994 sur le droit au respect du corps.[36]

Le sacrement de la vie privée s'est effectué de concert avec l'émergence du droit à la protection des données personnelles, témoignant d'une prise de conscience visionnaire du législateur. Ces deux notions sont en parfaite occurrence, puisque l'une ne peut aller sans l'autre. En effet, envisager la protection d'une identité numérique revient à protéger les éléments la composant, qui ne peuvent être diffusés publiquement, afin de garantir à l'individu une certaine sphère d'intimité — la vie privée, quant à elle, est une notion englobant tout ce qui relève du domaine personnel d'un individu, et est devenue un droit fondamental. Malgré sa reconnaissance textuelle, il n'en va pas de même pour l'identité numérique — à juste titre ou non, cela reste contestable : toujours est-il qu'une liaison assumée entre ces deux notions apporterait sans nul doute de la clarté juridique.

---

[35] BOISTEL (A.), *Philosophie du droit*, 1889, t. 1, n° 131 et s., *in* LEPAGE (A.), « Droits de la personnalité », 2009, actu. 2018, *Rép. civ.*

[36] LEPAGE (A.), « Droits de la personnalité », 2009, actu. 2018, *Rép. civ.*

Paragraphe 1. La corrélation indéniable entre le respect de la vie privée et de la protection de l'identité numérique

Les procédés d'identification et les éléments que ceux-ci prennent en compte ne sont pas les seuls composants d'une identité. En effet, il est totalement possible de rapprocher certains droits existants à la notion d'identité, en lien direct et total avec la personne, qui se verrait difficilement refuser la qualification de droit de la personnalité. Pourtant, aucun lien n'a été légalement réalisé jusqu'à présent entre les deux, alors que, fondamentalement, leurs visées sont similaires. L'histoire de la vie privée témoigne d'une volonté croissante de dissimuler certaines informations de l'ordre de l'intime, là où l'enjeu majeur de l'identité numérique est de protéger celles-ci d'exploitations abusives. À définitions divergentes, objectif similaire : la protection de la personne.

L'histoire de la vie privée témoigne d'une volonté croissante de protection de la personnalité des individus. Les premières évocations de cette notion remontent au siècle des Lumières, et s'expliquent par une opposition populaire au régime en vigueur, et par la volonté de s'affirmer contre l'État. Initialement, la vie privée n'a pas de raison d'être, puisque rien n'est dissimulé, pas même la vie du Roi. Elle apparaîtra donc avec l'idée d'un certain « raffinement » de la vie, et se développera concomitamment à la naissance des premiers médias.

Légalement, il faudra pourtant attendre la loi du 17 juillet 1970 pour que naisse l'article 9 du Code civil, disposant que « chacun a droit au respect de sa vie privée ». Jusqu'à cette date, les atteintes en la matière s'indemnisaient sur le fondement de l'article 1382 ancien du Code civil. Le Code pénal reprend ces dispositions dans son article 226-1, en réprimant toute atteinte volontaire à la vie privée d'autrui.[37] D'autres textes, et non des moindres, la consacre également, tels que la Convention européenne des droits de l'Homme, en son article 8.

Pourtant, nulle mention n'en est faite dans les constitutions françaises successives de 1946 et 1958. Le Conseil constitutionnel ne s'emparera timidement de la notion qu'en 1977, par le biais d'une décision sur la fouille des véhicules — considérant que celle-ci, donnant trop de pouvoir aux forces de police, était par trop attentatoire aux libertés individuelles.[38]

L'appui d'une vraie reconnaissance ne se fera que presque vingt ans plus tard, lorsque le Conseil reconnaît, après avoir examiné un projet de loi sur des systèmes de vidéosurveillance, que « la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle ».[39] En ce sens, ne serait pas inconstitutionnelle la loi qui instaure un régime général de vidéosurveillance dès lors que des garanties de recours s'offrent au citoyen

---

[37] ANTIPPAS (J.), et BEIGNIER (B.), « La protection de la vie privée », pp. 224-263, *in* CABRILLAC (R.), *Libertés et droits fondamentaux 2017*, Hors collection Dalloz, mai 2017, 1062p.

[38] C. Constit, n° 76-75 DC, 12 jan. 1977.

[39] C. Constit, n° 94-352 DC, 18 jan. 1995.

en cas d'abus. Fondé sur l'article 66 de la Constitution, qui place l'autorité judiciaire en garante de la liberté individuelle, la décision rattachait le droit à la vie privée comme une composante de cette dernière.

La vie privée ne deviendra un droit constitutionnel à part entière qu'en 1999, le Conseil estimant que « la liberté » proclamée par l'article 2 de la Déclaration des droits de l'Homme et du citoyen « implique le respect de la vie privée ».[40] En revanche, ces consécrations législatives n'excluent pas de nombreux débats sur le contenu de la vie privée, et les informations qui sont, ou non, inclues en son sein et protégées.[41]

Selon Aristote, la vie publique relève de l'État, et la vie privée de l'individu — mais le problème, encore récurrent aujourd'hui, est de placer le curseur de cette frontière. L'on peut malgré tout en définir trois composantes majeures : le secret de l'individu sur certains aspects de lui-même, la possibilité d'être isolé des atteintes extérieures et de protéger l'intimité, et l'autonomie individuelle, au travers d'un contrôle sur les informations divulguées ou non.[42] De nombreux débats agitent la sphère juridique en la matière, notamment sur les divergences entre la vie privée et l'intimité. L'article 9 du Code civil, en son alinéa 2, évoque en effet une « atteinte à l'intimité de la vie privée ».

Le flou sur la notion ne peut que trouver matière à s'accentuer ici, puisqu'alors l'intimité serait une partie encore plus sensible de la vie privée, elle-même regroupant déjà des développements ? Faute d'une véritable réponse, la jurisprudence s'est construite en considérant au cas par cas si une information ou non était protégeable à ce titre. Selon les contextes et les enjeux, l'appréciation sera différente. La notoriété de la personne entre par exemple en jeu puisque « ces droits, lorsqu'ils sont invoqués au profit d'une personne que sa naissance ou ses fonctions exposent à la notoriété et la curiosité du public, ou qui a elle-même divulgué certains faits relatifs à sa vie privée, ne peuvent s'apprécier avec la même rigueur que lorsqu'il s'agit d'un citoyen anonyme éloigné des médias ».[43]

La Cour Européenne des Droits de l'Homme s'est également confrontée à ce souci de distinction dans plusieurs cas d'espèces, l'amenant à favoriser casuistiquement la liberté d'expression ou le droit au respect de la vie privée — consacrée par l'article 8 de la Convention européenne de sauvegarde des Droits de l'Homme et du Citoyen. Bien souvent, le journalisme et le droit d'information du public se confrontent à la vie privée, et tout particulièrement à celle des personnes « publiques ». La Haute juridiction effectue donc une mise en balance entre ces deux piliers des droits français et européens, afin de ne porter d'atteinte majeure ni à l'un, ni à

---

[40] C. Constit, n°99-416, 23 juil. 1999.

[41] MAZEAUD (V.), « La constitutionnalisation du droit au respect de la vie privée », *Nouveaux cahiers du Conseil constitutionnel*, n° 48, juin 2015, pp. 7-20.

[42] ROCHELANDET (F.), *Économie des données personnelles et de la vie privée*, La Découverte, 2010, pp.6- 20.

[43] ANTIPPAS (J.), et BEIGNIER (B.), « La protection de la vie privée », pp. 224-263, *in* CABRILLAC (R.), *op. cit.*

l'autre.

Ainsi, dans une série d'arrêts opposant la princesse monégasque Caroline de Hanovre à des magazines allemands, les solutions furent divergentes. Dans une première décision de 2006, la Cour censura la publication de nombreuses photos d'elle et de sa famille, considérant que celles-ci ne contenaient aucun contenu en relation réelle avec les clichés, dépourvus en outre d'intérêt informationnel. Ici, la vie privée de l'intéressée prenait le pas volontairement afin de lutter contre le comportement parfois intrusif et gênant d'une presse à scandale.[44] Mais dès lors que les mêmes publications seraient importantes pour le public, celles-ci ne sauraient être censurées — il était donc impossible de faire disparaître un article illustré sur la santé du prince régnant, car il en va de l'intérêt des gouvernés que de connaître les actualités de la famille royale.[45]

La Cour rappelle systématiquement, dans les arrêts en la matière, qu'elle n'est pas juge de la légitimité de la mise en balance effectuée par les juridictions étatiques, mais bien garante de sa réalisation et de sa justification. En réalité, il n'existe pas non plus de définition de la vie privée dans l'article 8 de la Convention, caractérisée par opposition à d'autres intérêts, que sont la liberté de la presse, le droit du public à l'information ou la liberté d'expression. L'exemple le plus marquant restera un arrêt de 2014 dans lequel la Haute juridiction considéra que la publication d'un livre sur la vie du président François Mitterrand, instantanément après son décès, constituait une atteinte à la vie privée de sa famille, atteinte qui s'amoindrirait avec le temps, jusqu'à ce que lui prévale le droit du public à l'information.[46]

Au sein du droit français, d'autres propositions ont été émises, notamment opposer la vie privée à la vie publique. Or la séparation entre ces deux notions ne peut être tant stricte, car se pose le problème de la pratique de certaines activités privées, qui pourtant se déroulent en public : aller au cinéma ou au théâtre, à titre d'exemple.[47]

Mais la vie privée — à l'image de tous les droits de la personnalité, celui-ci faisant figure de référence car le plus atteint et le plus monopolisé — est constamment mise à l'épreuve dans le numérique, qui ici encore, fait évoluer les usages et le droit. Désormais, ce qu'englobe le terme de vie privée fait peu d'écho à la réalité des choses, puisque la notion elle-même est amenée à évoluer du fait des nouvelles technologies. L'homme étant constamment fiché et surveillé, le niveau de fondamentalité des droits a baissé. La technologie n'a, en réalité, pas modifié les techniques ou la fréquence du fichage : elle a simplement fait entrer dans les mœurs l'intervention d'un regard observateur.

---

[44] VOORHOOF (D.), note sous CEDH, 24 juin 2004, n°59320/00, Affaire Von Hannover c. Allemagne, *IRIS*.

[45] Note d'information sur la jurisprudence de la Cour n°149, greffe de la Cour, 7 fév. 2012, n°60641/08, Von Hannover c. Allemagne (n°2).

[46] CEDH, 2ème sec., 18 mai 2014, n° 58148/00, Affaire Éditions Plon c. France.

[47] LEPAGE (A.), « Droits de la personnalité », 2009, actu. 2018, *Rép. civ.*

En outre, celle- ci est renforcée par le principe d'acceptation selon lequel les utilisateurs dévoilent d'eux-mêmes leurs informations sur les réseaux sociaux ou les espaces numériques, rendant plus difficile la garantie des droits et libertés fondamentaux — car se pose alors la question de la délimitation du rôle du juge et de l'utilisateur. Le juge doit-il protéger une atteinte à la vie privée dès lors que l'information en question aurait été divulguée par la personne elle-même ?[48]

Il existe bien un lien indéfectible entre la vie privée et l'identité numérique, ces deux notions n'ayant pas la même signification, mais se rapportant finalement au même objet : les informations personnelles de l'individu. La vie privée se manifeste par toute information confidentielle pour une personne, se devant de rester secrète. Or les enjeux de la protection de l'identité numérique sont de protéger de la divulgation les informations qui la composent.

Ces deux notions n'ont donc pour but final que d'empêcher que l'intimité d'une personne, qu'il s'agisse de son image ou de son identité, ne soit divulguée à tous. Dans ce cas, la reconnaissance d'un droit sur l'identité numérique ne pourrait être qu'un bénéfice juridique, qui permettrait alors d'y englober la vie privée, afin que ces deux aspects de la personne soient efficacement protégés des atteintes extérieures.

Paragraphe 2. Le ralliement nécessaire du respect de la vie privée et de la protection de l'identité numérique

Certains auteurs ont envisagé une solution afin de lier la vie privée et l'identité numérique, suivant une américanisation de la vie privée. En effet, le *right to privacy* conféré aux citoyens des États-Unis leur donne un droit d'agir positif, en choisissant de dévoiler ou non certaines informations, à la différence de la France qui garantit une protection contre les atteintes à posteriori. Ainsi, aucune atteinte n'est invocable après leur diffusion puisque le consentement a été préalablement donné — en revanche, si des données potentiellement destinées à rester privées fuitent, alors une action en justice est envisageable. Le droit américain en la matière est tiré du *Privacy Act* de 1974 qui définit des lignes de bonne conduite, telles que l'interdiction de collecte des données par des systèmes d'enregistrements dissimulés. Certaines données sont, elles, protégées automatiquement à raison de leur nature : les données de santé, les données financières, ou les données rattachées aux mineurs, considérées comme sensibles.

[48] RODOTA (S.), « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements*, 2010, n° 62, pp. 55-70.

Le droit à la vie privée résulte en fait de l'appréciation que tout un chacun en a, et du niveau de protection que l'ensemble de la société pourrait attendre en la matière.[49] Ainsi, dans son arrêt « *Katz c. États-Unis* », la Cour suprême américaine, en 1967, considérait que le fait d'enregistrer et d'utiliser à son insu et contre lui les conversations téléphoniques d'un détenu était contraire au quatrième amendement de la Constitution, qui dispose du « droit pour les personnes de voir leurs identités, domiciles, documents et effets protégés des perquisitions et saisies non motivées ». Sa motivation était l'affirmation selon laquelle l'opinion publique était en droit de considérer qu'une fois à l'abri d'une pièce close, une conversation téléphonique demeure privée — à ce titre, l'enregistrement, même d'un détenu, constituait une violation constitutionnelle.

Ce « *legitimate expectation of privacy test »* permet d'établir des critères de mesure de l'atteinte à la vie privée plus proches de la réalité, puisque plus proches de l'opinion publique. Si le test est positif, des dommages-intérêts sont alors versés — le cas échéant, aucune atteinte n'est sanctionnée. Ce système permet de donner de la valeur à la conception juridique de la vie privée par les premiers concernés : les individus eux-mêmes.[50]

En France, les atteintes à la vie privée sont contrôlées à posteriori d'une éventuelle infraction, ce qui limite considérablement l'effet des moyens de sensibilisation. Il semble clair que donner plus de pouvoirs aux citoyens sur leurs informations serait une nécessité, car dans certains cas, face au numérique, la voie juridique n'offre pas pleinement satisfaction. D'un autre côté, l'usage du dévoilement de sa personne est tant rentré dans les mœurs qu'il paraît difficile de croire que, même avec la possibilité de ne rien dévoiler, le citoyen dissimulerait ses informations. L'exposition de soi est devenue une habitude, dont peu pourraient se passer — y compris les plus jeunes d'entre nous.

Sans nécessairement tomber dans ces extrêmes, il serait louable d'envisager un recoupement des deux notions, au sein d'un même et unique droit, englobant alors le respect à la vie privée dans son volet digital — réseaux sociaux, blogs, géolocalisation — et l'identité numérique. Outre une simplification du droit, cela permettrait de réunir les prérogatives rattachées à ces deux notions, et les atteintes seraient sans doute moins nombreuses, car mieux sanctionnées. De plus, il existe déjà des droits sur l'identité numérique, bien qu'elle ne soit pas consacrée textuellement ainsi, qui trouveraient à s'intégrer dans un tel droit de la personnalité.

---

[49] Conseil d'État, *Le numérique et les droits fondamentaux*, étude annuelle, 2014, pp. 72-73.

[50] Supreme Court of the United States, 18 déc. 1967, Charles Katz c. United States, *in* WALTER (J-B.), « La protection du droit au respect de la vie privée : entre texte et prétextes (Retour sur les arrêts Van Hannover…) », *RLDI*, n° 98, 1er nov. 2013, pp. 34-40.

Chapitre 2. De l'identité numérique aux données personnelles

Étymologiquement, le terme d'identité est issu du grec *idem*, signifiant « le même ». Elle renvoie donc à l'image personnelle que se fait l'individu de sa personne, et de toutes les caractéristiques qui le composent. Jusqu'à la numérisation mondiale que connaît aujourd'hui notre époque, les principales caractéristiques de l'identité étaient appréhendables. Les titres d'identité étaient basés sur les informations d'état civil et sur les caractéristiques physiques, matérialisées par l'individu lui-même ou par des actes juridiques authentifiants.

Il est notable que ces caractéristiques ont vu leur liste, non exhaustive, s'allonger au fur et à mesure des avancées techniques. Les photographies sont venues étayer les documents d'identité, les caméras ont enrichi les fichiers de police de preuves visuelles, et les instruments de mesure de plus en plus perfectionnés ont accru la potentialité de mesures de la personne — la fréquence cardiaque, l'odeur, ou encore le niveau d'activité physique sont également devenus des caractéristiques identitaires.

Dès lors, les données personnelles ont pris une double ampleur. Elles sont devenues des éléments de l'identité, en sa partie numérique, puisqu'elles contribuent à déterminer la personne et permettent même parfois une identification — rappelons la définition textuelle de ces données qui ont pour vocation d'identifier un individu —, mais elles sont également devenues un moyen de s'exprimer pleinement. « Ce jeu identitaire (pseudo, photo, attirances, etc) est potentialisé par les sites de socialisation, que ce soit dans le domaine du jeu, des sites de rencontre amoureuse ou dans le réseautage professionnel, et permet de construire une personne ».[51]

Section 1. La numérisation progressive de l'identité personnelle

L'identité personnelle comprend des caractéristiques purement physiques, concrètes, ou tout du moins appréhendables. Elle recense les éléments d'état civil, mais également les informations sociales — le numéro de Sécurité sociale, l'adresse, l'âge, le casier judiciaire —, la description physique de la couleur des yeux à la taille, ou aux marques particulières. Ces informations sont purement descriptives et rattachées à la personne — elles ne sont pas des déductions faites à partir de la personnalité.

[51] PIERRE (J.), « Génétique de l'identité numérique », *Les Cahiers du numérique*, 2011/1, vol. 7, pp. 15-19.

L'identité numérique, elle, a d'abord changé de format. Les données personnelles, concrètement, ne sont que des suites de flux d'informations transformées en suites de 0 et de 1 afin d'être appréhendées par les machines qui les traitent — la mutation est énorme au regard des noms et des prénoms sagement inscrits dans des registres identitaires.

En outre, l'identité numérisée ne permet même plus de justifier de l'existence physique d'une personne. En effet, lorsqu'un individu naît, son identité lui permet de se nommer, comme évoqué précédemment, mais elle lui est également un marqueur sociétal et légal puisqu'elle lui confère une personnalité juridique. L'identité atteste des droits dévolus à un citoyen, qu'il perdra au jour de son décès. Il n'en va pas de même pour l'identité numérique. La science-fiction n'est pas la seule à évoquer la possibilité future de transférer les consciences dans un ordinateur à la mort.[52]

La mort numérique va réellement commencer à un poser un problème, tant juridique qu'anthropologique, puisqu'il est estimé que chaque jour, trois personnes inscrites sur Facebook meurent par jour, laissant derrière elles des profils abandonnés — devant lesquels le législateur reste pour le moment assez perplexe.[53] Sur le fond, l'identité personnelle et l'identité numérisée composent chacune une partie de l'identité globale d'un individu, avec leurs similitudes et leurs divergences, qui seraient à prendre en compte dans l'élaboration d'un droit sur celle-ci.

Paragraphe 1. L'identité personnelle numérisée

L'histoire des procédés techniques d'administration et d'identification est intéressante, car ils ont conduit l'identité personnelle à évoluer — or, se faisant, des implications juridiques particulières ont vu le jour, qu'il a fallu prendre en compte et qui sont devenues une partie de la loi. En effet, sans le développement du numérique, jamais il n'aurait été nécessaire de dédoubler la matérialité de la personne dans un univers digital. La combinaison des apprentissages techniques que sont le codage, la création de logiciels, et le perfectionnement des systèmes d'exploitation avec l'apparition des ordinateurs a ainsi impacté plus que de raison la notion d'identité sous toutes ses formes.

[52] FIÉVET (C.), « Une vie numérique éternelle en 2067 ? », *Inria*, 12 nov. 2017, article en ligne.

[53] FORÊT (É.), « Il y aura bientôt plus de morts que de vivants sur Facebook », *France Inter*, 31 oct. 2017, article en ligne.

L'utilisation des machines permit en effet, tout comme la mécanographie en son temps, d'augmenter les performances de traitement des informations. Ainsi, les fichiers informatisés contenant les identités des personnes sont vite apparus. C'est d'ailleurs un projet de répertoire de la population française dans le fichier SAFARI — Système automatisé pour les fichiers administratifs et le répertoire des individus — qui causa une grave polémique nationale, à l'origine de la loi du 6 janvier 1978 garantissant la protection des informations nominatives.

Mais c'est avec l'alliance de la technologie et du processus internet, que l'identité sera réellement amenée à évoluer. La connectivité va révolutionner la conception de l'informatique : l'ordinateur autrefois seul compétent à traiter et à stocker des données, va désormais pouvoir les partager avec d'autres machines, et en déduire de nouvelles masses d'informations. Il ne sera pas nécessaire d'attendre longtemps pour que les industriels réalisent les potentialités de bénéfices rendus possibles par la commercialisation de ces masses de données. L'entrée dans le monde du « big data » est en réalité une intrusion dans le domaine privé de chaque utilisateur du numérique.

Quelles conséquences juridiques ? L'identité personnelle va progressivement être recopiée dans les abysses numériques et devenir un fond d'investissement pour les entreprises privées y ayant accès. Du simple programme de fidélité d'un magasin aux données divulguées sur les réseaux sociaux, toute information est importante en ce qu'elle permet de déterminer une personnalité numérique. Celle-ci se détermine grâce à la présence numérique, l'ensemble des « traces » qu'un utilisateur laisse derrière lui, volontairement ou non, en surfant sur le Web.

Elle passe par le biais de toute connexion fixe ou d'objet connecté, lors de la consultation de moteurs de recherches, ou de pages fonctionnant avec des cookies. S'il est possible d'utiliser ces informations et de les relier à une personne déterminée, alors, elle devient une partie de l'identité numérique.[54] Or derrière cette notion se cache la nécessité de protéger l'individu auquel elle est rattachée, afin que ses droits et libertés fondamentaux restent pleinement efficients.

Cette identité numérique peut être scindée en trois facettes. La première est l'identité déclarative. Il s'agit d'une description de la personne faite par elle-même, de son plein gré. Celle-ci peut donc être fausse — plus elle est étoffée, et plus la différenciation des autres usagers du Web est forte. Ensuite vient l'identité agissante, composée de l'ensemble des actions réalisées par l'internaute.

Enfin, la dernière est l'identité calculée. Elle est faite des recoupements de toutes les informations sur une personne, qui permettent d'en déduire de nouvelles — à titre d'exemple, une personne qui compte beaucoup de relations sur les réseaux peut être considérée comme une personne sociale. À partir de cette facette de l'identité sont notamment déterminées les

[54] ROCHFELD (J.), « L'identité numérique », p. 151., *in* BOLLÉE S. et PATAUT É. [dir], *L'identité à l'épreuve de la mondialisation*, IRJS Éditions, 2016.

habitudes de consommation, et les publicités personnalisées que proposent les navigateurs en sont le résultat.[55]

Mais il n'existe pas que des caractéristiques matérielles à la composition identitaire. Certains auteurs, tels que Daniel Gutmann, traitent également d'un « sentiment d'identité », c'est-à-dire de l'appréhension globale que peut avoir un individu sur sa propre constitution. Ce sentiment est impacté par le droit, car la constitution d'un état et son régime politique peuvent influencer ce ressenti.[56]

Ce sentiment d'identité peut rejoindre la notion d'e-réputation qui a une importance non négligeable dans la vie des utilisateurs. La sociabilisation est une composante essentielle du bien-être d'une personne, mais elle suppose l'existence d'un réseau. Ce réseau, autrefois matérialisé par le voisinage, l'amitié, ou la famille, est désormais matérialisé dans les applications sociales telles que Facebook, Instagram, ou Twitter. Or ce besoin de lien humain est désormais une composante à part entière de l'identité, tant il apporte une satisfaction inexplicable.

L'individu ressentira une sorte d'apaisement à se doter d'un réseau numérique étendu et diversifié. La réputation digitale et la popularité numérique sont désormais des éléments à part entière de l'identité — ces constatations sont d'autant plus véridiques lorsqu'elles s'appliquent aux jeunes populations.[57] Qui plus est, de nouvelles caractéristiques sont venues se rajouter à celles préexistantes à l'identité traditionnelle.

Paragraphe 2. L'apparition de caractéristiques inhérentes à l'identité numérique

Bien qu'il ne s'agisse que d'une transposition de l'identité personnelle, l'identité numérique présente des divergences : lors de la rédaction de la loi du 6 janvier 1978, qui préconisait de protéger les données personnelles afin qu'internet reste un service pour ses utilisateurs, l'engouement pour le numérique et son utilisation étaient encore limités. En outre, si l'on prend pour référence l'identité personnelle au sens des éléments d'état civil, l'identité numérique ne reflète pas véritablement la personne que nous sommes. Les caractéristiques physiques des personnes dans les fichiers de police sont telles qu'elles permettent de retrouver

---

[55] GEORGES (F.), « L'identité numérique dans le web 2.0 », *Le mensuel de l'Université,* n°27, juin 2008, article en ligne.

[56] MUIR WATT (H.), « Gutmann (Daniel) : Le sentiment d'identité (Étude de droit des personnes et de la famille », *Rev. crit. DIP*, 2000, pp. 947-950.

[57] MERCKLÉ (P.), *Sociologie des réseaux sociaux*, La Découverte, 2016, pp. 37-54.

un fugitif rapidement, dans la mesure où les descriptions et les photographies sont une représentation fidèle de celui-ci.

L'identité numérique demeure plus floue. Partager une information intime sur un réseau social n'a pas nécessairement de véracité tant que personne ne l'a vérifiée — en outre, elle peut très bien être modifiée volontairement par l'utilisateur [58] Nombre de réseaux sociaux témoignent parfois d'un besoin de popularité, passant par la publication constante de parts de leur identité — ce qui entraîne beaucoup de considérations philosophiques sur la vision qu'ont désormais les personnes d'elles-mêmes. Digitalement, le regard et l'acceptation de la sphère numérique sont plus qu'importants.

L'identité numérique se développe à l'ère de « l'extime » — en tant que contraire à l'intime » — : ce que l'on accepte de dévoiler et que l'on ne considère pas comme de la vie privée. Cette contradiction humaine pousse à choisir les informations qui peuvent être partagées, ou non, parfois selon les récepteurs. L'identité numérique se scinde en deux blocs : ce qui est diffusable, et ce qui ne l'est pas. On assiste ainsi à une floraison de pages personnelles et de blogs, véritables espaces de parole — qui parfois font oublier qu'il ne s'agit pas de lieux dématérialisés, mais bien d'une place publique, tout autant accessible que si le message était crié dans la rue devant des centaines de personnes.

En outre, mentir ou améliorer la réalité pour accroître sa réputation numérique devient une habitude qui a nécessairement un impact sur l'identité — si la personne ne parvient plus à se définir elle-même, il est compliqué pour les autres d'y arriver. Ces nouvelles habitudes digitales peuvent modifier la structuration de l'identité et la perception personnelle, et ce notamment pour les adolescents, qui grandissent avec la technologie et se perdent dans tant de facettes.[59]

L'identité personnelle relève donc de l'ipséité des données, là où le numérique pose un paradoxe : les individus perdent la maîtrise sur leur identité, mais la protègent également par le biais de nouvelles méthodes d'identification — digitale, ou visuelle, par exemple. Si l'on s'en tient à cette approche, alors l'identité numérique n'est qu'une fidèle transposition de l'identité civile — or y ont été ajoutés d'autres éléments constitutifs non pas de l'identité, mais de la personnalité. Bien que très proches, ces deux notions sont divergentes.[60]

Pour autant, à considérer l'identité numérique plus comme une composante de l'identité que comme une de ses formes, sa reconnaissance légale serait également bénéfique. Sa consécration permettrait en effet de mieux appréhender les infractions commises en ligne — infractions facilitées par l'anonymat que procure internet —, et donc de renforcer la sécurité publique. L'identification passe par tout un faisceau d'indices dans la vie réelle, notamment les photographies, les descriptions physiques, les éléments d'état civil, les

---

[58] ROCHFELD (J.), « L'identité numérique », p. 153., *in* BOLLÉE S. et PATAUT É. [dir], *op. cit.*

[59] PUYUELO (R.), « Journaux "extimes" et communauté de l'anonyme », *EMPAN*, n°176, 2009, pp. 30-36.

[60] MERLAND (L.), « L'identité civile des personnes : "Is big data beautiful ?" », *RLDI*, 1er déc. 2015, n°121, pp. 37-39.

empreintes — faisceau qui ne peut être reproduit à l'identique sur le Web, où y sont pour l'instant assimilés l'adresse IP, les pseudonymes ou les photographies, à manipuler avec précaution puisque potentiellement mensongers.

Reconnaître une identité numérique légalement permettrait de mieux délimiter les contours de la notion et de lui conférer une utilité sécuritaire. Le droit est parfois incohérent sur le sujet puisqu'il reconnaît déjà un délit d'usurpation de l'identité numérique, incluant notamment des pratiques telles que le *pishing*, le vol d'identifiants bancaires. « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération », telle est la définition qu'en donne l'article 226-4-1 du Code Pénal.[61] Il s'agit déjà d'un progrès dans la mesure où, avant cette reconnaissance, il n'était possible de se plaindre d'une usurpation d'identité que pour les infractions résultant de ce vol, qui, de ce fait, n'étaient souvent pas caractérisées.[62]

Dans certains domaines, une identité numérique existe déjà en tant que moyen d'identification autonome. Un arrêté de 2016 a en effet créé un système d'interconnexion entre les greffes des tribunaux de commerce, dans le but de permettre aux parties d'avoir accès aux documents plus facilement. Lorsqu'un utilisateur s'enregistre pour la première fois, il donne son consentement pour toutes les connexions futures, et se créé ainsi une identité sur la plateforme. Les documents ainsi déposés et consultés sur la plateforme auront une authenticité numérique.[63] Évoluerait-on vers une caractérisation de l'identité numérique en tant que telle ?

Notons, en ce sens, qu'il ne s'agit pas du seul concept juridique à n'être défini que par les textes qui les protègent. C'est le cas de la vie privée, comme évoqué précédemment, qui n'est jamais définie textuellement, mais est déduite par la doctrine et la jurisprudence des textes garants de la protection des données personnelles ou des droits de la personnalité. Pourtant, il s'agit d'une notion fondamentale, et efficacement protégée. L'absence de consécration textuelle n'est pas nécessairement un frein à la reconnaissance de droits et à leur protection législative — ainsi, de nombreux droit sont apparus autour de la notion d'identité personnelle.

[61] Art. 226-4-1, Code pénal, inséré par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

[62] SAENKO (L.), « Le nouveau délit d'usurpation d'identité numérique », RLDI, n°72, 1er juin 2011, pp. 63-69.

[63] BLÉRY (C.), « SECURIGREFFE : l'identité numérique judiciaire opposable est née », *JCP G*, n°9-10, 29 févr. 2016, p. 256.

Section 2. Les droits de l'individu sur les données personnelles

Bien que les tergiversations sur l'identité numérique rendent pour l'instant compliquée la délimitation de cette notion, il est un ensemble de droits émergents dont les gouvernements français et européens se sont emparés avec une rigueur constante. Les données personnelles sont désormais au cœur des préoccupations gouvernementales dans le domaine du digital. Il est impossible d'ignorer la réglementation européenne qui rentrera en vigueur en mai 2018, et son impact sur les acteurs privés et publics. Cet intérêt croissant pour une telle problématique illustre bien le paradoxe constant en la matière : une volonté de protection de la vie privée et des données personnelles face à la pratique sociale de dévoilement de soi poussée à l'extrême, notamment sur les réseaux sociaux.[64]

En France, la création de la loi du 6 janvier 1978, très visionnaire pour son époque, fut le résultat d'un scandale civil : l'affaire SAFARI. Pourtant, les évènements liés à l'exploitation de données personnelles — et également reliées au respect de la vie privée — ont toujours été récurrents dans l'histoire. En témoigne d'ailleurs la fameuse affaire « des fiches », qui, en 1904, mettait à mal le gouvernement français. Le Figaro révélait en effet des documents attestant de l'existence d'un réseau national de surveillance des fonctionnaires, impliquant l'organisation franc-maçonne, et auquel participait des hauts dirigeants administratifs.[65]

Les premières difficultés liées à l'exploitation des informations nominatives individuelles n'ont pas eu besoin de la numérisation et de l'apparition d'internet pour émerger. En revanche, elles en ont été renforcées et la nécessité de poser un cadre juridique était pressante. Bien que l'État français ait pris de l'avance en la matière sur ses voisins européens, l'anticipation d'une telle avancée technologique ne fut pas vaine, en témoigne aujourd'hui le vaste débat dont elles sont l'objet principal.

---

[64] PERRIAULT (J.), « Traces numériques personnelles, incertitude et lien social », *Hermès, La Revue* 2009/1, n°53, pp. 13-20.

[65] LALOUETTE (J.), *L'État et les cultes, 1789-1905-2005*, La Découverte, 2005, pp. 37-52.

Paragraphe 1. L'émergence d'une réglementation des données personnelles

La notion de données personnelles évolue nécessairement avec ce que l'on intègre ou non dans la notion de vie privée, c'est-à-dire ce qu'il est acceptable de dévoiler ou pas. Révélatrice de mécanismes sociaux, la donnée personnelle témoigne, tout comme les procédés d'identification, d'un certain contexte politique. C'est le cas de l'identification biométrique, populaire dans certains pays d'Amérique latine, mais qui a pourtant du mal à s'implanter en Europe. La raison principale en est une immigration très forte, mais aussi un manque de reconnaissance envers l'identité étatique. Les pays ont un besoin assez important de sécurisation de l'identité, passant par des procédés techniques d'identification, assez compliqués à pirater. Falsifier un visage ou tenter de prendre celui d'une autre personne semble en effet assez ardu.[66]

Les données personnelles sont l'ensemble des données permettant de distinguer un individu d'un autre, au sein d'un collectif. Inutiles lorsqu'elles sont prises séparément, elles deviennent personnelles dès lors qu'un recoupement avec un individu peut être effectué. Elles sont pérennes ou obsolètes, collectées légalement ou non, publiques ou privées, cédées par l'utilisateur volontairement ou à son insu — leurs modes de collecte sont tout autant variés, puisqu'ils vont du formulaire d'abonnement, au réseau personnel, en passant par les requêtes sur les moteurs de recherches, les fichages des administrations ou encore la géolocalisation. Ce bien à part n'appartient pas réellement à l'individu auquel il se rattache, car il peut y avoir des dizaines de détenteurs d'une même donnée personnelle.[67]

La maîtrise des données personnelles permet de gérer au mieux les relations avec les autres : l'on accepte de dévoiler certaines choses ou pas selon les personnes, comme dans la vie réelle. La vie privée est en effet interdépendante du contexte social : l'autonomie informationnelle dépend de notre environnement. Dans une dictature ou un pays intolérant, il serait par exemple impossible de revendiquer une sexualité différente ou de s'opposer au pouvoir politique en place. C'est en cela que les textes protecteurs des données personnelles permettent de réguler les individus : sans anéantir l'intolérance, ils limitent les atteintes aux personnes — en effet, attaquer une caractéristique personnelle revient à dénigrer une identité.

---

[66] DUBEY (G.), « Sur quelques enjeux sociaux de l'identification biométrique », *Mouvements*, 2010/2, n° 62, pp. 71-79.

[67] ROCHELANDET (F.), *op.cit*., pp. 38- 66.

Les réseaux sociaux ne sont pas de bons outils en la matière, car la vigilance diminue face aux écrans. Il est plus difficile d'imaginer une fuite d'informations, et ainsi l'on en arrive à des abus : les parents dénichent des secrets sur leurs enfants, les patrons sur leurs employés, et les litiges en la matière deviennent de plus en plus complexes.[68]

En outre, les vices entraînés par ces nouvelles habitudes sont poussés à leur paroxysme par certaines entreprises peu scrupuleuses. C'est le cas de celles qui développent des *keyloggers*, logiciels espions qui enregistrent chaque saisie sur un clavier d'ordinateur — permettant ainsi d'obtenir identifiants, mots de passes, ou recherches de l'historique. L'un d'entre eux a d'ailleurs récemment défrayé la chronique, utilisant comme argument de vente la possibilité de surveiller ces enfants ou la fidélité de son conjoint.[69]

Une réglementation autour des données personnelles était donc plus que nécessaire. Celle-ci s'est construite autour de la numérisation des informations nominatives. Les horreurs des conflits successifs du XX^{ème} siècle marquèrent en effet les esprits, de par l'utilisation massive des fichiers identitaires et de leurs conséquences funestes. La plus célèbre des dystopies en résultant reste, encore aujourd'hui, la fiction de Georges Orwell, *1984*.[70] Ceci explique et légitime la réaction des français lors de la présentation du fichier SAFARI. Le Monde titrait, le 21 mars 1974, : « Safari, ou la chasse aux français » — celui-ci aurait permis, par une centralisation des données personnelles, d'attribuer un identifiant à chaque citoyen, pour accéder à toutes les administrations et les institutions étatiques.

De nombreuses organisations manifestèrent de concert avec la population pour rejeter le projet et, face à cette détermination, le premier Ministre Pierre Messmer commanda un rapport à Bernard Tricot, secrétaire général de la présidence de la République, afin d'étudier la question. Parmi les propositions que contenait ce dernier, il en est une notoire qui n'a pas perdu de son utilité : la création d'une autorité de contrôle. Une proposition de loi plus que visionnaire l'instituera, aboutissant à la loi du 6 janvier 1978 et à la création de la CNIL, la Commission nationale pour l'informatique et les libertés.

Les débats parlementaires de 1977 témoignent déjà d'une ouverture d'esprit et d'une capacité d'anticipation spectaculaire, au vu de l'utilisation pourtant encore limitée du numérique par le grand public. Jean Foyer, président de la Commission et rapporteur, envisageait déjà les difficultés à appréhender certains fichiers de données, tels que ceux des « organes de presse et des agences de publicité », ou les fichiers privés non recensés par l'État. Sa vision était très claire : l'informatique n'a pas créé le recensement des données, car après tout, « le *liber status animarum* prévu par le concile de Trente n'était-il déjà pas un fichier ? ».[71]

---

[68] ROCHELANDET (F.), *ibid.*

[69] GUITON (A.), « Le scandaleux logiciel espion vendu pour "savoir si son fils est gay" », *Libération*, 22 août 2017, article en ligne.

[70] ABOUT (I.), DENIS (V.), *op. cit.*, p. 94.

[71] *Déb. parl.* AN (CR), 4 oct. 1977, 1ère séance, 1977, p. 5782.

Il a simplement contribué à améliorer les performances de collecte et de traitement de l'information.

En étant plus efficaces, il était à prévoir que ces méthodes finiraient par révéler des dangers, déjà perçus à l'époque. « 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 ? Traits fâcheux déjà lorsque les données stockées par l'ordinateur sont exactes mais combien plus graves encore quand elles sont erronées ! » [72]

Ainsi étaient posés, dans la loi, le point de départ de la réglementation des données personnelles, de leur définition, de leur champ d'application, et des prérogatives de la CNIL. L'article premier de la loi établit d'ailleurs avec force les intentions de ses créateurs : « « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Encore aujourd'hui, malgré les successifs remodelages législatifs, ces affirmations trouvent à s'appliquer. L'asservissement du citoyen et de son identité à la technologie est un écueil que beaucoup de scientifiques, d'ingénieurs, de techno-sceptiques et de citoyens redoutent. La maîtrise sur les données personnelles est donc devenue un réel enjeu juridique et social.

La loi du 6 janvier 1978 ayant déjà envisagé la question sous tous ses aspects, elle n'eut besoin de transposer la directive européenne de 1995[73] que plus tardivement. Cette directive, exception faite de quelques recommandations en 1980 par l'OCDE — l'Organisation de coopération et de développement économique, un groupement de 35 pays travaillant en collaboration — et de la Convention 108 du Conseil de l'Europe[74], sera le premier texte européen à entrer en vigueur, presque vingt ans après la loi Informatique et Libertés.

C'est une loi du 6 août 2004 qui viendra mettre en conformité le droit français, tout en précisant que la France était « l'un des premiers États européens à se doter d'une législation globale de protection des données à caractère personnel ». Trois exigences étaient visées : intégrer le texte européen au droit français, tirer un bilan de l'efficacité de la loi de 1978 depuis son entrée en vigueur, et maintenir un niveau de protection constant aux citoyens.[75] En outre,

---

[72] *Déb. parl.* AN (CR), *op. cit.*

[73] Dir. 95/46/CE, 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la circulation de ces données.

[74] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, 28 jan. 1981.

[75] Loi n° 2004-801, 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, Dossiers législatifs – Exposé des motifs.

en mai 2018, c'est désormais le règlement européen[76] qui entrera en vigueur et qui sera donc applicable de plein droit, sans que ne soient nécessaires de mesures de transposition.

Ces textes ont donc servi à consacrer un droit à la protection des données personnelles, et tendent, avec la multiplication des atteintes causées à ces dernières, à un droit sur les données personnelles. Nouveau pontet de la protection identitaire, il se manifeste au travers de nouvelles prérogatives, consacrées notamment dans le règlement européen : le droit d'accès consacré par l'article 15 permet d'obtenir confirmation auprès du responsable de traitement que des données sont bien entre ces mains, le droit de rectification de l'article 16 permet de modifier des informations erronées, et le droit à l'effacement de l'article 17 qui, bien que controversé, permet d'obtenir la déréférencement de certaines contenus en ligne.

Il est fondamental de comprendre que toutes ces certifications n'auraient aucune raison d'être si les données personnelles n'étaient pas le moteur des nouvelles technologies. Il est, certes, souvent fait au droit le reproche d'être constamment en retard sur les avancées techniques, mais cela semble pourtant logique — bien qu'il soit possible d'anticiper, personne ne saurait prédire avec exactitude les effets désastreux d'une invention à venir. En ce sens, beaucoup prônent une adaptation, voire une mutation, des droits déjà existants.

Le Conseil d'État a d'ailleurs étudié la question dans son rapport annuel de 2014, considérant qu'une articulation pertinente de nos normes existantes devait se faire en parallèle d'un développement constant des techniques — celles-ci imposant d'être plus exigeants sur la mise en balance de la vie privée et de la liberté d'information par exemple.[77] Les facilitations engendrées par la cohabitation de technologies intuitives et de la connectivité ont souvent un revers juridique, mis de côté par l'enthousiasme populaire qui les accueille.

Ainsi, l'accès quasi-instantané, et gratuit, à des œuvres cinématographiques sur des sites illégaux de streaming fait oublier aux consommateurs qu'ils nuisent gravement aux droits d'auteurs de l'équipe artistique. L'engouement causé par les taxis autonomes de Google, normalement opérationnels dans le courant de cette année à Phoenix, en Arizona, fait occulter le risque encore trop élevé d'accidents, et l'enregistrement des données personnelles qui serait possible par leur utilisation — la récurrence et le détail des trajets, par exemple.[78]

La Haute juridiction française considère qu'il n'est pas nécessaire de créer de nouveaux droits fondamentaux, ou de tenter d'en dresser une liste exhaustive. Selon elle, une adaptation seule est nécessaire, après avoir entendu cadrer le potentiel du numérique sans en subir les effets pervers.[79] En réalité, le « Big Data » ne se résume pas à l'explosion du nombre de données, mais à leur utilisation - généralement commerciale. Mais la rentabilité des données n'est pas

---

[76] Règ. (UE) 2016/679, 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, abrogeant la directive 95/46/CE.

[77] Conseil d'État, *op. cit.,* p. 37.

[78] ESCANDE (P.), « Les taxis autonomes de Google sur la grille de départ », *Le Monde Économie*, 20 déc. 2017, article en ligne.

[79] Conseil d'État, *op. cit.,* p. 39.

qu'économique, elle permet aussi de répondre à la fonction première de l'internet envisagée par la loi du 6 janvier 1978 : être un service pour les utilisateurs.

Ainsi, le Massachussetts Institute of Technology lance le *Billion Prices Project*, un calculateur d'indices économiques en fonction de données, choisies précisément : le prix des biens. Par l'utilisation d'algorithmes, l'équipe du MIT parvient à prédire les tendances économiques avant certains experts. Pour éviter que les progrès permis par l'utilisation des données personnelles ne tombent dans les travers trop capitalistiques des entreprises les moins scrupuleuses, il est plus que nécessaire que la protection de celles-ci évolue, vers un renforcement. Malgré tout, il existe déjà de nombreuses prérogatives allouées aux individus, qui ont les moyens législatifs de se défendre contre l'exploitation abusive des données personnelles.

Paragraphe 2. La consécration des droits sur les données personnelles

La loi du 6 janvier 1978 est le texte fondateur protégeant les données personnelles, qui impose aux responsables de traitement ou de collecte de ces dernières de respecter un certain nombre d'obligations. Ces jalons, posés par la loi française, seront repris dans le règlement européen, tant ils sont conformes aux exigences de sauvegarde de la vie privée. Ainsi, l'article 6 de la loi prévoit que la collecte d'informations personnelles doit être « loyale », et répondre à des finalités déterminées, sans qu'elles ne soient réutilisées ultérieurement sans une autorisation renouvelée. Cela va de pair avec l'obligation d'information prévue par l'article 32, contraignant le responsable à dévoiler la finalité du traitement, son identité, ou encore la nature des données utilisées.[80]

La Cour de Cassation est attentive à ce que ces principes soient respectés. Déjà, en 2006, elle venait condamner un particulier pour avoir récolté les adresses e-mails de consommateurs potentiels, par l'installation frauduleuse d'un logiciel sur leurs ordinateurs — à des fins, naturellement, d'envoi de messages publicitaires. Elle considérait que « constitue une collecte de données nominatives le fait d'identifier des adresses électroniques et de les utiliser », et qu'est « déloyal le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition ».[81]

[80] COSTES (L.), et MARCELLIN (S.) [dir.], *Lamy Droit du numérique (Guide)*, 2009, p. 4786.

[81] C. Cass., Ch. cr., 14 mars 2006, n° 05-83.423.

Le principe de finalité est également garanti par les hautes juridictions, qui exigent d'un responsable de traitement que les légitimations de celui-ci soient clairement exposées avant une quelconque collecte. Le Conseil d'État validait ainsi une décision de refus d'autorisation de la CNIL à une centrale bancaire, aux motifs que celle-ci ne fournissait pas aux clients une information totale et éclairée suffisante à ce que leur consentement soit éclairé, et qui ne légitimait nullement la conservation des données pour une durée de trois ans. Il n'y avait en outre aucune garantie concernant la réutilisation des informations bancaires pour une exploitation différente, ce que le juge administratif avait sanctionné.[82] L'appréciation de la légitimité du traitement est donc une des conditions de « l'effectivité de la protection des données personnelles ».[83]

En sus des obligations incombant aux responsables de traitement, la loi a également doté les individus de prérogatives quant à la protection de leurs données. La première est le droit d'information, évoqué ci-dessus, mais elle n'est pas la seule. Un droit d'accès est délivré aux personnes physiques « justifiant de leur identité », donnant possibilité de réclamer à un responsable de traitement des informations sur l'utilisation et la finalité des données, la légitimation du traitement, ou tout simplement en vue d'obtenir une copie de l'ensemble des informations détenues par l'entreprise. Ce droit est garanti par l'article 39 de la loi du 6 janvier 1978.

Enfin, l'article 40 du même texte dispose que, sous la même condition de justification identitaire, les personnes concernées peuvent « exiger du responsable de traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées », si celles-ci venaient à être « inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ». Ainsi, le Conseil d'État a déjà pu admettre dans une décision de 2008 que le droit d'accès et de rectification au motif d'une « homonymie alléguée » était justifié, alors même qu'il s'agissait de services des renseignements généraux, dans la mesure où la communication des informations concernées ne portait nullement atteinte à l'objet de ces services.[84]

La loi a également ajouté un volet particulier à la protection des données personnelles, intégrée dans une section précise du Code pénal, « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques ». Ainsi, les articles 226-16 à 226-24 prévoient les sanctions assorties au non-respect des obligations posées par la loi du 6 janvier 1978, qui restent malgré tout plus une technique de dissuasion qu'une réelle arme législative.[85]

---

[82] CE., 10ème et 9ème sec., 30 déc. 2009, n°306173, *Leb*.

[83] VIVANT (M.) [dir.], « Un principe de finalité », *Lamy Droit du numérique*, 2017, p. 563.

[84] CE., 10ème et 9ème sec., 21 mai 2008, n°301178, *Leb*.

[85] DAOUD (E.), TROUVÉ (M.), et CHAUVIÈRE (E.), « Libertés fondamentales et protection des données personnelles », *Lamy dr. aff.*, n°87, 1er nov. 2013, p. 87.

Ainsi, l'établissement d'un traitement de données personnelles ne respectant pas les conditions prévues par la CNIL est « puni de cinq ans d'emprisonnement et de 300.000€ d'amende ».[86]

Il existe en complément de ce droit commun une protection externe aux données personnelles, propres à certains domaines d'activités. Ainsi, le Code de la santé publique envisage des garanties spécifiques et renforcées quant aux données de santé. L'article L.1110- 4 du Code dispose bien que « toute personne prise en charge par un professionnel de santé […] a droit au respect de sa vie privée et au secret des informations la concernant », impliquant de la part des professionnels médicaux une vigilance toute particulière quant à la mise en place de systèmes de collecte sécurisants. Leur commercialisation est interdite.[87]

Enfin, un nouveau droit fonde de nombreux espoirs quant à son importance future dans la lutte pour la protection des données personnelles : l'autodétermination informationnelle. Ce droit, inscrit de manière détournée dans l'article premier de la loi du 6 janvier 1978, donne la possibilité aux individus de choisir dans quelle mesure ils souhaitent communiquer leurs données et ce, totalement librement. Ce principe avait été dégagé par la Cour constitutionnelle fédérale allemande, dans un arrêt du 15 décembre 1983.[88] Initialement, c'est une loi sur le recensement qui avait été censurée par la juridiction, s'appuyant sur le cas d'espèce pour dégager ce principe au nom de la vie privée garantie par la Constitution allemande.[89]

Ce principe d'autodétermination informationnelle ne figure pas explicitement dans la loi française de protection des données personnelles, mais son esprit habite l'article premier, qui dispose que l'informatique est un service pour les citoyens, et non un moyen d'asservissement. Cette formulation permet de légitimer une garantie générale à toutes les prérogatives prévues par la loi, garantie hiérarchiquement supérieure à celles-ci, et légitimant que le citoyen fasse un usage libre et éclairé de ses données personnelles.

En outre, désormais, avec la nécessité croissante de protection, de nouveaux contenus entrent en jeu sous couvert des données personnelles. C'est le cas de l'adresse IP, qui est désormais une donnée personnelle en ce qu'elle permet non pas d'identifier une personne, mais d'obtenir ses données de connexion par le biais du fournisseur d'accès, notamment lorsqu'elle commet une infraction. Il est donc possible de recouper indirectement une identité. Cette inclusion de l'adresse IP dans la protection législative ne contrevient pas aux textes, mais témoigne d'une acception non exhaustive de la notion des données personnelles.[90]

---

[86] Art. 226-16, Code pénal.

[87] CNIL, fiche thématique, « Qu'est-ce qu'une donnée de santé ? », article en ligne.

[88] VIVANT (M.) [dir.], « Le principe d'un contrôle sur les données traitées », *Lamy droit du numérique*, 2017, p. 580.

[89] KAPLAN (D.)., *Informatique et libertés 2.0*, éd. FYP., 2010, p. 68.

[90] PÉRONNE (G.), « L'adresse IP est bien une donnée à caractère personnel », obs. sous CJUE, n° C-582/14, 19 oct. 2016, Patrick Breyer c. Bundesrepublik Deutschland et C. Cass., 1ère Ch. civ., n°15-22.595, 3 nov. 2016, *Dalloz IP/IT*, 2017, pp. 120-123.

Les données personnelles sont donc multiples, et l'intégration de nouveaux éléments dans cette notion est à prévoir, au regard des évolutions sociétales — puisque de nouvelles informations naissent sans cesse, permettant de dévoiler les caractéristiques des individus. À terme, tout ce qui constitue potentiellement un indice sur l'identité d'une personne pourrait devenir une donnée personnelle : la fréquence cardiaque, l'odeur, la voix, le visage — la reconnaissance faciale étant déjà utilisée par certaines entreprises, telle qu'Apple, qui a commercialisé récemment un smartphone se déverrouillant grâce à ce procédé.

Leur protection doit donc être solide et étoffée, et à l'heure de l'entrée en vigueur du RGPD, des modifications législatives françaises sont à prévoir, car malgré l'importance accordée par la loi à ces données, de trop nombreuses emprises, extérieures à l'État, ont la main mise sur celles-ci.

Titre second – La réification de l'identité numérique

Selon le courant utilitariste, les biens répondent simplement à des fonctions triviales pour les hommes : il s'agit de tout objet constituant la richesse de l'individu, grâce à sa mise à profit.[91] À l'énoncé de cette définition, les éléments constitutifs de l'identité numérique peuvent être considérés en tant que des biens. Dans la société numérisée, la donnée personnelle prend toute son utilité dans sa commercialisation par des entreprises extérieures. Son rendement économique permet aux individus d'avoir accès à des services « gratuits », bien que le terme soit controversé au regard des déséquilibres conséquents entre les entreprises et les consommateurs : l'inscription aux réseaux sociaux n'est que très rarement payante, tout comme l'accès aux services mobiles de GPS, ou encore l'accès aux sites de e-commerce.

Au sein de l'environnement numérique s'est développé un marché économique spécial, celui de la donnée personnelle, actuellement au cœur des tergiversations juridiques. Le combat parfois acharné que se livrent les entreprises pour obtenir les données personnelles témoigne bien d'une volonté d'appropriation. Cette recherche de puissance révèle que, malgré l'absence de qualification juridique, la donnée personnelle est considérée — du moins par les acteurs privés du numérique — comme un bien, susceptible d'être appropriée afin d'en dégager des bénéfices commerciaux.

Pour en améliorer le rendement, les responsables de traitement des données personnelles utilisent des supports particuliers, tels que les algorithmes. Logiciels de collecte, de reconnaissance identitaire, de classification, assistants vocaux, moteurs de recherche, *nudges* : bien qu'invisibles à l'œil nu, il est désormais difficile de naviguer sur internet sans avoir affaire à ces intelligences artificielles — ce qui n'est pas sans poser de problèmes, dans la mesure où leur existence récente entraîne des imperfections chroniques, parfois tant importantes qu'elles en bousculent l'ordre du droit.

Très performants, ces algorithmes sont devenus les bras droits des entreprises, dont la rémunération et le fonctionnement sont basés sur la collecte des données personnelles, à tel point que certains demeurent jalousement gardés par leurs détenteurs. Malgré les explications données par le moteur de recherche Google sur les nombreux algorithmes qui aident au fonctionnement de son immense base de données et au référencement naturel, ou optimisé, des contenus qu'elle agrège, il est difficile de savoir sur quelles bases se fixent le choix de favoriser un lien plutôt qu'un autre. Les algorithmes sont devenus un puissant support de commercialisation des données, à tel point qu'elle en est parfois excessive, au détriment des droits et des libertés garanties aux consommateurs et aux individus.

[91] REBOUL-MAUPIN (N.), *Droit des biens*, 6ème éd., Dalloz, Hypercours, p. 10.

Chapitre 1. L'algorithmisation croissante de l'identité numérique

L'émergence des algorithmes est souvent associée au XX^{ème} siècle, de par leur lien puissant à l'informatique et aux ordinateurs — pourtant, la notion est connue depuis l'Antiquité, en ce qu'elle est une équation, résolue après plusieurs étapes, et produisant un résultat utile à celui l'ayant impulsé. En revanche, la technologie numérique a propulsé leur développement, tant ceux-ci sont désormais perfectionnés, nécessitant toujours plus de puissance et plus de capacité à traiter les données en masse.[92]

Envisagés comme des logiciels perfectionnés et spécialisés dans le traitement des données, les algorithmes permettent un classement et une étude toujours plus poussée de celles-ci, devenant indispensables au bon fonctionnement d'un service en ligne ou d'une application mobile. Initialement utilisés pour apprendre les caractéristiques d'un individu — recueillir ses goûts, ses préférences, ses habitudes, afin de lui proposer des publicités adaptées —, ils peuvent aussi devenir des influences pour le consommateur.

La pratique très critiquée des *nudges* en est un bon exemple. Ces « incitations vertueuses » sont en réalité des algorithmes capables de pousser un individu vers un comportement plutôt qu'un autre. Ils peuvent prendre la forme de publicités incitatives prônant une économie d'argent, ou la favorisation d'un choix jugé plus sensé par l'apparition d'un bouton plus attrayant.[93] Extrapolant légèrement à la manière de la science-fiction, il pourrait s'agir d'une fourchette connectée qui émettrait un signal lorsqu'un individu diabétique atteindrait son taux de calories maximal.[94]

De manière globale, la présence d'algorithmes dans la société conduit nécessairement à ce qu'ils entrent en contact avec l'identité, afin de l'appréhender ou de la contrôler — quel que soit l'objectif dissimulé, cette banalisation est rentrée dans les mœurs, puisque peu de protestations sociales s'élèvent contre cette pratique, malgré les dangers qu'elle révèle en filigrane.

---

[92] HERNET (P.), *Les algorithmes*, 2002/2928, 2ème éd., PUF, pp. 5-6.

[93] DUBUC (D.), « Les nudges : incitations vertueuses ou flicage invisible ? », *Usbek & Rica*, 10 oct. 2017, article en ligne.

[94] Anonyme, « HapiFORK, la fourchette qui vous dit comment manger », *Les Échos*, 12 avr. 2013, article en ligne.

Section 1. La banalisation de l'utilisation des algorithmes

Depuis le début de l'utilisation massive de la technologie, que l'on peut estimer raisonnablement entre les années 1980 et 2000, l'exploitation des données par les algorithmes n'a fait qu'accroître. Cette pratique s'est pourtant accompagnée d'un effet pervers — ces intelligences étant si discrètes que leur développement n'a pas pour autant engagé une meilleure connaissance de ceux-ci par les individus. Aujourd'hui encore, la population n'est pas suffisamment sensibilisée aux dangers que peuvent représenter ces logiciels, que certains voient comme des nouveaux régulateurs sociaux.

Les algorithmes prédictifs, qui engrangent le plus de connaissances possibles sur un individu afin de lui proposer des contenus, sont tant focalisés sur l'individu qu'ils ne sont pas créés pour favoriser la pluralité des messages. Ainsi, une étude démontre que 40% des utilisateurs de Facebook sont conscients qu'ils ne voient pas tous les contenus postés par leurs amis.[95] Cette dictature du numérique est pourtant sciemment acceptée de tous.

Au contact des données personnelles et des identités des personnes, les dangers sous-jacents ne peuvent que sauter aux yeux, et pourtant, il n'est pas encore de prise de parole collective afin qu'un contrôle juridique soit récupéré sur ces logiciels. Le paroxysme de cette banalisation est d'ailleurs atteint au sein des projets de *smart cities*, ces quartiers ou ces villes entièrement connectées, qui tendent initialement à améliorer la qualité de vie urbaine, mais fonctionnent sur un échange permanent de données personnelles et non-personnelles. Google envisage d'ailleurs de construire un nouveau quartier de Toronto, complètement connecté.[96]

Le problème essentiel qui se pose, juridiquement, dans le développement massif de ces algorithmes, est qu'ils fonctionnent sur la collecte et l'analyse des données personnelles, créant parfois des atteintes aux personnes, et engendrant des litiges complexes à résoudre au vu du silence textuel en la matière.

---

[95] LEBRET (M.), « Notre manque de connaissances des algorithmes nous nuit », *Slate*, 24 mars 2015, article en ligne.

[96] HOURCADE (B.), « Une filiale de Google construit un quartier entier à Toronto », *Usbek & Rica*, 21 oct. 2017, article en ligne.

Paragraphe 1. L'alliance du droit et de l'intelligence artificielle

La reconnaissance identitaire a changé de support au fil du temps et des connaissances techniques. D'abord effectuée entre les pairs par leur mémoire et leur vue, elle s'est ensuite progressivement figée sur le papier, par les actes d'authentification, l'état civil, et les photos. Cette reconnaissance, d'abord effectuée par la main de l'homme, s'externalise depuis l'apparition des technologies. Derrière la reconnaissance faciale ou digitale se cachent des machines, des logiciels et des algorithmes. Un basculement s'est opéré entre un support logistique supervisé par l'homme, à des moyens d'identification facilitant les habitudes du quotidien mais qui nous échappent de plus en plus. Désormais un lien anthropologique unit la machine et l'homme, les rendant indissociables.[97]

Mais que sont réellement ces algorithmes ? Quelle réalité se cache derrière ce terme savant, et quelles en sont les implications juridiques, en lien avec les données personnelles et l'identité de l'individu ? Pour le comprendre, il est nécessaire de se pencher sur le fonctionnement de ceux que l'on appelle, parfois à tort, parfois à raison, des intelligences artificielles. Sur un panel de 1001 personnes interrogées, 83% ont déjà entendu parler des algorithmes mais 52% ne savent pas de quoi il s'agit. Et même si la majorité semble consciente qu'il ne s'agit que de réflexions mécaniques, 47% pensent qu'ils sont plutôt fiables et 43% qu'ils proposent plus de choix aux individus grâce à une meilleure connaissance de leurs comportements et de leurs pratiques.[98] Cette affirmation est, en outre, bien erronée, puisque l'accumulation de données sur les utilisateurs permet de leur proposer des contenus très, voir trop, ciblés, nuisant de fait au pluralisme.

En réalité, les algorithmes ont une importance considérable dans nos vies, à tel point que certains considèrent que « nous sommes devenus de la chair à algorithmes, victimes de la plus formidable extorsion de valeur des temps modernes ».[99] Ils pourraient même être entendus, à terme, comme une nouvelle source de droit, tant leur puissance est grande, et tant les entreprises qui s'en servent ont obtenu un statut social.[100]

Lorsque le cerveau humain se heurte à un problème, les connexions neuronales cherchent ensemble comment le résoudre et aboutissent à une solution. Qu'elle soit juste ou erronée, le procédé qui a conduit l'élève à celle-ci peut s'apparenter à un algorithme. La fonction première de ces calculateurs artificiels est de trouver la réponse la plus adaptée à une équation, qu'elles qu'en soient ses variables. Pour cela, il est doté par l'homme d'une base de

---

[97] RODOTA (S.), *ibid.*

[98] *Notoriété et attentes vis-à-vis des algorithmes*, Sondage IFOP pour la CNIL, jan. 2017.

[99] KOENIG (G.), « Nous ne voulons pas être de la chair à algorithme ! », *Les Échos*, 27 jan. 2016, article en ligne.

[100] BARRAUD (B.), « Le coup de data permanent : la loi des algorithmes », *RDLF*, chron. n°35, 2017, pp. 4-7.

données sur laquelle s'appuyer, et de mécanismes techniques cherchant à lui insuffler une procédure de réflexion.

Les algorithmes ne sont que des tentatives de dédoublement de la réflexion humaine. La raison en est une volonté de facilitation de la réflexion dans de nombreux cas où l'homme pourrait perdre son temps et son énergie face à un problème aisé, potentiellement solvable par une machine. C'est le cas notamment des Legaltechs, ces logiciels armés d'algorithmes juridiques, qui permettent seulement — pour l'instant — de calculer le montant d'une indemnité ou d'une pension alimentaire, ou de résoudre des litiges peu complexes.

Les algorithmes sont au cœur des problématiques actuelles liant données personnelles et nouvelles technologies. Le sujet de l'intelligence artificielle, en 2017, a été évoqué 200 fois dans les articles du Monde.[101] De nombreuses capacités leur sont désormais dévolues.[102] Un algorithme est tout à fait capable d'identifier un visage, puisque désormais les smartphones Apple se déverrouillent de la sorte. Il s'agissait là d'un véritable défi technique, puisque la reconnaissance du visage se fait via une base de données normalement stockée sur des serveurs étrangers, ce qui est ici contenu en une simple puce du smartphone.

Ces intelligences permettent également de créer des œuvres, puisqu'il existe des logiciels de création musicale assistée par ordinateur, tels que Avia ou Flow Machines, mais également de jouer à des jeux. En témoigne la célèbre intelligence AlphaGo de Google, capable de battre le champion sud-coréen de ce jeu chinois, et qui n'a trouvé de maître assez puissant pour la terrasser que sa version 2.0.[103]

Mais il n'est pas que de futiles fonctions aux algorithmes, qui aident désormais à la neuroscience, promettant parfois des solutions utopiques, mais dont l'utilité est indéniable. L'entreprise Kernel, fondée par Bryan Johnson, cherche par exemple à développer des outils de compréhension du cerveau humain afin de créer des applications de traitement des pathologies mentales. Injectée de 100 millions de dollars par son fondateur, en 2016, la société travaille sur la possibilité d'une puce intégrée au cerveau afin d'en faire une interface et de pouvoir communiquer avec. Le projet, encore utopique, s'explique selon lui par un puissant désir d'améliorer la vie des autres.[104]

Toutes ces évolutions ne vont pas, malheureusement, pouvoir s'intégrer si facilement dans une société française juridique, tant elles peuvent parfois engendrer des litiges, la donnée personnelle étant au cœur du fonctionnement des algorithmes.

---

[101] TUAL (M.), et LAROUSSERIE (D.), p.1, *in* Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

[102] D. (L.), pp. 2-3, *in* Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

[103] Anonyme, « AlphaGo a trouvé son maître : sa version 2.0 », *Sciences et Avenir avec AFP*, 19 oct. 2017, article en ligne.

[104] text. « an "overwheelming desire to improve lives of others" », NIENTUS (Z.), « Humans 2.0 : meet the entrepreneur who wants to put a chip in your brain », *The Guardian*, 14 déc. 2017, article en ligne.

Il ne faut pas non plus négliger l'importance des assistants artificiels, tels que Cortana sur Microsoft, ou Siri sur Apple, désormais capables de dialoguer avec nous et de trouver la solution à nos problèmes basiques. Algorithmes et chatbots, quel que soit le nom qu'ils prennent, sont désormais présents dans nos vies, et de manière bien plus conséquente que nous ne le pensons. Mais il y a une chose qu'il est impératif de ne pas occulter : leur fonctionnement se fait majoritairement par l'utilisation de nos données — personnelles ou non. Ce qui permet aux algorithmes de Google de faire de la publicité ciblée ? Les données que laissent les utilisateurs derrière eux : leurs préférences commerciales, leurs historiques d'achats, leurs orientations sociales et tant d'autres. Or cela pose des problèmes tant juridiques qu'éthiques, ce que le droit englobe également.

Paragraphe 2. La donnée personnelle, moteur des algorithmes

L'exemple de la neuroscience vient étayer la thèse selon laquelle l'utilisation des algorithmes vient heurter le droit en vigueur. L'objectif de Bryan Johnson est d'aider la médecine — nul doute n'est permis sur la louabilité du projet. Mais l'implantation d'une puce cérébrale n'est pas sans poser des questions juridiques parmi les plus délicates. En admettant que le projet se concrétise — ce que le créateur estime réalisable d'ici une quinzaine d'années —, il serait impératif qu'il respecte, en France, le Code de la santé publique, qui dispose que « le consentement de la personne examinée ou soignée doit être recherché dans tous les cas ».[105]

Le Code civil, quant à lui, dispose qu'il « ne peut être porté atteinte à l'intégrité du corps humain qu'en cas de nécessité médicale pour la personne ou à titre exceptionnel dans l'intérêt thérapeutique d'autrui ». À moins de prouver la nécessité d'un tel procédé pour l'intérêt général, il serait impensable de passer outre le consentement des patients.

Qui plus est, deux autres problèmes majeurs se dessinent. Considérer le cerveau comme une interface, avec une puce intégrée dans celui-ci, implique nécessairement des procédés de récolte des informations. Les données médicales sont considérées comme des informations personnelles, puisque le règlement européen les définit en tant que données « 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 ».[106]

[105] Art. R41-27-36, Code de la santé publique.

[106] Art. 4, Règlement européen à la protection des données.

Or l'idée d'une telle puce cérébrale est précisément de collecter des informations dans les cerveaux de personnes aux troubles mentaux, afin d'en tirer des moyens de guérison — il s'agit précisément du cadre des données personnelles. *Quid* alors de la protection de ces données ?

La puce cérébrale ne serait finalement qu'un objet connecté de plus, se devant de respecter les législations nationales de protection des données personnelles, d'autant que le législateur fait face à une expansion du domaine d'application de celles-ci. La Cour de Justice de l'Union Européenne a effectivement reconnu, en 2016, qu'une adresse IP est bien une donnée personnelle au sens de la loi européenne. Le requérant, las de constater que les services administratifs allemands conservaient systématiquement l'adresse IP qui lui était dévolue, attaquait l'État afin que celui-ci cesse cette pratique, considérant qu'il y avait là une information suffisante pour l'identifier.

La Cour lui donnait raison, jugeant « qu'une adresse IP dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de [la directive 95/46/CE], lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires » en possession du fournisseur.[107] Qui plus est, cette consécration arrivait peu de temps après que la Cour de Cassation en ait tiré des conclusions similaires en France.[108]

En poussant la réflexion encore plus loin, se pose la question des éventuels litiges nés à propos des décisions des algorithmes. De nombreux juristes ont déjà évoqué le problème à venir en traitant de la responsabilité de ces machines. Prenons l'exemple de la start-up Case Law Analytics, développée par deux avocats et juristes, Jérôme Dupré et Jacques Lévy Véhel. Le logiciel permet de soumettre à un juge virtuel une affaire portant sur du droit civil ou du droit commercial, en se basant sur un formulaire de questions — qui sont majoritairement des données personnelles ou à tout le moins potentiellement recoupables. À partir de ces résultats, il est apte à calculer le montant estimé d'une prestation complémentaire ou de proposer aux parties une procédure amiable. Le but initial est de désengorger les tribunaux pour des petites affaires pouvant être réglées hors des voies judiciaires.[109]

---

[107] CJUE, 2ème Ch., C-582/14, 19 oct. 2016, Patrick Breyer c. Bundesrepublick Deutschland.

[108] Cass. 1ère Ch. civ., n°15-22.595, 3 nov. 2016, *in* PAUTROT (B.), « Adresse IP : victoire du relativisme sur les dogmatismes quant à la qualification de données à caractère personnel », *RLDI*, n°134, 1er fév. 2017, com. de CJUE, 2ème Ch., C-582/14, 19 oct. 2016, Patrick Breyer c. Bundesrepublick Deutschland.

[109] EUDES (Y.), p. 5, Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

Bien qu'il ne s'agisse pour l'instant que d'un support d'aide dépourvu de toute autorité de chose jugée, face aux ambitions de certains pays[110] et aux progrès de la science, le logiciel pourrait devenir à terme un juge à part entière. Qu'adviendrait-il alors si l'algorithme venait à rendre un verdict injuste, voir illégal ? Serait-il possible de faire appel ou de se pourvoir en Cassation pour la décision d'un robot ?

Certains auteurs ont déjà évoqué le problème que poseraient les algorithmes en termes de responsabilité, tout en commençant par les identifier juridiquement. Ils peuvent être scindés en deux catégories : les algorithmes d'automatisation, qui répondent à une simple procédure exécutive, et les algorithmes d'apprentissage, qui développent une forme d'intelligence autonome basée sur le *machine learning*.[111]

Pour les premiers, un système de responsabilité simple existe déjà. Il est en effet possible d'invoquer la responsabilité traditionnelle du fait personnel, prévue par l'article 1240 du Code civil, qui dispose que « tout fait quelconque de l'homme, qui cause un dommage à autrui, oblige celui par la faute duquel il est arrivé à la réparer ». Cette obligation viserait le constructeur de l'algorithme, à qui reviendrait la charge de prouver l'absence de faute — et cette responsabilité pourrait se manifester, par exemple, dans un préjudice causé par l'insertion d'une base de données erronée.

En revanche, pour les seconds, le système est plus complexe. Il est impossible d'appliquer une responsabilité du fait des animaux, car une machine n'est pas un être vivant — et il l'est tout autant de doter les machines d'une personnalité morale, à l'instar des sociétés, puisqu'elles ne sont que des objets autonomes technologiquement. Il pourrait être envisageable de créer une responsabilité « du fait de l'autonomie décisionnelle » de l'algorithme, à la charge de son concepteur d'en supporter les éventuelles indemnisations.[112]

Cette théorie montre bien que les algorithmes et leurs potentiels effets ne sont pas encore intégrés dans le droit de la responsabilité — pour le moment, il s'agit d'appliquer ce qui, dans les textes, pourraient le plus s'en rapprocher, mais le manque de législation adaptée se fera vite ressentir. D'aucuns préconisent déjà un réel droit des robots.[113] Quoi qu'il en soit, leur banalisation ne se fait pas sans l'apparition de dangers juridiques bien réels, qu'il appert nécessaire de réguler.

---

[110] BARRAUD (B.), « Un algorithme capable de prédire les décisions des juges : vers une robotisation de la justice ? », *Les Cahiers de la justice*, 2017, pp.121-139.

[111] GODEFROY (L.), « Les algorithmes : quel statut juridique pour quelles responsabilités ? », *Comm. com. élec.*, n°11, nov. 2017, p. 18.

[112] GODEFROY (L.), *op.cit.,* p.20.

[113] NEUER (L.), « Alain Bensoussan : "Il faut construire un droit spécifique aux robots" », *Le Point*, 20 nov. 2017, article en ligne.

Section 2. Les dangers de l'utilisation des algorithmes

En reprenant l'exemple de la *smart city*, les principaux risques liés aux algorithmes apparaissent clairement. La création d'un environnement entièrement basé sur la connaissance des individus, où une seule entité — un acteur majeur du numérique, sans nul doute — serait détentrice des données, aboutirait à créer un micro-état dans lequel les lois en vigueur ne seraient qu'une coquille vide. Cette affirmation est loin d'être dénuée de toute preuve, puisque certaines entreprises se sont déjà exprimées sur le sujet.

Larry Page, l'un des fondateurs de Google, s'exprimait en mai 2014 sur la question, considérant qu'il serait judicieux pour une entreprise comme la sienne de posséder un territoire hors de portée des lois afin de mener à bien des expérimentations nouvelles, rendues pour le moment impossible à raison des législations existantes. Une proposition avait même été émise pour faire de la Silicon Valley, le berceau des entreprises montantes dans les nouvelles technologies, un État à part entière — qui seraient les gouvernants ? Nul besoin d'y réfléchir outre mesure.[114]

Bien que cette thèse semble pour l'instant bien futuriste, l'idée générale est, quant à elle, bien réelle. L'utilisation des algorithmes dans les processus de reconnaissance identitaire, dans les services numériques, ou même dans l'influence de l'identité numérique, pourrait à terme s'affranchir des règles juridiques en la matière.

Bien qu'à l'aune du règlement européen, les principaux acteurs semblent réellement vouloir se conforter aux législations, la question des algorithmes, de leur partialité, et de leur efficacité, n'est nullement abordée par les textes. Un long travail sociétal reste à effectuer afin que le droit ne se trouve pas affecté par ces intelligences artificielles omniprésentes.

[114] NORA (D.), « Micro-États, villes flottantes : le projet fou des nouveaux maîtres du monde », *Nouvel Obs*, 13 avr. 2014, article en ligne.

Paragraphe 1. La partialité des algorithmes

Les avantages des algorithmes sont appréciés et appréciables, d'autant plus dans le domaine juridique — et pour cause, ils permettraient d'avoir des jugements plus neutres. En effet, certaines études démontrent que, dans certains systèmes, certains préjugés sont encore solidement ancrés dans les mœurs et déséquilibrent les verdicts que peuvent rendre les juges. Une chronique de l'ONU démontrait, en 2007, que dans certaines communes des États-Unis, la discrimination raciale persistait de manière plutôt radicale — elle s'appuyait à l'époque sur l'affaire Mychal Bell, qui avait fait grand débat aux États-Unis, suiteà la condamnation douteuse d'un jeune américain noir.[115]

Ces évènements pourraient voir leur nombre diminué grâce aux algorithmes, qui, théoriquement, ne doivent pas opérer de telles discriminations. Ainsi, la directrice de l'Institut National des hautes études de la sécurité et de la justice, Hélène Cazaux-Charles, reconnaît qu'il sera nécessaire de s'habituer à l'intelligence artificielle dans les procédures judiciaires. Elle permettrait en effet d'éviter des dérives de la sorte, mais également accélérer les décisions dans certains cas peu problématiques, tels que les arrestations pour conduite en état d'ivresse.[116]

Ces constatations révèlent malgré tout un paradoxe : l'algorithme peut apporter plus de partialité — puisqu'il ne prendra pas en compte le physique, l'âge, ou les caractéristiques physiques telles que les tatouages —, mais il tendrait parfois à en manquer, puisque les données peuvent être biaisées.[117] Une intelligence artificielle, jury d'un concours de beauté en 2016, éliminait tous les candidats de couleur noire. Des chercheurs de Stanford ont, quant à eux, créé un programme capable de déceler l'homosexualité sur un visage — sur des critères non scientifiques sinon douteux.[118] Les exemples en la matière sont pléthore.

---

[115] Anonyme, « La discrimination raciale et le système juridique aux États-Unis : les leçons récentes de la Louisiane », Chronique de l'ONU, *Le magazine des Nations Unies*, vol. XLIV, n°3, sept. 2007, *et* COJEAN (A.), « Mychal Bell, rescapé de la justice sudiste », *Le Monde*, 1er oct. 2007, article en ligne.

[116] EUDES (Y.), p. 5, Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*.

[117] DOWEK (G.), p7, Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*.

[118] TUAL (M.), et LAROUSSERIE (D.), p. 2, Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*.

En témoigne également Northpointe, un logiciel calculateur de risque de récidive, dont disposent désormais les juges de Floride, devenu un précieux support dans les rendus de décision.[119] Il attribue, en fonction des éléments du dossier, une note de danger de récidive sur une échelle de 1 à 10.[120] L'intention était louable, et pourtant, le logiciel a engendré une polémique de taille aux États-Unis : la base de données étant biaisée, les résultats qu'il rendait étaient discriminatoires. Une étude a ainsi démontré qu'une personne de couleur noire ayant commis un délit juvénile se voyait attribuer un risque de récidive bien plus élevé qu'une personne de couleur blanche, déjà condamnée pour plusieurs braquages.

Les résultats étaient sans appel : la première n'avait pas récidivé, alors que la seconde, oui. L'ensemble de ces constatations n'a, hélas, rien d'étonnant dans la mesure où elles démontrent des conceptions des sociétés contemporaines, puisque l'algorithme n'invente rien — dès lors que sa base de données est guidée spécifiquement, ses décisions ou ses créations seront nécessairement orientées.[121]

Un rapport confié au député Cédric Villani, sur la demande du premier Ministre Édouard Philippe, rendu en mars 2018, apporte un éclairage sur la question. Selon lui, la solution serait d'enrichir les bases de données auxquelles les algorithmes ont accès afin que ceux-ci aient plus de points de comparaison et ne soient pas induits en erreur vers de fausses solutions. Concrètement, cela impliquerait plus d'accès aux données qu'il n'est déjà possible de le faire, par la légitimation de la publicité de certaines informations ou par une ouverture plus grande des bases de données existantes — alors que les réglementations européennes et françaises se battent actuellement pour renforcer leur protection.

Il s'agit d'un paradoxe bien étrange que de vouloir ouvrir les bases de données aux algorithmes qui n'avaient pour vocation que l'optimisation du traitement de ces dernières. Malgré tout, le rapport préconise également la création d'une institution de contrôle afin de faire respecter une certaine éthique au sein des processeurs des intelligences artificielles.[122] Quelques jours après la parution du rapport, le Président français Emmanuel Macron annonçait que ce réseau prendrait la forme de plusieurs institutions répandues sur le territoire national, et que l'amélioration des bases de données algorithmiques se feraient sur base de dons citoyens. Quant à l'amélioration des conditions de développement de ces logiciels, un débloquement de

[119] LEVENSON (C.), « Un logiciel censé prédire le risque de récidive aux États-Unis a un problème de racisme », *Slate*, 24 mai 2016, article en ligne.

[120] 1 étant un risque faible, 10 le risque maximal.

[121] ANGWIN (J.), LARSON (J.), MATTU (S.), et KIRCHNER (L.), « Machine Bias », *ProPublica*,23 mai 2016, étude en ligne.

[122] FAGOT (V.), et TUAL (M.), « Intelligence artificielle : ce qu'il faut retenir du rapport de Cédric Villani », *Le Monde*, 28 mars 2018, article en ligne.

fonds et la création de chaires seront mis en œuvre afin d'attirer les « jeunes talents » dans ce domaine spécial mais si innovant.[123]

L'ouverture des bases de données peut, qui plus est, constituer un véritable défi juridique, comme en témoigne l'accès public aux décisions de justice, permis par la loi du 7 octobre 2016, qui dispose que « les décisions rendues par les juridictions judiciaires sont mises à la disposition du public à titre gratuit dans le respect de la vie privée des personnes concernées ».[124] Sans se prononcer sur la légitimité du projet, une opération d'une telle envergure nécessitera bien évidemment la mise en place de garanties pour la vie privée, ce qui peut s'annoncer compliqué, dès lors qu'il est déjà malaisé de protéger les données existantes.[125]

En outre, l'utilisation des algorithmes dans ce que beaucoup appellent la « justice prédictive » pourrait avoir également des conséquences néfastes. Avoir accès aux fameuses *legaltechs*, ces bases de données juridiques, pourrait influencer les juges dans leur office. En présence de données statistiques, qui exposeraient par exemple le nombre de cas similaires à l'espèce et les décisions des juges précédents, l'avocat pourrait totalement influencer sa plaidoirie en se basant sur de simples mathématiques.

Or le droit est une science à part entière qui ne peut ignorer une partie d'intuition humaine et de contextualisation. Cette utilisation des données est biaisée, car elle ne prend en compte que des éléments purement scientifiques, et ne s'intéresse nullement aux circonstances de l'affaire, qui sont propres, elles, à influencer le juge. « Si la justice est toujours représentée les yeux bandés, n'est-ce pas pour lui éviter de consulter les bases de données qui pourraient influencer son jugement ? »[126]

En outre, d'un point de vue plus juridique qu'éthique, qu'arriverait-il si l'algorithme, dans son état actuel, était piraté ? Si un employeur venait à refuser un poste à une personne dont le risque de récidive est estimé à 8 par Northpointe, par exemple, que pourrait-elle faire contre cette décision injuste ? Il s'agit, encore une fois, d'un problème de responsabilité qui n'est pas solvable pour le moment.

---

[123] GEORGES (B.), « Macron annonce 1,5 milliards d'euros pour développer l'intelligence artificielle », *Les Échos*, 29 mars 2018, article en ligne.

[124] Art. 21, loi n°2016-1321 du 7 octobre 2016 pour une République numérique.

[125] BUAT-MÉNARD (E.), et GIAMBIASI (P.), « La mémoire numérique des décisions judiciaires », *D.*, 2017, pp. 1483-1489.

[126] DONDERO (B.), « La justice prédictive : la fin de l'aléa judiciaire ? », *D.*, 2017, pp. 532-538.

Paragraphe 2. La responsabilisation nécessaire de l'utilisation des algorithmes

L'impartialité des algorithmes n'est pas le seul risque inhérent à l'utilisation des algorithmes. En Californie, les forces de polices travaillent désormais avec le logiciel PredPol, qui guide les équipes vers des zones potentiellement risquées, en leur indiquant sur un plan des zones sensibles — le système fonctionne en corrélation avec Street View, l'application de cartographie de Google. La base de données qui fait vivre cette intelligence artificielle comprend l'ensemble des fichiers de police recueillis sur une décennie, ainsi que tous les rapports postérieurs à sa création, enregistrés automatiquement dès leur rédaction. Selon l'un de ses fondateurs, Jeffrey Brantingham, le fonctionnement du logiciel est similaire aux sismographes qu'utilisent les scientifiques.

Basés sur la première secousse, qu'ils ne pouvaient pas anticiper, les logiciels calculent et déduisent les futurs tremblements. PredPol serait donc incapable de détecter les premières infractions, et indiquerait simplement les zones potentielles de récidive criminelle. À terme, les zones indiquées pourraient être constamment les mêmes, faisant passer les forces de l'ordre à côté d'autres troubles, pour avoir suivi les avis d'un logiciel statistique.[127]

En outre, et bien que cette réflexion puisse paraître légèrement futuriste, les algorithmes de la sorte supposent un passage à l'acte qui n'a pas encore eu lieu. Aucun outil ne permet encore de détecter les intentions avant la réalisation d'un acte criminel, mais les nouvelles technologies progressant avec force, il ne serait pas exclu qu'un jour, cela ne soit une réalité. Quelle serait la réaction à adopter face à un individu ayant été tenté de commettre une infraction, mais qui ne serait jamais passé à l'action ? L'article 121-5 du Code Pénal dispose que l'infraction est « constituée dès lors que, manifestée par un commencement d'exécution, elle n'a été suspendue ou n'a manqué son effet qu'en raison de circonstances indépendantes de la volonté de son auteur ».

L'infraction ne saurait être qualifiée à partir de la seule intention — c'est le cumul de la volonté criminelle et de la réalisation de l'acte qui permet une incrimination. Or, le déclenchement d'un tel acte dépend de facteurs sociaux, émotionnels, matériels, humains, mais surtout d'une intention humaine qu'aucun système ne pourrait appréhender.

« Verra-t-on un jour la police débarquer au domicile de toutes les personnes dont il est probable qu'elles commettront un jour un méfait ? Cela signifierait que, après la vie privée, le libre arbitre a disparu lui aussi — c'est-à-dire le libre choix de chacun, jusqu'au bout, de commettre ou non un acte un instant envisagé ».[128]

---

[127] EUDES (Y.), « PredPol, le Big Data au service de la police », *Le Monde*, 22 avr. 2015, article en ligne.

[128] KERDELLANT (C.), *Dans la Google du loup*, Plon, 2017, p. 56.

Les algorithmes, les données personnelles qu'ils en extraient, et la vie privée, sont trois notions qui sont aujourd'hui inséparables car au cœur de nombreux problèmes — finalement, l'écueil avec de telles intelligences en puissance est l'utilisation qui en est faite. Après les attentats de 2015, en France, la SNCF annonçait sa volonté d'expérimenter un programme de reconnaissance faciale dans les gares, à partir des caméras de surveillance, afin d'anticiper de tels évènements par la détection de troubles comportementaux — une hausse de la température, des signes d'anxiété. Ici encore, l'intention est louable, mais « couplé à des technologies de reconnaissance faciale, ce type de système pourrait permettre de détecter en direct une personne abandonnant un colis suspect. Mais aussi un militant pour les droits de l'homme dans une dictature… ». [129]

Les systèmes existant se rapprochent lentement de cette dystopie — la Chine a installé 170 millions de caméras dans les rues de ses villes, et en prévoit 600 millions d'ici 2020. Lors d'une expérience gouvernementale réalisée avec un journaliste, la reconnaissance faciale l'a identifié comme suspect en moins de sept minutes et a envoyé une brigade policière instantanément. L'installation vise également à punir les mauvais comportements citoyens, tels qu'un piéton qui traverserait au feu rouge. [130] Il est ainsi aisément facile d'imaginer les potentialités d'atteintes aux droits des individus et d'inculpations abusives rendues possibles par la multiplication de telles technologies — sans évoquer la conception particulière de la vie privée ici mise en avant.

Ce panel des potentielles dérives de l'utilisation algorithmique illustre les nombreux obstacles juridiques qui pourraient émerger des suites du couplage de ces intelligences avec la collecte des données personnelles. Bien que certaines craintes ne soient pour l'instant utopiques, la technologie ne cesse de surprendre et de nouvelles évolutions éclosent quotidiennement. Le droit a encore beaucoup à apprendre de ces intelligences — tant lorsqu'ils sont des supports que des problèmes à encadrer. Les législations en termes de responsabilité ne sont pas encore adaptées à ces nouvelles technologies.

L'utilité de ces logiciels n'est plus à prouver et leur but initial d'optimisation des conditions de vie n'est un secret pour personne — le réel problème est l'utilisation qui en est faite. Toute technologie est un atout dans la mesure où elle est exploitée avec raison — la machine ne devant pas prendre le pas sur l'homme. Si l'algorithme développe un système de réflexion propre, alors il est à craindre que même les ingénieurs qui l'ont créé ne le comprennent pas et n'en puissent légitimer aucune décision.

---

[129] TUAL (M.), et LAROUSSERIE (D.), p. 2, Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*.

[130] TRUJILLO (E.), « En Chine, le grand bond en avant de la reconnaissance faciale », *Le Figaro*, 13 déc. 2017, article en ligne.

Cela s'est en outre déjà produit, puisque deux intelligences artificielles de Google, Alice et Bob, programmées pour s'envoyer des messages cryptés, se sont créées leur propre langage crypté, après avoir été hackées par un troisième logiciel, Ève.[131] Ce langage avait complètement dérouté les ingénieurs, incapables de le déchiffrer.

Finalement, l'utilisation de tels outils nécessite une bonne appréhension des données personnelles et une compréhension des dérives potentielles par les utilisateurs qui en génèrent, couplées à un maniement raisonnable et proportionnel à un objectif précis. Ces deux objectifs demanderont du temps et de la patience de la part des gouvernés et des gouvernants, car la sensibilisation sociétale et l'apaisement de l'engouement qui entoure parfois le maniement de tels supports émergeront doucement.

De soucieux entrepreneurs ont d'ores et déjà œuvré en quête de solutions contre les dangers de ces intelligences artificielles — c'est le cas d'Elon Musk, patron de Tesla, qui finance à hauteur de plusieurs millions de dollars des organismes scientifiques travaillant en ce sens.[132] Il avait d'ailleurs déjà signé, avec une centaine de chefs d'entreprise travaillant au contact des algorithmes, une lettre ouverte afin de dénoncer les dangers de ces intelligences dans le domaine des armes, et tout particulièrement dans le cas des robots tueurs.[133]

Tout un travail de conscientisation juridique et éthique reste à mettre en place pour que les algorithmes deviennent des outils et non des freins à nos libertés fondamentales, telles que notamment la vie privée. La loi du 6 janvier 1978 disposait déjà, dans ses termes visionnaires, que « l'informatique doit être au service de chaque citoyen », ne devant « porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».[134]

Cette vigilance se devra d'être accrue face à une tendance plus que difficile à contrer : la commercialisation des données personnelles résultant de leur surexploitation, notamment par les géants du numérique. Ce second problème entraîne lui aussi de nombreuses dérives qu'il est parfois délicat d'endiguer juridiquement.

---

[131] MOUREN (L.), « Des intelligences artificielles ont créé un langage pour communiquer entre elles », *L'Express*, 8 oct. 2016, article en ligne.

[132] Anonyme, « Les 37 projets d'Elon Musk contre les dangers de l'intelligence artificielle », Pixels, *Le Monde*, 6 juil. 2015, article en ligne.

[133] « An open letter to the United Nations Convention on certain conventional weapons », lettre ouverte, *Future Institute of Life*, lettre disponible en ligne.

[134] Art. 1, loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Chapitre 2. La commercialisation abusive des éléments de l'identité numérique

Tout le paradoxe — et l'intérêt — de la commercialisation de l'identité numérique est qu'elle est issue de l'individu, et devrait donc être sensément rattachée à eux par un procédé juridique ; or « la numérisation est à la racine d'un écosystème qui place l'utilisateur – tout individu connecté – au centre du dispositif ».[135] Autour de cette simple affirmation se cristallisent toutes les problématiques juridiques ayant trait à l'exploitation des données personnelles : il est nécessaire de protéger les droits et les libertés fondamentales qui se rattachent à l'individu, et pourtant cela passe par la régulation de données personnelles qui sont, pour le moment, considérées comme des biens par leurs exploitants.

Tous les plus grands acteurs du numérique — notamment les GAFA — ont surfé sur la vague du Big Data et se sont appuyés sur le déferlement de connectivité qu'ont connu les individus. C'est en réalisant que les individus se connectaient en masse sur internet et utilisaient de plus en plus ses services qu'ils ont développé leurs produits — qu'il s'agisse d'ordinateurs, de réseaux sociaux, ou d'applications. Plus la connectivité a grandi et plus l'accès au numérique s'est démocratisé, plus leurs ventes ont été importantes. Facebook réalisait plus de 27 milliards de dollars de bénéfices de chiffre d'affaires en 2016, et au vu du nombre d'objets connectés, que l'on estime à vingt milliards en 2020, ces revenus ne sont pas en voie d'extinction.[136]

L'opposition entre les commerciaux, les individus, et les États, a créé un triangle relationnel où des problématiques juridiques se sont dessinées à chaque niveau — les premiers cherchant un profit perpétuel, parfois au détriment des libertés que les individus cherchent à protéger, soutenus par les gouvernants en quête de leur souveraineté éraflée. Une confrontation permanente est née avec les grands acteurs privés, qui ont tant de pouvoir et de puissance économique que celle-ci en devient influente juridiquement. En outre, les données personnelles deviennent l'objet d'un marché économique, ce que l'État français ne légitime pas, bien que factuellement, elles soient déjà considérées comme des biens de haute valeur.

[135] GUYADER (A.), « Les enjeux du grand bouleversement », *Pouvoirs*, 2018/1, n°164, éd. Le Seuil, p. 7.

[136] GUYADER (A.), *ibid.*

Section 1. L'influence juridique des détenteurs privés des données personnelles

L'industrie développée autour des données personnelle et des individus s'est imposée par l'intelligence de son modèle. Les services proposés par les GAFA se sont d'abord rendus indispensables, et ce grâce à peu de choses — Steve Jobs a créé un ordinateur qui est aujourd'hui l'objet d'une plébiscité massive, les créateurs de Google ont commencé à travailler dans un garage et n'indexaient que quelques contenus, et Facebook est né d'un projet universitaire sans que son créateur n'ait aucune idée de son ampleur à venir.

Pour autant, ils sont désormais au cœur des pratiques quotidiennes de millions de personnes. En outre, ce modèle économique s'est appuyé, à raison, sur les données personnelles, puisqu'à considérer qu'elles sont des biens, elles sont non rivales : leur exploitation ne les fait pas disparaître.[137]

Une fois cette assise anthropologique et économique installée, les obstacles qu'ont rencontré ces entreprises avec le droit se sont vus minimisés. Une société sans aucune importance pour un État ne peut clairement tenter de tourner le vent en sa faveur — il a été plus dur pour les gouvernements de s'attaquer aux problèmes juridiques causés par les GAFA, pour cette raison. Malgré une volonté croissante de les soumettre aux législations en vigueur, volonté soutenue par l'opinion publique, il reste encore difficile d'encadrer à la perfection toutes leurs pratiques, tant le fichage des données est devenu une habitude.

Paragraphe 1. Du fichage social au fichage commercial

La collecte des données est extrêmement révélatrice du contexte politique d'un État — il suffit de regarder l'histoire pour s'en convaincre. Les Romains, dans l'Antiquité, ne recensaient pas les femmes, celles-ci n'étant pas considérées comme des citoyens. En période de guerre, et notamment au cours des deux conflits mondiaux, toute la population considérée comme ennemi du pouvoir en place était fichée — en 1912, il existait déjà un carnet anthropométrique des nomades. Le régime de Vichy, quant à lui, a instauré le fichier national des cartes d'identité, et le système d'identifiant personnel à 13 chiffres, qui correspond encore de nos jours au numéro de Sécurité sociale. Initialement, son but était le fichage des personnes

[137] ISAAC (H.), « La donnée numérique, bien public ou instrument de profit », *Pouvoirs*, 2018/1, éd. Le Seuil, p. 75.

de confession juive, mais malgré cette première intention criminelle, il demeure aujourd'hui l'un des premiers fichiers existants.[138]

Nonobstant les déviances nées des utilisations de fichiers, nombreux de ceux-ci ont eu une utilité, qu'elle soit culturelle, administrative, historique, ou juridique. Les archives sont, encore de nos jours, l'un des meilleurs moyens de découvrir sa famille ou de comprendre les civilisations précédentes. De nombreux registres, tels que le dictionnaire Maitron — du nom de son créateur — n'ont eu aucune visée commerciale ni implication politique.

En l'occurrence, cet ouvrage se contente de recenser des biographies de personnalités et d'ouvriers engagés dans les mouvements syndicaux depuis 1964, afin d'améliorer la connaissance d'un mouvement en plein essor à cette période.[139] La ville de Bordeaux détient un fichier administratif tenu depuis 1942, réparti entre la police d'État et la commune, qui recense des enquêtes sur les aliénés, les notifications de décès des militaires, ou d'autres études — ce fichier est une mine d'or pour tout sociologue intéressé par le XX^{ème} siècle.[140]

Bien avant l'apparition du numérique existait déjà une préoccupation pour le fichage et le recensement, qui s'explique par un intérêt des gouvernants et des gouvernés à étudier leur histoire et leurs comportements. Le digital n'a en rien révolutionné cette façon de penser mais a contribué à y apporter de nouveaux outils. Ainsi, avec l'apparition du commerce en ligne, et la facilitation des flux et des échanges, les données personnelles sont, elles aussi, devenues un objet de convoitise.

Leur exploitation, notamment par les grandes entreprises de la Silicon Valley, témoigne d'une hyper-mondialisation et d'une connectivité accrue, poussant les industriels à utiliser les données personnelles dans une logique purement capitalistique, parfois au détriment de l'intimité et de la vie privée. D'ailleurs, ne sont-ils pas à l'assaut de l'individu sous toutes ses formes, puisqu'il semblerait que même le sommeil cause aux GAFA des profits amoindris ?[141]

La marchandisation des données personnelles est d'ores et déjà une réalité — les moteurs de recherche sont les premiers à se rémunérer ainsi. En la matière, Google est sous le feu des projecteurs. Certaines sociétés proposent même aux internautes de commercialiser volontairement leurs données contre une rémunération. Ces pratiques sont rentrées progressivement dans les mœurs, et bien qu'une prise de conscience citoyenne semble émerger,

---

[138] Anonyme, « Images, lettres et sons », *Vingtième Siècle, Revue d'histoire*, 2012/2, n° 114, pp. 215-231.

[139] BOULLAND (P.), « Récolte et usages des données personnelles dans les recherches socio-biographiques du Maitron », *La Gazette des archives*, n°215, 2009, résumé du colloque « Archives et coopération européenne : enjeux, projets et perspectives » et « Les données personnelles, entre fichiers nominatifs et jungle Internet ». pp. 161-168.

[140] VATICAN (A.) « Le fichier de la surveillance administrative de la ville de Bordeaux, 1945-1995 », *La Gazette des archives*, n°215, 2009, résumé du colloque « Archives et coopération européenne : enjeux, projets et perspectives » et « Les données personnelles, entre fichiers nominatifs et jungle Internet ». pp. 139-148.

[141] CRARY (J.), 24/7 - *Le capitalisme à l'assaut du sommeil*, La Découverte, mai 2014, 180p.

l'ensemble des dérives possibles ne sont pas encore totalement appréhendées et, de ce fait, craintes par le législateur et le gouvernement.

Les droits français et européen refusent pour autant d'intégrer — et contrôler — cette notion de commercialisation dans les textes, se bornant pour le moment à renforcer la législation existante. Le marché que les acteurs américains ont pu créer autour des données personnelles n'est encadré juridiquement que partiellement, à l'instar de tout autre — et bien que le règlement européen à la protection des données démontre une prise en compte de ces enjeux, le contrôle total sur la commercialisation des données reste au stade embryonnaire. [142]

Serait-ce dû au poids économique et politique des acteurs du numérique ? Ces derniers ont une puissance considérable, allant parfois même jusqu'à influencer les décisions gouvernementales. Le 28 janvier 2017, les propriétaires des plus grandes entreprises de la Silicon Valley, dont Sergueï Brinn — patron de Google —, manifestaient ainsi contre le décret anti-immigration proposé par le président Donald Trump.

Après s'être réunies, les entreprises avaient ainsi convenu, d'un commun accord, d'utiliser la procédure de l'Amicus Brief, permettant à des organismes de « fournir des arguments ou des informations à un juge dans une affaire, sans faire partie des plaignants ». La Maison Blanche, sous le mandat de Barack Obama, recevait régulièrement les dirigeants des GAFA dans des réunions politiques privées, de la même manière qu'il en aurait été pour des chefs d'État étrangers. Le poids de ces institutions est donc massif : elles dégagent de gros bénéfices pour les États, et en ont acquis un levier politique, leur ouvrant une possibilité d'influencer les décisions juridiques.[143]

Paragraphe 2. Le poids juridique des grandes entreprises du numérique

Grâce à leur popularité auprès du public, les entreprises du numérique acquièrent une sorte de pouvoir qui se légitime par l'utilisation massive qui en est faite. Ainsi, certaines entreprises deviennent parfois les juges de la liberté d'expression. Il en est ainsi pour Instagram, célèbre réseau social, qui est désormais censeur de la parole publique — certains mots sont en effet interdits par l'application lorsqu'ils sont apposés à un *hashtag*. C'est le cas du mot « *sex* », et, de manière plus générale, de tous les termes renvoyant à la pornographie.

---

[142] GIUSTI (J.), et NDIAYE (A.), « L'identité numérique, monnaie d'aujourd'hui et rente de demain… », *RLDI*, 1er août 2017, n°140, pp. 56-60.

[143] COSTES (L.), « La Silicon Valley vent debout contre le "MuslimBan" », *RLDI*, n° 134, 1er février 2017, p. 3.

Il en va de même pour la propagande de maladies — notamment l'anorexie — et pour l'apologie du racisme ou de la violence. À priori, il n'appert pas illégitime de bloquer le recensement de ces termes, ayant tous un rapport à des contenus potentiellement choquants ou violents. Mais aucun contrôle juridique n'est assuré sur ces censures, et rien ne garantit que d'autres termes ne soient pas volontairement déréférencés par l'application — en outre, d'autres noms, tels que « *Instagram* » sont interdits, sans qu'aucune explication ne soit donnée.

Doit-on y voir un intérêt économique lié à la protection de la marque ? Quoi qu'il en soit, cette réglementation autonome de la part d'une entreprise privée tend à affaiblir le rôle du juge en la matière.[144] Malgré cela, avec du recul, force est de constater que l'initiative du réseau peut aider à endiguer la diffusion de contenus inadaptés, d'autant que cette plateforme réunit une majorité de mineurs. Il serait peut-être envisageable d'évoluer vers une collaboration entre les forces judiciaires et les dirigeants de telles applications afin que la protection des utilisateurs soit effective factuellement, mais supervisée par une autorité de droit.

Ces grandes entreprises, et majoritairement les GAFA, considèrent le consommateur comme « un objet, et non un sujet de droit » : il est au cœur du ciblage, puisque toutes les informations collectées sur lui permettent de dégager des bénéfices. Tous les enjeux économiques reposent sur lui.[145] Mais cette vision capitaliste de l'humain engendre parfois des dérives que le système juridique ne semble pas parvenir à endiguer. À trop vouloir contrôler les données qu'ils ont entre les mains, les géants du numérique semblent parfois occulter les obligations légales leur incombant. Des conflits éclatent en la matière, puisque les entreprises privées et les institutions étatiques n'ont parfois pas la même conception de la légitimité d'une norme.

Ce fut le cas dans l'affaire opposant le FBI à la société Apple. La firme américaine avait été mise en demeure, le 16 février 2016, par la Cour californienne, de « développer une version *ad hoc* d'iOS, le système d'exploitation de l'iPhone, pour permettre aux enquêteurs de tester un grand nombre de mots de passe ». Les forces de police tentaient par ce biais d'accéder au contenu du smartphone d'un terroriste. Apple refusait catégoriquement de s'exécuter, estimant devoir protéger le respect des données personnelles de ses utilisateurs, et ce sans condition ni exception. Le FBI ayant finalement réussi à y accéder sans l'aide de la société, celle-ci avait abandonné les poursuites, mais la porte est restée entrouverte à d'autres cas d'espèce.

Une question reste alors en suspens : peut-on légalement obliger une société à délivrer, directement ou non, des données sur ses utilisateurs ?[146] Le règlement européen à la protection des données personnelles précise bien, dans la délimitation de son champ d'application matériel, qu'il exclut les traitements de données « par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou

---

[144] Anonyme, « #NO #SEX – Les mots clefs interdits par Instagram », *Le Monde*, 3 sept. 2013, article en ligne.

[145] LANDREAU (I.), « Pour une approche éthique de la valorisation des données du citoyen », *RLDI*, n° 124, 1er mars 2016, pp. 33-36.

[146] COSTES (L.), « Apple vs FBI : confidentialité vs sécurité… », *RLDI*, n°125, 1er avril 2016, p. 3.

d'exécution de sanctions pénales, y compris la protection contre des menaces à la sécurité publique et la prévention de telles menaces.[147] En outre, l'article 23 du même texte ajoute des possibilités de limitations par les États aux protections dévolues aux utilisateurs — telles que le droit d'accès ou le droit de rectification, mais également la nécessité du consentement —, limitations qui doivent respecter « l'essence des libertés et droits fondamentaux » et la « société démocratique ».

Elles sont acceptées dès lors qu'elles ont trait à « la sécurité nationale, la défense nationale, la sécurité publique ». Il est à prévoir que, selon les pays, le régime de limitations comportera des divergences, laissant à penser que certains États seront plus stricts sur la communication de ces données que d'autres. Dans le cadre de l'Union Européenne, il est fort plausible qu'une situation telle qu'a connu les États-Unis ne pourrait se reproduire — mais il reste encore le problème de la territorialité puisqu'en matière de données personnelles, la puissance américaine a sa propre législation.

Cet exemple illustre un paradoxe poignant : ces entreprises se servent des données de leurs utilisateurs pour dégager des bénéfices qui leur reviennent directement, mais refusent de collaborer avec la justice. Cet égoïsme d'exploitation des données personnelles qui, en outre, fait obstruction à des enquêtes judiciaires, s'explique par la chasse au profit à tout prix — et en ce sens, capter l'attention de l'individu devient un véritable marché. La publicité est constante et avec l'apparition des nouvelles technologies de l'information, il est difficile de lui échapper. Il est même possible désormais d'acheter un produit directement par le biais d'un QR code affiché sur une publicité.[148]

Le marché de l'attention, tel qu'on pourrait le nommer, s'est créé et se renforce au quotidien. « Au niveau de l'offre, l'objectif peut être de transformer celui dont on a capté l'attention en acheteur. »[149] Ce but s'atteint plus aisément par le traitement des données personnelles — mieux le consommateur est connu, et plus il est aisé de lui proposer des biens ou des services lui correspondant. Ces intrusions répétées dans les goûts personnels pousse parfois les personnes à se protéger de la publicité, par le biais de bloqueurs, de souscription à des listes noires, ou simplement en refusant de s'inscrire à des listes.

---

[147] Art. 2, Règlement (UE) 2016/679 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.

[148] ORSINI (A.), « Au Japon, une start-up lance le paiement par QR Code », *Numerama*, 11 fév. 2017, article en ligne.

[149] ROCHELANDET (F.), *op. cit.,* pp. 38-66.

L'utilisation des logiciels bloquant la publicité a augmenté de 20% en 2016, témoin de l'agacement citoyen face à de constantes sollicitations.[150] La surexploitation commerciale des données commence à entraîner un recul de cette économie, mais ces réactions sont encore peu nombreuses et leur impact trop faible pour engendrer des pertes pour toutes ces entreprises.

Section 2. La donnée personnelle, un bien potentiel

À mi-chemin entre l'écosystème politico-juridique et le marché économique, le marché des données personnelles est devenue un micro-État, que certains qualifient même de « datacratie », étymologiquement un régime politique où la donnée a le pouvoir. Ces données ne font qu'augmenter, puisque, comme l'avait prédit la loi de Moore, « la quantité de mémoire stockée par pouce sur un disque dur a été multipliée par cinq mille entre 1990 et 2010 ».[151] À capacité de conservation augmentée, multiplication des données et complexification des litiges en résultant.

Comment ne pas considérer comme sérieuse l'éventualité où la donnée personnelle serait un bien, dans la mesure où autour d'elle, s'est créé un marché totalement viable ? L'ensemble des GAFA réalise plus de 300 milliards de dollars de chiffre d'affaires, soit l'équivalent du produit intérieur brut d'un pays de la taille de la Grèce ou du Danemark. En outre, ces entreprises pratiquent une optimisation fiscale telle qu'il semble difficile de penser qu'elles réalisent ces bénéfices sur des personnes, alors qu'il est bien question ici de biens patrimonialisés.[152]

Tout ce processus de commercialisation repose donc sur des pratiques spécifiques liées à la considération de la donnée comme un bien — et ce même en l'absence de confirmation législative et étatique, à tel point qu'est venue émerger une responsabilité de ces acteurs sur ces pratiques, seule riposte que les gouvernements ont pour l'instant réussi à instaurer. Ces abus monétaires enrichissent le débat permanent sur la nature de la donnée personnelle, que la loi française persiste à raison à ne pas reconnaître comme un bien, mais qui est paradoxalement considérée comme telle dans les relations financières.

---

[150] PEZ-PÉRARD (V.), LANDREAU (I.), et LÉGER (L.), « Les aspects socio-économiques et éthiques des données personnelles », Partie 1, p. 36, *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, GénérationLibre, rapport numérisé, janv. 2018, 148p.

[151] GUYADER (A.), « Les enjeux du grand bouleversement », *Pouvoirs*, 2018/1, n°164, éd. Le Seuil, p. 9.

[152] SIMONNET (D.), *Les 100 mots de l'entreprise*, PUF, 2016, p. 77.

Paragraphe 1. L'émergence de pratiques commerciales autour des données personnelles

Un marché des données personnelles s'est donc créé, défiant les règles juridiques existantes, et où les utilisateurs sont devenus une partie du commerce. « You've got data, we've got connections » — ce slogan n'est qu'un exemple de ceux que l'on peut trouver sur le site Datacoup. Partenaire d'organismes très sérieux tels que le MIT, le Time, ou The Economist, ce site permet de se créer un compte personnel où l'utilisateur délivre un certain nombre d'informations afin que leur prix en soit évalué. Si le client l'accepte, il est rémunéré en dollars pour le don et l'analyse de ses données — le site se charge ensuite de les communiquer à diverses entreprises privées.[153]

Un autre exemple illustre à merveille les utilités de la commercialisation des données : il s'agit de la tarification dynamique. Cette méthode consiste à faire varier les prix d'un service ou d'un bien en fonction de divers facteurs, afin d'optimiser les rendements économiques. La pratique est utilisée par des plateformes émergeantes aux services nouveaux : c'est le cas d'Uber, plateforme de mise en relation d'utilisateurs avec des chauffeurs, et dont le nom revient régulièrement dans les doctrines juridiques. En se basant sur les données personnelles des clients — et dans ce cas précis, la demande d'un chauffeur à un lieu et une heure déterminés, ainsi que les informations nominatives et bancaires de la personne — les tarifs du service évoluent.

Lorsque la demande sur une zone concentrée est en forte hausse pendant un créneau horaire, des « majorations tarifaires » apparaissent, afin d'encourager les chauffeurs à se déplacer massivement dans la zone. En satisfaisant la demande, et en assurant une prise en charge rapide des clients, la plateforme réalise une plus-value pour un service normalement *low-cost*, devenu temporairement plus cher que les services de taxi des communes.

Ce système peut être aisément appliqué à tout type de services. AirBnb, la plateforme de location d'appartements, fonctionne sur le même principe. En outre, le danger de cette tarification dynamique est de créer des inégalités entre les consommateurs. Bien qu'intéressante, car créant des services généralement moins onéreux, et donc plébiscités par les consommateurs, cette tarification est néanmoins basée sur un modèle capitaliste. Des dérives pourraient en résulter : quid, par exemple, en cas de refus de prise en charge de personnes ayant été à découvert sur le compte en banque au cours de l'année ?[154]

Le domaine de la santé est également concerné par la délivrance d'avantages aux clients — certains services d'assurances se penchent sur la question. La société Axa s'associait par exemple en 2014 à Withings, une entreprise spécialisée dans les objets connectés, pour

---

[153] ROCHELANDET (F.), *op. cit.*, pp. 38-66.

[154] ROCHELANDET (F.), *op. cit.*, pp. 38-66.

offrir à ses nouveaux adhérents un bracelet capteurs de mouvements.[155] Une fois activé, celui-ci enregistrait l'activité physique de son propriétaire et lui confère des gains en fonction de ses résultats. La société permettait ainsi aux assurés en bonne santé physique ou amateurs de sport de remporter des soins de médecine douce.

Apple envisage également de s'associer à une entreprise américaine, Aetna, spécialisée dans la santé, pour relancer les ventes de l'Apple Watch, sa fameuse montre connectée qui dispose également d'un programme de santé — enregistrement des pas quotidiens, fréquence cardiaque et calories dépensées pendant le sport, ou encore suivi diététique, ne sont que des exemples de ce qu'elle est capable de réaliser.[156]

Loin d'être des cas isolés, cette pratique déjà popularisée aux États-Unis se répand en France, et pour cause : attirer le consommateur avec des avantages est une technique commerciale qui a fait ses preuves.[157] Generali, assureur français, cherche à se lancer également, mais l'entreprise est encore frileuse. Elle se lance en effet dans l'incitation à l'activité physique, en proposant aux entreprises bénéficiaires d'un contrat collectif d'inscrire leurs salariés à un encadrement sportif, sur base de volontariat.[158] Ainsi, elle ne contrevient pas à la loi française prohibant les variations de prix basées sur les questionnaires médicaux dans les contrats collectifs des entreprises, pour leurs salariés.[159] Ses bénéfices seront tirés des contrats des souscripteurs satisfaits.

Il est, de ce fait, un problème juridique qui se dessine en filigrane. L'article 16-5 du Code Civil dispose que « les conventions ayant pour effet de conférer une valeur patrimoniale au corps humain, à ses éléments ou à ses produits sont nulles ». Toute marchandisation du corps humain est donc illicite. Pour le moment, il n'est nullement question pour le juge de reconnaître que les données personnelles sont des objets du corps humain — mais, au vu de l'évolution fulgurante des technologies et de la nécessité d'adaptation législative à laquelle il fait face, cette éventualité n'est pas totalement écartée. Dans ce cas-là, un conflit juridique émergerait. À reconnaître textuellement un droit sur l'identité numérique, pourquoi les données personnelles ne deviendraient-elles pas le prolongement numérique du corps humain matériel ?

Elles entreraient alors dans le champ d'application de l'article 16-5 du Code Civil, ce qui rendrait cette nouvelle pratique totalement illicite. Tout d'abord, elle ne serait pas éthique, car rien ne justifie qu'une personne en bonne santé, adepte du sport et dont l'alimentation est irréprochable, bénéficie d'ajustements considérables sur le prix de son contrat, face à une

---

[155] BEMBARON (E.), « Axa s'associe à Withings dans la santé connectée », *Le Figaro*, 2 juin 2014, article en ligne.

[156] MARIN (J.), « L'assureur américain Aetna prévoit d'offrir 500.000 Apple Watch », *Le Monde*, 12 fév. 2018, article en ligne.

[157] LEQUILLERIER (C.), « L'"ubérisation" de la santé », *Dalloz IP/IT*, 2017, p. 155.

[158] THEVENIN (L.), « Santé : Generali va récompenser les bons comportements », *Les Échos*, 6 sept. 2016, article en ligne.

[159] Art. 4, loi du 31 déc. 1989.

personne inactive ou en surpoids. Ensuite, accepter une tarification individuelle arbitraire, basée sur des habitudes de consommation, elles-mêmes déduites d'une collecte de données personnelles, conduirait à monétiser son identité numérique contre une garantie sociale. Il s'agirait bien d'une convention conférant au corps humain une valeur économique, ce qui est formellement prohibé.

Tout cela, bien sûr, devant se faire dans le respect de la loi du 6 janvier 1978, mais également du Code de la santé publique, qui ajoute une disposition supplémentaire concernant les données de santé, du fait de leur nature particulièrement sensible. Le texte dispose en effet que « toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code a droit au respect de sa vie privée et du secret des informations la concernant ».[160]

Tant qu'il existe encore une frontière entre la valorisation des comportements vertueux et la tarification dynamique qu'il peut en résulter, le danger est à priori contenu. Mais ce simple exemple témoigne bien d'une nécessité d'éclaircir rapidement le statut des données personnelles, afin de mieux réguler le marché des données personnelles.

Enfin, il est à noter que ces plateformes et ces techniques d'attraction du consommateur sont très populaires, alors que ces nouvelles applications entre utilisateurs peuvent totalement nuire à la concurrence. Le problème d'Uber est qu'il a créé un marché entre les consommateurs, basé sur les commentaires que laissent les utilisateurs sur le chauffeur, par exemple. Ce système est basé sur la confiance inter citoyenne, et sur des tarifs bas et attractifs, mais sa communauté peut légitimer les augmentations temporaires, puisqu'elle en connaît les raisons. Elle va ainsi s'étendre et pourrait, à terme, faire émerger un monopole du service sur les autres.[161]

Ces nouveaux services acquièrent une e-réputation auprès de la sphère citoyenne, qui les font également émerger au rang d'indispensables du quotidien, et leur influence est telle qu'il est très facile, à terme, d'occulter qu'ils fonctionnement majoritairement avec les données personnelles de leurs clients.

L'on rentre dans une « interconnexion collaborative », un comportement nouveau qui consiste à ne plus laisser les médias ou l'État régner dans ces domaines, mais à voir apparaître une collaboration et une confiance entre les individus.[162] Mais quelle est alors la place des exploitants des données personnelles ?

---

[160] Art. L1110-4, Code de la santé publique.

[161] MEURIS-GUERRERO (F.), « L'attrait croissant des plateformes numériques », *Comm. com. électr.*, n°9, sept. 2016, p. 52.

[162] MERZEAU (L.), « Habiter l'hypersphère », *Documentaliste-Sciences de l'Information* 2010, vol. 47, pp. 30- 31.

Paragraphe 2. La responsabilité des acteurs du marché des données personnelles

Les nombreuses critiques adressées aux géants du numérique ne semblent pas les effleurer. Leur vision semble même beaucoup différer de celle des législateurs français et européens, notamment sur la notion de vie privée et sur la place du numérique dans une société déjà judiciarisée. Dans un de leurs ouvrages, Éric Schmidt et Jared Cohen, deux des principaux dirigeants de Google, témoignent de « l'importance […] qu'une main humaine conduise l'avènement du nouvel âge numérique, car toutes les possibilités que représentent les technologies de la communication, leur bon ou leur mauvais usage, ne dépendent que des individus ».[163]

Que doit-on y comprendre ? Qu'une entreprise comme Google, que l'on pourrait presque qualifier aujourd'hui d'institution mondiale, tant elle a pris d'ampleur, se contente de mettre à disposition du grand public des nouvelles technologies, se délestant à posteriori de toute responsabilité ? N'est-il pas trop aisé de créer des techniques posant des problèmes juridiques, et d'attendre que les États ou les individus mettent en œuvre des « garde-fous […] pour protéger [leur] vie privée et nous prémunir de la perte de données » ?[164]

Ici réside le cœur d'un problème que tente de résoudre l'Union Européenne depuis quelques années. Avoir conscience de créer des technologies utiles à la société, se démunir de toute responsabilité, et attendre des États que ceux-ci imposent des limites et des réglementations en la matière semble très peu responsable de la part d'acteurs majeurs — d'autant qu'ils sont y sont généralement réfractaires, en témoigne l'affaire Apple évoquée précédemment. Qui plus est, la technologie étant en constante évolution, la cadence législative ne peut nécessairement pas la suivre au plus près.

Ces développements sont pourtant à nuancer, car il est un point sur lequel Éric Schmidt ne manque pas de clairvoyance. « Il est au fond beaucoup plus facile de s'en prendre à un produit ou à une entreprise donnés pour une application néfaste de la technologie que d'accepter les restrictions qu'impose la responsabilité individuelle. »[165]

En réalité, un équilibre est à trouver entre la responsabilité des entreprises et celle des utilisateurs. En effet, il serait totalement hypocrite de se plaindre de la divulgation des données dès lors que l'on n'aurait volontairement pas utilisé les mécanismes de confidentialité déjà prévus — tels que celui de Facebook, qui permet notamment de masquer les messages à un certain public.

Sans se dédouaner totalement, les GAFA doivent apprendre à manager le risque d'atteinte aux droits et libertés fondamentaux de leurs utilisateurs — et clients —, en

---

[163] SCHMIDT (E.), et COHEN (J.), *À nous d'écrire l'avenir*, éd. Denoël, 2013, p. 22.

[164] SCHMIDT (E.), et COHEN (J.*), op. cit.*, p. 28.

[165] SCHMIDT (E.), et COHEN (J.*), op. cit.*, p. 97.

s'intéressant aux problématiques juridiques causés par leurs biens et services, et en proposant des mécanismes de protection adaptés, que les utilisateurs doivent apprendre à utiliser en leur faveur. Hormis ces cas précis, le juge ne serait amené à intervenir qu'en cas de litige.

De facto, la jurisprudence française reconnaît une responsabilité à ces acteurs, et notamment aux moteurs de recherche — Google est, évidemment, le premier concerné. La question s'était déjà posée en 2016, en termes de droit d'auteur, lorsque des syndicats d'artistes et de producteurs l'attaquait, ainsi que Free, Orange, et d'autres fournisseurs d'accès à internet. Ceux-ci demandaient le déréférencement de sites renvoyant à des œuvres disponibles en ligne sans que le consentement préalable des auteurs n'ait été obtenu. L'article L332-6 du Code de la propriété intellectuelle prévoit qu'en cas d'atteinte au droit d'auteur, le Tribunal de grande instance peut ordonner toute mesure en référé de nature à la faire cesser, y compris à l'encontre des personnes en charge du support de cette atteinte.

Dans ce cas d'espèce, l'on cherchait à savoir si les moteurs de recherche, en tant qu'intermédiaires de l'infraction, étaient susceptibles de rentrer dans le champ de cet article. La Cour d'Appel allait dans ce sens, autorisant le déréférencement des sites — mais elle ne poussait pas sa reconnaissance jusqu'à assimiler cette responsabilité à la responsabilité traditionnelle. Le moteur de recherche devient un vecteur de la contrefaçon, mais non un contrefaisant, rendant impossible un engagement total de sa responsabilité, et donc une réparation éventuelle en dommages et intérêts. Cet arrêt illustre bien les problèmes de qualification que posent ces nouveaux acteurs, et il pourrait très bien se produire le même cas de figure lors de l'utilisation des données personnelles.[166]

Conscients de ces risques, les législateurs européens ont donc tenté de mettre en œuvre des moyens juridiques afin de parer à ces dérives. L'article 24 du RGDP a innové, en ce qu'il a placé au sommet des obligations à la charge des responsables de traitement un principe de responsabilité conséquent, tenant en la mise en « œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement ».

Ce principe, usuellement appelé *accountability*, va contraindre les grandes entreprises à effectuer des analyses d'impact et des audits afin de vérifier leur conformité au droit, le règlement préconisant même l'adoption d'un code de bonne conduite. Cette offensive juridique permettra aux législateurs de contrôler le respect du règlement pour les entreprises existantes, et de s'assurer que les entreprises à naître seront responsabilisées avant même leur création.[167]

Il demeure malgré tout un problème de taille : les sanctions peuvent être dissuasives et importantes, mais elles n'empêchent pas une mauvaise utilisation des données avant

---

[166] BRUGUIERE (J-M.), « Un moteur de recherche est bien "une personne" susceptible de remédier aux atteintes aux droits d'auteur et droits voisins sur l'internet », note sous CA Paris, Pôle 5, Ch. 1., n°14/01359, 15 mars 2016, Syndicats APC, FNDF, SEVN, UPF, et SPI c. Orange, SFR, YAHOO ! Darty, Bouygues télécom, Free, Google, Microsoft, Numéricâble, *PI*, 1er juil. 2016, n°60, pp. 344-346.

[167] BOUT (R.) [dir.], « Le principe de responsabilité ou "accountability" », *Lamy Droit économique*, 2018, p. 4570.

l'intervention législative, et, en outre, lors du prononcé d'une sanction financière, si importante soit-elle, elle ne sera qu'une faible partie des bénéfices massifs dégagés par de telles entreprises. Ainsi, lorsque Google était sanctionnée, en 2017, d'une amende de plus de 2 milliards d'euros par la Commission Européenne, pour abus de position dominante, cela représentait seulement 1,6% environ de son chiffre d'affaires annuel.[168]

Se pourrait-il qu'émergent alors des velléités de contournement de la loi, quitte pour les entreprises à hériter d'amendes ponctuelles, finalement peu dérangeantes au regard des bénéfices massifs dégagés par l'exploitation des données personnelles ? La mise en œuvre d'un principe de responsabilité à l'égard de ces acteurs implique tout naturellement qu'une sanction intervienne à posteriori de la commission d'une infraction, et donc de la réalisation du préjudice. Or en la matière, le préjudice cause souvent bien plus de dommages qu'il n'y paraît et il serait sans nul doute bon d'opter pour des solutions axées sur l'interdiction à priori de certaines pratiques — dans l'esprit de l'*accountability*, mais peut-être de manière renforcée.

L'ensemble des problématiques de droit entourant la responsabilité des exploitants des données personnelles témoigne des difficultés d'encadrement. De nouvelles questions émergent, allant bien au-delà de la réflexion sur la nature de la donnée, telles que la teneur de son régime juridique. D'aucuns s'interrogent sur la nécessité d'un renforcement de la législation en vigueur afin que les gouvernements retrouvent une souveraineté totale sur ce domaine — d'autres prônent plutôt une régulation souple émanant des individus.

Cette hésitation est purement logique si l'on s'en tient à la rigueur du droit qui, par la qualification d'un concept, permet de lui rattacher un régime juridique spécifique. Les débats sur la nature de la donnée personnelle engendrent également des débats sur l'encadrement de droit qui lui correspondrait le mieux.

Rattacher la donnée à la notion de bien reviendrait à avoir un idéal plutôt capitaliste que le droit tend pourtant généralement à éviter, et aboutirait à consentir aux puissances du numérique une force sociale et normative qu'elles ne devraient pas avoir. Laisser le contrôle sur les données aux États de manière totale entraînerait nécessairement des incohérences tant le gouvernement manque de connaissances techniques pour englober la matière. Conférer une liberté d'autorégulation aux individus, aptes à gérer des services qu'ils utilisent quotidiennement, diminuerait la souveraineté étatique et bien qu'utile, l'idée n'est réalisable qu'en collaboration avec le gouvernement.

Un équilibre est donc à trouver entre ces conceptions, et plus fondamentalement, entre la régulation et la réglementation des données personnelles. Ces interrogations, loin d'être résolues, seront les premières bornes d'une évolution juridique nécessaire, qu'elle que soit le sens dans lequel elle tendra.

---

[168] DUCOURTIEUX (C.), « L'Union Européenne punit Google d'une amende record de 2,42 milliards d'euros », *Le Monde*, 27 juin 2017, article en ligne.

SECONDE PARTIE. L'IDENTITÉ NUMÉRIQUE, ENTRE RÉGLEMENTATION ET RÉGULATION

Il est des domaines que le droit seul ne saurait efficacement encadrer. La règlementation, concrétisation d'un système juridique créé par le législateur et appliquée par les pouvoirs publics, est le modèle de droit classique — mais dans le droit de la communication et du numérique, cela est impossible. Lui est donc traditionnellement opposée la régulation, une forme d'encadrement plus social, puisque émanant des individus. Cette forme de droit souple se manifeste par l'apparition de comportements des acteurs sociaux en réaction à la réglementation en vigueur — l'ensemble de ces réactions permettent le maintien de celle-ci, en compensant ses failles ou en y ajoutant des spécificités que ne dévoile que la réalité matérielle.

« Notre société semble fonctionner à coup de "réglages" entre les différentes dimensions de la vie sociale, de l'économie, de la politique, de la culture, mais aussi de réglages entre l'intégration et l'exclusion, entre la contribution et la rétribution de chacun : c'est au travers de ces réglages que se construisent les notions de justice et d'équité. »[169]

Autour de l'opposition de ces deux modes d'encadrement se cristallisent des problèmes juridiques d'actualité. La volonté déterminée des États de réglementer de plus en plus autour de l'identité numérique se manifeste clairement par un renforcement des règles existantes — en témoigne l'entrée en vigueur du règlement européen en mai 2018. Malgré cela, les hésitations en la matière entraînent l'apparition d'un nouveau débat : l'instauration d'un droit de propriété sur la donnée, ayant considéré pour cela qu'elle est un bien, susceptible d'appropriation.

Les individus, face à l'omniprésence de ce sujet dans leur vie et la sensibilisation croissante à laquelle ils sont exposés, commencent à prendre conscience des risques liés à l'exploitation de leurs données. *De facto*, une résurgence de volonté de réappropriation des données voit le jour, se manifestant par diverses initiatives citoyennes, qui tendent, elles, à considérer l'identité juridique comme une facette d'un individu, faisant ainsi écho à la protection des droits et des libertés fondamentales.

La notion d'identité juridique et la protection des données personnelles qu'elle implique est l'objet d'un constant balancement, oscillant entre le droit de propriété sur ce que pourraient être ces biens particuliers, et les droits de la personnalité existants qui y sont rattachés par leur nature. Cette hypothèse appert comme la plus légitime — pourtant les partisans de la première ont su avancer des arguments non dénués d'intérêt et de logique juridique. Mais, quelle que soit la solution adoptée, il est indéniable qu'une clarification du statut et du régime de l'identité juridique est souhaitable afin d'en assurer une protection efficace — qu'elle mélange, ou non, la réglementation et la régulation.

---

[169] DE TERSSAC (G.), *La théorie de la régulation sociale de Jean-Daniel Reynaud*, La Découverte, 2003, p. 11.

Titre premier – L'identité juridique, entre droit de propriété et droit de la personnalité

En 1982, le Conseil Constitutionnel reconnaissait que « les principes mêmes énoncés par la Déclaration des droits de l'Homme ont pleine valeur constitutionnelle tant en ce qui concerne le caractère fondamental du droit de propriété, dont la conservation constitue l'un des buts de la société politique et qui est mis au même rang que la liberté, la sûreté et la résistance à l'oppression, qu'en ce qui concerne les garanties données aux titulaires de ce droit et les prérogatives de la puissance publique ».[170]

Le droit de propriété, lien indéfectible entre l'individu et le bien qui lui appartient, est un droit complet, composé de prérogatives — l'*abusus*, l'*usus* et le *fructus* —, aux caractères exclusifs et perpétuels. Ancienne réaction au système féodal français, ces spécifictés très individualistes sont les fruits de la Révolution française, puisque c'est à cette période que ce droit était inscrit pour la première fois dans un texte : la Déclaration des droits de l'Homme et du Citoyen, en son article 17, qui dispose que la propriété est un droit « inviolable et sacré ». Ce n'est qu'en 1804 qu'elle sera reprise dans le Code civil.[171]

L'assimilation de l'identité numérique a un bien sur lequel l'individu aurait une propriété semble à première vue quelque peu extravagant juridiquement parlant — il est en effet question ici d'une relation entre une personne et un bien, or la relation qui unit l'individu à son identité est une relation immatérielle, celui-ci n'ayant aucune emprise matérielle sur celle-ci. Pourtant, le développement de certaines prérogatives plus que matérielles — telles que le droit d'accès ou le droit de rectification prévus par la législation européenne — pourrait porter à croire qu'il s'agit d'une catégorie particulière de biens, tant le parallèle avec les prérogatives du droit de propriété pourrait être démontré.

Malgré cette constatation, des remparts se dressent à cette théorie naissante, dont les premières pierres sont les droits de la personnalité. Ces prérogatives conférées aux individus pourraient tout autant être qualifiées de droits de la personne, tant leur vocation initiale et leur raison d'être est la protection de l'individu. Quel enjeu existe-t-il réellement derrière la protection de l'identité numérique ? Empêcher le dévoilement massif de la vie privée, protéger l'intimité de l'individu dans un monde sur-digitalisé, maintenir une frontière étanche entre la sphère privée et la sphère publique — autant de raisons qui rejoignent le fondement même des droits de la personne. La question de savoir si les droits autour de l'identité numérique sont des prérogatives matérielles ou individuelles permettra de déterminer la nature d'un éventuel régime juridique autour de cette notion.

---

[170] C. Constit., 16 jan. 1982, n°81-132 DC, sur la loi de nationalisation.

[171] REBOUL-MAUPIN (N.), *Droit des biens*, 6ème éd., Dalloz, Hypercours, pp. 207-209.

Chapitre 1. La complexité d'une identité numérique monétisable

Face aux tentatives étatiques de réinstaurer une légitimité sur les données personnelles, certains juristes et scientifiques cherchent des alternatives afin que celles-ci soient mieux gérées. Ainsi, en janvier 2018, le thinkthank GénérationLibre, sous l'impulsion de son fondateur, le philosophe et auteur Gaspard Koenig, publiait un rapport en faveur de la monétisation des données personnelles — relançant ainsi le débat sur leur qualification. Biens meubles, propriétés des individus, ou simples éléments numériques insoumis à une quelconque législation préexistante ? La question est vaste, et entraîne déjà détracteurs et partisans.

Nul doute quant à l'attrait d'une telle initiative : que l'individu récupère la maîtrise sur ses données face aux géants du numérique qui les exploitent allègrement séduit à son énoncé, et correspond parfaitement à la philosophie que Gaspard Koenig nomme la « propriété de soi ». En effet, la gratuité de l'internet empêche l'utilisateur d'en tirer un quelconque bénéfice, puisqu'il est « exclu de la chaîne de la valeur de l'économie numérique et prisonnier du ciblage publicitaire ».

Le but de l'étude était donc de proposer des solutions afin de réintégrer les individus dans cette économie, en faisant payer les exploitants des données personnelles, et en échange, en payant pour la *privacy.*[172] Quelles sont alors les raisons juridiques qui freinent les gouvernants à passer le cap de la monétisation des données personnelles ?

[172] LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, Génération Libre, rapport numérisé, pp. 8-10.

Section 1. La nécessité éthique d'une propriété sur les données personnelles

Selon la définition des biens donnée par Christian Atias, qui en expose une conception utilitariste, les données personnelles sont déjà considérées comme telles, puisqu'elles peuvent totalement rapporter des bénéfices à une ou plusieurs personnes par leur usage — en l'occurrence leurs exploitants —, à ceci près qu'elles n'appartiennent pas à un propriétaire unique, qui concentrerait pour lui les prérogatives juridiques allouées.[173]

La numérisation a positionné ses entreprises vectrices comme des acteurs majeurs de la vie économique, et ce sont généralement celles-ci qui exploitent les données personnelles. Il est très difficile d'échapper à cette connectivité permanente tant elle est usuelle, ce qui contribue parfois à l'affaiblissement de la protection des individus ou des consommateurs. La réification de la donnée personnelle prend en ce sens un fondement éthique, un facteur indéniablement à prendre en compte dans la détermination du régime juridique de l'identité numérique. Ce fondement servirait de base au rééquilibrage des relations entre les citoyens et les grandes entreprises du numérique exploitant leurs données, au sein d'une chaîne de valeur dont ils sont normalement exclus.

L'instantanéité et la gratuité des services numériques sont parfois si porteuses d'engouement qu'il est vite oublié à quel point elles sont rendues possibles par la désagrégation des éléments de notre identité dans une sphère virtuelle. Les responsables de traitement, qui eux, ne l'oublient pas, en tirent souvent des comportements abusifs, contrevenant aux lois en vigueur et bafouant les protections de l'individu. L'instauration d'un droit de propriété sur les données personnelles pourrait être l'un des remparts à ces agissements sociaux condamnables.

[173] ATIAS (C.), *Le droit civil*, 2004/2161, 7ème éd., PUF, pp. 87-102.

Paragraphe 1. Le droit de propriété, rempart aux comportements abusifs des entreprises privées

Partant du principe que lorsqu'un utilisateur accepte les conditions générales d'utilisation d'une application telle que Facebook, ce pacte, que Gaspard Koenig nomme le pacte softien, comporte au minimum cinq clauses abusives.[174]

La première est culturelle : les algorithmes publicitaires prennent en compte les recherches effectuées et n'ouvrent jamais à de nouveaux contenus. « Que devient le monde, si le monde est mon monde ? »[175] L'enfermement culturel est présent dans les réseaux sociaux et dans l'information en ligne, car force est de constater que le numérique nous coupe d'un regard extérieur sur le monde. Les personnes que nous ajoutons sur nos réseaux sont rarement des étrangers — proches, amis, familles, tous ont de près ou de loin les mêmes attraits. Les idées opposées aux nôtres sont peu nombreuses, et il est, qui plus est, possible de les écarter de notre fil d'actualité. Or le pluralisme est déjà protégé par le droit, tant il est important pour la liberté d'expression, dans le domaine de la presse — il pourrait en être totalement de même dans ce cas précis.

La seconde est sociale. Certains acteurs, et ici encore il est possible de prendre l'exemple de Facebook, tentent de poser eux-mêmes des normes comportementales. Ainsi, un enseignant parisien avait vu son profil désactivé par le réseau social pour avoir publié *L'origine du monde*, la célèbre œuvre de Gustave Courbet, représentant une femme nue. Après avoir tenté de le faire réactiver auprès de l'entreprise, et face à un refus total, c'est heureusement grâce à la décision de la Cour d'appel de Pau que celui-ci avait pu gagner contre le réseau social.[176] En effet, Facebook avait déclaré que la juridiction française était incompétente, au vu de l'article 15 de ses conditions générales d'utilisation, qui désignaient l'État de Californie comme juge des litiges potentiels.

C'est en qualifiant la relation unissant l'enseignant au réseau de contrat de consommation, au regard de l'utilisation personnelle qui en avait été faite et des bénéfices commerciaux tirés des publicités pour Facebook, et supposant par ce biais un établissement de la société en France, que les juridictions françaises avaient légitimé leur compétence.[177] Ces grandes sociétés jouent — abusivement — avec leur pouvoir d'influence des masses,

---

[174] KOENIG (G.), Introduction, *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, Génération Libre, rapport numérisé, pp. 14-15.

[175] FINKIELKRAUT (A.), et SORIANO (P.), *Internet, l'inquiétante extase*, Mille et une nuits, 2001, p. 23.

[176] CA Paris, n° 15/08624. 12 fév. 2016.

[177] ANDRÉ (S.), et LALLEMAND (C.), « Facebook contre le consommateur français : l'hallali de la clause attributive », *Dalloz IP/IT*, 2016, pp. 214-215.

choisissant parfois d'influencer la liberté d'expression, ce qui était clairement le cas dans l'affaire Courbet.

Certaines autres pratiques ne sont pas en reste et il semble pour l'instant impossible d'y déroger : Instagram — racheté par Facebook en 2012[178] — pratique notamment le *shadow ban*, le blocage des contenus d'un profil par l'algorithme d'indexation, lorsque celui-ci a utilisé des moyens douteux de promotion pour gagner en popularité. Il serait très néfaste que ces géants du numérique ne finissent par jouer de leur pouvoir massif pour influencer les comportements du quotidien — d'autant qu'ils attirent de plus en plus d'adolescents, voire d'enfants. Une récente étude démontrait en ce sens que 78% des américains entre 18 et 24 ans utilisent majoritairement Snapchat, et 71% d'entre eux ont également de multiples autres plateformes qu'ils consultent au minimum une fois par jour.[179]

La troisième raison est économique. Tout d'abord, l'accès à un service gratuit, légitimé par l'exploitation des données, est un faux avantage, puisque les GAFA extirpent des bénéfices énormes. En 2017, Facebook a augmenté son chiffre d'affaires de 47% par rapport à l'année précédente, soit 40.65 milliards de dollars.[180] Quant à Apple, pour le premier trimestre de l'année 2018, les bénéfices dégagés atteignent 88,3 millions de dollars, soit une augmentation de 13% par rapport à 2017.[181]

La raison suivante est politique, car il pourrait être à craindre que l'utilisation des objets connectés soit imposée par les États, et que le droit à la déconnexion — qui n'existe d'ailleurs pour l'instant qu'en droit social, matérialisé par la possibilité de ne plus consulter les boites mails ou les appareils professionnels au-delà de certains horaires, par exemple — soit menacé. Le compteur Linky et l'obstination gouvernementale de le faire installer pour des raisons économiques et écologiques en est un bon exemple — et cette installation cause beaucoup de débats.

En effet, le remplacement des anciens compteurs vise une facturation réelle de la consommation électrique, par l'envoi des données personnelles des utilisateurs au fournisseur. L'entreprise vise à terme la pose de 35 millions de compteurs.[182] Le problème est que certaines associations de consommateurs, notamment l'UFC Que Choisir, qui publie régulièrement des dossiers afin d'évaluer l'impact réel en termes de santé sur les consommateurs, démontrent que

---

[178] Dépêche AFP et Reuters, « Facebook boucle l'achat d'Instagram », *Le Monde*, 23 août 2012, article en ligne.

[179] SMITH (A.), et ANDERSON (M.), « Social Media Use in 2018 », *Pew Research Center*, 1er mars 2018, étude en ligne.

[180] Dépêche 6Médias, « Facebook : le chiffre d'affaires bondit malgré une baisse du temps d'utilisation », *L'Opinion*, 1er fév. 2018, article en ligne.

[181] Press release, « Apple Reports First Quarter », 1er fév. 2018, rapport en ligne.

[182] LE BILLON (V.), « Compteurs Linky : une bonne affaire pour Enedis », *Les Échos*, 7 fév. 2018, article en ligne.

certaines études témoignent d'un risque d'exposition aux rayonnements électromagnétiques que le compteur dégagerait.

Pour l'instant, aucune preuve scientifique n'a été apportée et l'Agence nationale de sécurité sanitaire a conclu, dans un rapport de juin 2017, qu'il « n'existe aucune donnée suggérant que l'exposition à des courants transitoires à haute fréquence puisse affecter la santé à ces niveaux d'exposition ».[183] Cela n'empêche pas le doute de subsister, et certains élus locaux cherchent à lutter contre ces installations parfois arbitraires. Le maire de Montreuil avait donc fait suspendre l'équipement sur sa commune, mais le Tribunal administratif avait censuré cette décision face à l'absence de risque établi pour la santé des individus.[184]

Les initiatives se multiplient en ce sens. En avril dernier, Corinne Lepage, avocate et ancienne ministre de l'environnement, soutenue par un groupe d'avocats, a demandé aux Ministres de la santé et de la transition écologique et solidaire de suspendre l'installation des compteurs Linky, au nom du principe de précaution, puisque s'il n'est pas exclu qu'ils soient sans danger, l'inverse n'est pas prouvée non plus.[185]

Le cas du compteur Linky, dont l'issue des conflits ne sera révélée qu'avec le temps, n'est qu'un exemple parmi tant d'autres d'une éventuelle dictature des objets connectés — encore que, dans ce cas précis, l'installation de compteurs électriques vise l'amélioration urbaine et s'inscrit dans une perspective écologique. En outre, ce compteur utilise les données personnelles des utilisateurs, et la majeure partie des objets connectés existants et à venir ne feront pas exception à cette règle. La CNIL a d'ailleurs mis en demeure le fournisseur Direct Énergie, pour avoir demandé par trop de données à Enedis, l'exploitant des compteurs, et ce sans le consentement des individus.[186]

Enfin, l'ultime raison, et non des moindres, est juridique. L'acceptation de l'utilisation de nos données personnelles et l'impassibilité devant ce phénomène nous pousse à cautionner une certaine vision de la vie privée qui n'est pas réellement en adéquation avec sa définition textuelle. À force d'accepter, par une inanité ou une impossibilité d'agir, les utilisations qui sont faites de nos données personnelles, une porte est laissée entrebâillée à d'autres dérives. Or, « nos traces numériques, si elles ne servent pas encore à la compilation de score de crédit social

---

[183] Avis de l'ANSES, « Exposition de la population aux champs électromagnétiques émis par les "compteurs communicants", Rapport d'expertise collective, juin 2017, éd. scientifique, version révisée de l'avis de déc. 2015, p. 96.

[184] TA Montreuil, n°1700278,7 déc. 2017, Préfet de la Seine-Saint-Denis, *in* CLÉMENT (J-M.), BOUILLIÉ (A.), et FOURÈS (M.), *BDEI*, n°73, 1er jan. 2018, p. 34.

[185] WAKIM (N.), « Linky : Corinne Lepage et un groupe d'avocats lancent une action collective contre le compteur électrique », *Le Monde*, 11 avr. 2018, article en ligne.

[186] CNIL, Décision n°2018-007, 5 mars 2018, mettant en demeure la société DIRECT ENERGIE.s

des citoyens », sont représentatives de notre identité et des aspects les plus intimes de notre personnalité.[187]

Certaines de ces potentielles dérives sont d'ailleurs en train d'émerger, pour l'instant sous couvert d'utilité citoyenne, en Chine notamment. Ainsi, depuis quelques années, le gouvernement chinois a instauré un système de fichage de la population, en fonction des casiers judiciaires, qui induit pour eux la possibilité ou non de réaliser certaines actions, telles que prendre l'avion en première classe. Les personnes ne s'étant pas conformées à leurs condamnations judiciaires sont interdites d'accès aux transports.

C'est la solution qu'a trouvé le législateur chinois pour lutter contre la mauvaise exécution des décisions de justice. Mais pendant l'installation d'un tel système, certaines personnes aux activités sensibles — avocat, par exemple —, voient parfois leur embarquement refusé à l'aéroport pour des raisons qui leur sont totalement inconnues.[188] Rien ne prouve pour le moment que ce système de liste noire se transformerait en système de notation sociale de l'individu, mais en attendant, il semble inutile de décrire plus en avant les potentielles dérives engendrées par un tel mécanisme.

Face à ce pacte abusif préexistant à la création d'un compte avec un réseau social ou sur une application numérique, la patrimonialisation des données permettrait aux individus de renverser la balance des pouvoirs qui est pour l'instant à l'avantage des entreprises. Mais la réalisation concrète d'un tel projet a des avantages et des inconvénients qui ne sont pas tous envisageables d'un point de vue juridique.

Paragraphe 2. La mise en œuvre concrète de la patrimonialisation des données personnelles

Malgré toutes les initiatives citoyennes déjà engagées, l'hyperpuissance des GAFA semble pour l'instant très peu affectée. Prenons l'exemple de Google : malgré les amendes qui lui ont été enjointes, la concurrence n'est pas très rude. Les petits moteurs de recherche qui tentent de se développer face à ce géant ont beaucoup de mal à maintenir le cap — l'exemple le plus marquant demeure Qwant, l'alternative française, qui connaît beaucoup de problèmes techniques. Google reste en situation monopolistique.[189]

---

[187] PEZ-PÉRARD (V.), LANDREAU (I.), et LÉGER (L.), « Les aspects socio-économiques et éthiques des données personnelles », Partie 1, p. 26., *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, GénérationLibre, jan. 2018, rapport numérisé.

[188] PEDROLETTI (B.), « En Chine, le fichage high-tech des citoyens », *Le Monde*, 11 avr. 2018, article en ligne.

[189] ERTZSCHEID (O.), « L'homme, un document comme les autres », *Hermès, La Revue*, 2009/1, n° 53, pp. 33- 40.

Comment fonctionnerait réellement la monétisation d'une donnée personnelle ? Pour les auteurs du rapport du thinkthank GénérationLibre, le prix d'une donnée est déjà connu puisque les GAFA les commercialise déjà. La CNIL serait placée au centre de cette gestion, soit par la création d'une plateforme qu'elle développerait avec des sociétés de gestion collective, soit par l'instauration d'une autorité indépendante, auprès de laquelle le citoyen consentirait à une exploitation catégorielle de sa donnée dans une finalité et dans un temps déterminés. Ce procédé serait bien évidemment rémunéré, par une chaîne de valeur détaillée, avec des courtiers, et tout ceci se réaliserait par des nanopaiements, en utilisant la technologie des *blockchains* et des *smart contracts*.

Cette authentification très sécurisée permettrait également de respecter la vie privée. La monétisation permettrait de lutter contre ce « pillage en règles » des données par les géants de l'internet — nos données sont collectées parfois à notre insu, le consentement est parfois flou et peu explicite. Le citoyen ne peut jamais négocier les contrats qu'ils passent avec les réseaux sociaux par exemple.[190]

Des études ont démontré, en ce sens, que rares sont les individus intéressés par la lecture des conditions générales d'utilisation, ce dont profitent ces entreprises — d'autant plus que cette lecture serait très longue. « Les conditions d'utilisation de PayPal sont plus longues que Hamlet ».[191] Deux chercheuses américaines avaient déjà tenté de quantifier ce temps en 2012, et en avaient conclu dans leur étude que la lecture intégrale des conditions générales d'utilisation reviendrait à 25 jours par an.[192]

Pourtant, l'importance de ce texte à la lecture chronophage est indéniable, puisqu'il est censé expliquer au contractant les termes du contrat qu'il ne peut négocier. Or trop souvent ces conditions passent à la trappe, jugées inutiles par les utilisateurs, désireux d'installer rapidement une application ou d'utiliser un réseau social. En termes de données personnelles, c'est généralement là que le bât blesse.

Pourtant, le Code de la consommation est très clair en la matière : « avant que le consommateur ne soit lié par un contrat de vente de biens ou de fourniture de services, le professionnel communique au consommateur de manière lisible et compréhensible, les informations suivantes : les caractéristiques essentielles du bien ou du service, compte tenu du support de communication utilisé et du bien ou du service concerné, le prix du bien ou du

---

[190] LANDREAU (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

[191] KOENIG (G.), Introduction, *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, Génération Libre, rapport numérisé, p. 13.

[192] Anonyme, « Combien de temps faut-il pour lire les règles de confidentialité ? », *Slate*, 6 mars 2012, article en ligne.

service », et d'autres mentions obligatoires telles que l'identité du fournisseur et les garanties légales.[193]

Pour pallier à la complexité des conditions générales d'utilisation, des initiatives en vue d'une meilleure compréhension ont vu le jour. Ainsi, le logiciel Polisis, installé sur le navigateur sous la forme d'une extension, les résume sous forme de graphique. L'algorithme fonctionne en *deep learning*, et il se charge de lire et de compiler toutes les informations incluses dans le texte — pour en aboutir à un schéma clair, indiquant quel type de données sont récoltées par l'application ou par le site, pour quelle utilisation, pour quelle durée, ainsi que certaines informations telles que les identités des responsables de traitement.[194]

En outre, il est désormais su de tous, y compris du législateur et des gouvernants, que ces conditions générales d'utilisation ne sont pas, ou mal, lues, et que cela pose des problèmes en termes de consentement. En droit français, l'article 1130 du Code civil dispose que « l'erreur, le dol et la violence vicient le consentement lorsqu'ils sont de telle nature que, sans eux, l'une des parties n'aurait pas contracté ou aurait contracté à des conditions substantiellement différentes ». Par conséquent, « les vices du consentement sont une cause de nullité relative du contrat », poursuit l'article 1131.

Il est indéniable que les conditions générales d'utilisation sont fournies, et que les applications ou les sites qui les proposent s'assurent de leur lecture par la présence d'une case à cocher, certifiant le consentement — mais il ne faut pas être dupes, puisque chaque partie sait qu'elles ne seront que survolées, dans le meilleur des cas. N'est-ce pas là une erreur du législateur, qu'il soit français ou européen, que de laisser ce mode d'acceptation du contrat persister, en sachant pertinemment que ce consentement est tangent ? « Le consentement doit être la cheville ouvrière de la protection du citoyen dans sa vie numérique », et pour le moment, il n'est qu'une protection relativement faible.[195]

Quoi qu'il en soit, certains des principaux acteurs du numérique sont dans le viseur des juges et des frondes législatives sont menées contre eux. Facebook a déjà été maintes fois mis en cause pour des défauts dans ses conditions générales d'utilisation, et cela a encore été le cas récemment, puisque le 16 janvier 2018, la justice belge l'a condamné. Le Tribunal de grande instance estimait en effet que cinq paramètres de réglementation de la confidentialité par défaut étaient illégaux, notamment le partage de localisation avec les autres utilisateurs dans les conversations mobiles. Les conditions générales d'utilisation étaient également visées, en ce qu'elles obligeaient les personnes à utiliser leur vrai nom d'identité, et pas un pseudonyme.[196]

---

[193] Art. L111-1, Code de la consommation.

[194] GROS (M.), « Polisis, du deep learning pour comprendre les CGU » *Le Monde informatique*, 19 fév. 2018, article en ligne.

[195] LANDREAU (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

[196] DE GROËR (S.), « Condamnation de Facebook par le Tribunal de grande instance de Berlin », *RLDI*, n°146, 1er mars 2018, pp. 62-63.

En revanche, dans sa décision, le Tribunal a également rejeté une des prétentions de l'association des consommateurs allemands partie au litige, prouvant ainsi que la patrimonialisation des données ne semble pas envisagée par le pays. En effet, les juges ont considéré que le slogan du réseau, « Facebook est gratuit et le restera toujours », n'était pas mensonger, puisque les utilisateurs ne paient pas le service. L'association considère pourtant que les utilisateurs paient avec leurs données, ce qui rapporte bien plus à l'entreprise que des dollars. C'est précisément ce que cherchent à démontrer les auteurs du rapport de GénérationLibre.

Le citoyen est le générateur de cette mine d'or que sont les données personnelles : quelle raison — éthique ou juridique — justifie son exclusion de cette chaîne de valeur ? Il existe actuellement un réel déséquilibre, auquel la propriété privée pourrait être un rempart. Donner un revenu au citoyen en échange de cette exploitation permettrait déjà de réajuster les rapports de puissance, car pour l'instant, le seul bénéfice qu'il en retire est un accès gratuit à ces services.

Certaines voix s'élèvent en ce sens pour obtenir des revenus de la part des GAFA. L'homme politique et ancien député Julien Dray exposait en janvier dernier sa position sur la question. Estimant que les géants du net étaient trop difficilement taxables, en raison de leurs techniques rodées d'optimisation fiscale, il envisageait une taxe spéciale sur ces entreprises, constituant une « dotation universelle pour chacun d'entre nous, de 50.000 €, à l'âge de 18 ans ».[197] Sans s'interroger sur la faisabilité fiscale et politique de la dévolution d'une telle somme, qui reste chimérique, l'idée n'est pas inintéressante, en ce qu'elle permettrait de résoudre un obstacle juridique conséquent en rééquilibrant les rapports de force.

Quelles conséquences auraient alors l'instauration d'un droit de propriété sur les données personnelles ? Une fois les données vendues, les droits des individus sur celles-ci sont-ils perdus ? Pour Isabelle Landreau, avocate et co-auteur du rapport GénérationLibre, les données sont des biens meubles incorporels pouvant faire l'objet de cessions ou de transmissions. Une fois vendues pour une exploitation catégorielle, pour un temps, et pour une finalité précise, le nanopaiement reçu concerne uniquement cette exploitation. Il n'y a pas de dépossession à vie des données, et l'arsenal juridique existant est maintenu. Le premier générateur de la donnée garderait son droit *d'abusus*, d'*usus* et de *fructus*, ainsi que les revenus sur l'exploitation de sa propriété.

Malgré ces intentions plus que louables, il est encore trop d'obstacles juridiques pour que cette monétisation soit rendue possible. De trop nombreuses raisons, qu'elles soient de droit, d'économie ou sociétales, empêchent ce projet d'aboutir.

[197] Dépêche 6Médias, « GAFA : l'étonnante proposition de Julien Dray », *Le Point*, 14 janv. 2018, article en ligne.

Section 2. L'impossible instauration d'une propriété sur les données personnelles

De nombreuses questions se soulèvent quant à la réelle utilité et à la concrétisation d'une propriété sur les données personnelles, certains allant même jusqu'à se demander si cette hypothèse n'aurait pas été soulevée uniquement par des lobbys afin que les règlementations soient allégées. Il est difficile de démêler les réels intérêts que pourraient y voir les juristes, tant un tel régime poserait des problèmes de droit. Centré sur l'individu, il suit pourtant une logique « d'*empowerment* », mouvement basé sur la reprise du pouvoir par les consommateurs, et n'est pas dénué de sens — mais la réalité témoigne de la complexité de mise en œuvre d'une telle théorie.

Les détracteurs de la propriété sur les données personnelles ont des arguments tant juridiques que philosophiques, à commencer par l'opposition avec le principe même du net, qui vise une liberté de circulation des informations. En effet, les données personnelles s'inscrivent dans les flux transmissibles qui sont désormais une partie intégrante de la vie quotidienne, et pourraient être ainsi à l'origine d'une troisième révolution industrielle, comme l'ont été à leurs époques respectives l'électricité ou les routes ferroviaires. Leur privatisation a toujours été source de discussion tant il semble fondamental que ces outils appartiennent à la collectivité.[198]

Mais ces considérations ne sont pas les seules à empêcher la patrimonialisation des données personnelles : la valeur de celles-ci tendrait à diminuer fortement si elles devenaient individualisées, tant en termes économiques que juridiques. En outre, cette théorie nécessiterait l'adaptation du régime traditionnel de propriété, puisqu'auquel cas celui-ci ne serait pas apte à couvrir tous les aspects spécifiques de ce domaine.

Paragraphe 1. La perte de valeur de la donnée personnelle individualisée

Le Conseil d'État, en 2014, reconnaissait le caractère « attrayant » de la monétisation des données personnelles, mais se refusait à accepter une telle logique, au motif que les lois de protection n'avaient pas été établies dans une logique patrimoniale. L'une de ses raisons, et non des moindres, était la divergence du système de propriété selon les États. À fortiori, une propriété sur les données personnelles reconnue en France ne le serait pas nécessairement dans un autre pays — l'exemple le plus flagrant étant la distinction entre les pays utilisant le

[198] OCHOA (N.), « Pour en finir avec l'idée d'un droit de propriété sur les données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, pp. 1157-1174.

copyright et les pays tels que la France privilégiant le droit d'auteur. Cette distinction ne ferait donc que renforcer les inégalités juridiques territoriales déjà existantes en termes de données personnelles malgré les efforts législatifs constants.[199]

Nombreuses sont les voix qui s'élèvent contre la monétisation des données, qui semble poser son lot de soucis et d'incohérences juridiques. Isabelle Falque-Pierrotin, présidente de la CNIL, ne croit pas en la faisabilité de cette théorie, et ce premièrement pour des raisons économiques, car cela entraînerait la création d'un marché secondaire de la donnée, qui serait contrôlé par l'individu, sans toutefois récupérer le réel pouvoir sur cette industrie.

Elle estime en outre qu'un tel marché finirait par faire perdre de la valeur à ces données : lorsqu'elles ne sont détenues que par certains acteurs majoritaires sur le marché, leur valeur prend de l'expansion. Mais si chaque individu venait à s'y greffer, alors elles perdraient toute leur importance et leur rendement s'effondrerait. Sans s'opposer à ce que l'on change le mode de régulation des données personnelles, il est nécessaire que la méthode remplaçante soit plus efficace que sa précédente — ce qui n'est pas le cas avec cette proposition.[200] Qui plus est, la valeur des données personnelles, rapportée à chaque individu, est dérisoire. Utilisant un simulateur, tel que celui mis en place par le Financial Times, les données d'un étudiant type, sans travail, et sans volonté spécifique de partir en voyages ou d'acheter un smartphone, équivalent à 0.0549 $.[201]

L'idée d'une rétribution aux citoyens pour l'exploitation de leurs données est éthiquement bien pensée, mais paraît difficile à mettre en œuvre à l'échelle individuelle, puisque c'est l'ajout de ces données ensemble qui leur confèrent une telle valeur. Pour chaque individu isolé, cette somme est dérisoire et ne mérite aucune combativité. C'est plutôt en termes de récupération de droits qu'il semble important de mener des actions.

En outre, juridiquement parlant, la patrimonialisation des données pourrait affecter la puissance de l'autorité gouvernementale. En créant un droit de propriété et en déléguant à un marché rémunérateur les données personnelles, et donc la vie privée, un sous-entendu libéral verrait le jour, à savoir que ce marché régulerait la vie privée plus efficacement que le droit, et les institutions qui en sont la matérialisation, telles que la CNIL. Cette solution mettrait en péril la légitimité des lois protectrices de la vie privée.

---

[199] Conseil d'État, *op. cit.,* p. 266.

[200] FALQUE-PIERROTIN (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

[201] STEEL (E.), LOCKE (C.), CADMAN (E.), et FREESE (B.), « How much is your personal data worth ? », *Financial Times*, 12 juin 2013, m.à.j 15 juil. 2017, article en ligne.

Vient ensuite l'argument défiant la patrimonialisation des données personnelles, selon lequel celles-ci pourraient être assimilées à des éléments du corps humain, en rendant la revente contraire au principe d'indisponibilité de ce dernier. En réalité, les données font écho à notre corps numérique, de plus en plus alimenté par la vie numérique. Elles sont accumulées via les éléments de notre réelle personnalité. Aux identités et aux corps que nous connaissons se sont ajoutés des données numériques.[202]

Cet argument pourrait être facilement renversable tant le corps numérique est déjà disponible, puisque les données personnelles sont exploitées par les GAFA. Elles sont déjà au cœur du commerce : en France, elles représentent 7 à 8% du produit national brut, soit des milliards d'euros, qui reviennent aux entreprises telles que Facebook.[203] Mais il est de bien faible qualité face aux détracteurs de la patrimonialisation. Cette analogie est incohérente puisque le droit au respect de son corps est ce que l'on pourrait qualifier de droit fondamental — or il n'y a pas, et il n'y aura jamais, de marché des droits fondamentaux.

Il est par exemple impossible de vendre son droit de vote, car si c'était le cas, cela reviendrait à commercialiser les droits et les libertés fondamentales. Par cette réalisation, le droit de contrôle individuel sur le vote, mais également le droit collectif qu'a la société française d'élire ses représentants, serait complètement réduit à néant. En outre, il ne peut y avoir de propriété réelle sur les données dans la mesure où rien ne peut déposséder l'individu de son droit de contrôle sur celles-ci, même après les avoir cédées.[204]

Pour la présidente de la CNIL, la proposition de monétisation des données équivaudrait peut-être à satisfaire les GAFA, car cela leur coûterait très peu par rapport à la marge de manœuvre tout aussi large qu'ils obtiendraient en contrepartie. Même si le droit français est encore parfois inefficace face à eux, en partie pour des raisons de territorialité, la législation reste un levier très fort — leur transférer la propriété sur les données personnelles ne leur enlèvera pas leurs bénéfices, et le retour en arrière pour les individus sera impossible. La solution afin de conserver une crédibilité et une puissance juridique face à ces acteurs résiderait plutôt dans un renforcement des mécanismes déjà existants.[205]

---

[202] FALQUE-PIERROTIN (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

[203] LANDREAU (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

[204] MAUREL (L.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

[205] FALQUE-PIERROTIN (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

Paragraphe 2. L'incompatibilité de la patrimonialisation avec le régime de propriété traditionnel

L'application d'un régime traditionnel de propriété poserait en sus des problèmes de cohérence juridique. Il suffit, pour le constater, d'examiner la faisabilité de l'hypothèse au regard des trois prérogatives du droit de propriété, que sont l'*usus*, l'*abusus* et le *fructus*. L'*usus* est défini par l'article 544 du Code civil comme le « droit de jouir et disposer des choses de la manière la plus absolue ». Il existe déjà, car l'on choisit ou non de divulguer nos données — un consentement est malgré tout recueilli.

L'obstacle, avec un droit de propriété, résiderait dans le cas de la vente de données : si un individu venait à vendre son nom et son prénom, en tant que donnée, l'usurpation de l'identité deviendrait légale.[206] Il n'est pas, en revanche, de problème pour le *fructus*, c'est-à-dire le droit de récolter et d'exploiter les fruits résultant du bien possédé : ce serait en effet le but de l'établissement d'un tel droit sur les données, qui existe déjà au profit des industries numériques.

Concernant l'*abusus,* la position peut être nuancée. Il apparaît que les GAFA pourraient, s'ils avaient un droit de propriété sur nos données, les supprimer à leur guise, créant de véritables problèmes de droit.[207] Mais cette argumentation peut être renversée en prenant un exemple. Si Facebook, détenteur du nom et du prénom d'un de ses utilisateurs, décidait de supprimer ces données, cela reviendrait matériellement à l'effacement de son compte sur le réseau. L'effacement de la donnée n'anéantit pas l'identité de la personne à l'état civil. En outre la suppression d'un compte ou d'une donnée personnelle, sans raison valable, pourrait parfaitement être contestée devant le juge.

Une autre solution fait également débat, consistant à gérer les données personnelles à la manière des droits d'auteur, avec une société de gestion collective et un système de répartition des revenus. Mais pour certains, l'analogie avec le droit d'auteur est dangereuse, car il ne s'agit pas des mêmes droits dont il est question. Le droit des données personnelles est un droit qui ne dépossède jamais des droits de contrôle, et il est quand même possible de les exercer, même après les avoir cédés. En outre, il est impossible d'être l'auteur de son nom et de son prénom, ou de son adresse. Générer n'est pas créer, et la donnée personnelle est générée par l'utilisateur, alors que l'œuvre protégeable par le Code de la propriété intellectuelle est créée par son auteur.[208]

---

[206] MATTATIA (F.), et YAÏCHE (M.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *RLDI*, n°114, 1er avr. 2015, pp. 60-63.

[207] MATTATIA (F.), et YAÏCHE (M.), *ibid.*

[208] MAUREL (L.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

Ce qui appert comme intéressant dans cette analogie avec le droit d'auteur est la possibilité de séparer les droits sur les données personnelles en droits moraux, incessibles, et en droits patrimoniaux, cessibles, puisqu'ils le sont d'ailleurs déjà. Mais cette possibilité est maigre face aux difficultés d'applicabilité du Code de la propriété intellectuelle aux données personnelles, notamment en ce qui concerne la preuve de l'originalité de l'œuvre.[209] Les définitions classiques de l'originalité tournent autour de sa représentativité de l'empreinte de l'auteur, de sa personnalité, de ce qui le rend reconnaissable. « L'œuvre originale est celle dans laquelle le créateur a pu déployer le minimum de fantaisie inhérent à toute création littéraire ou artistique, en échappant aux contraintes de la technique ».[210]

Or comment prouver qu'une suite de nombres élaborée mathématiquement par un algorithme est témoin de l'identité, dans la mesure où aucune personnalité juridique n'est dévolue aux intelligences artificielles ? Pourtant, les avancées sociales pourraient bien vite démontrer le contraire et imposer une mutation au droit. L'Arabie saoudite a en effet accordé la nationalité à Sophia, un robot d'apparence humaine, créé à Hongkong.[211]

En outre, en 2016, le Parlement européen envisageait de reconnaître une personnalité juridique spéciale aux robots, assortie d'un régime de droit d'auteur pour les œuvres créées par les intelligences artificielles — certains logiciels permettant d'ores et déjà de composer des musiques.[212] Bien loin encore de faire le lien entre la création d'une donnée personnelle par une intelligence artificielle et la personnalité juridique d'un robot, il ne faut pas non plus nier les avancées en la matière.

Les difficultés d'applicabilité du régime de la propriété, notamment en les exemples de ces trois prérogatives, démontrent bien qu'il semble compliqué d'aller vers une transposition d'un droit déjà existant à cet objet si spécial qu'est la donnée personnelle. La solution réside peut-être dans un autre type d'encadrement juridique, qui correspondrait en tous points aux problématiques posées en la matière.

---

[209] MATTATIA (F.), et YAÏCHE (M.), *ibid.*

[210] LUCAS (A.), et SIRINELLI (P.), « L'originalité en droit d'auteur », *JCP*, n°23, 9 juin 1993, doctr. 3681.

[211] MORIN (V.), « Sophia, robot saoudienne et citoyenne », *Le Monde*, 4 nov. 2017, article en ligne.

[212] CHAMPEAU (G.), « Reconnaître un droit d'auteur aux robots ? L'idée fait son chemin… », *Numérama*, 23 juin 2016, article en ligne.

Chapitre 2. Les prérogatives personnelles sur l'identité numérique

La réification des données personnelles est une hypothèse dont les fondements sont louables, mais qui ne peut se faire à raison de la primauté accordée à la personne sur l'économie. Reconnaître une patrimonialité sur les données personnelles équivaudrait à accepter la commercialisation abusive qui en est faite, en sachant que celle-ci est parfois contraire aux droits des individus — cela reviendrait, en quelque sorte, à cautionner l'hégémonie que les entreprises telles que les GAFA ont imposée.

De plus, la loi, qu'elle soit européenne ou française, fait d'emblée le lien avec la notion de personne, en y rattachant les données personnelles dans la définition qu'elle en donne. Or à compter que l'identité numérique, rattachée à l'identité personnelle, soit protégée par les droits de la personnalité, celle-ci ne pourrait décemment pas faire l'objet d'une exploitation commerciale.[213]

Il existe déjà dans la pratique des droits sur l'identité numérique, qui peuvent totalement être rattachés à des prérogatives relevant des droits de la personnalité. Elles permettent de rapprocher le droit sur l'identité numérique d'un droit à l'autodétermination informationnelle, reconnu par l'Allemagne, et parfois même de la conception dualiste américaine, entre le *right to privacy* et le *right to publicity*.

Section 1. La préséance de droits personnels sur l'identité numérique

L'identité a depuis longtemps dépassé sa simple fonction sociale de reconnaissance et d'inter-dénomination. Elle est désormais le fruit d'un procédé d'insertion sociale. Elle devrait être à la base des droits fondamentaux, puisque son abnégation par les régimes totalitaires dans les périodes de crise témoigne bien de son importance collective.

Le Conseil Constitutionnel n'évoque que très rarement la notion d'identité, et ne la consacre nullement comme un droit fondamental, lui préférant des réflexions sur l'accès à la vie privée. Cette position s'explique par la séparation entre l'aspect objectif de l'identité, c'est-à-dire ses caractéristiques réelles et concrètes, et l'aspect subjectif de l'identité, qui témoigne de la personnalité de l'individu. C'est sur le premier aspect que choisit de se concentrer le Conseil, laissant le second aspect à la loi.

---

[213] MOURON (P.), « Perspectives sur le droit à l'identité numérique », pp. 115-127, *in* MOURON (P.), et PICCIO (C.) [dir.], *L'ordre public numérique : libertés, propriétés, identités*, PUAM, 2015, pp. 115-117.

Pour autant, il n'est pas question de renier la fondamentalité de l'identité, d'autant plus numérisée. « L'identité, selon Ricoeur, se nourrit tout autant d'ipse (perception de soi comme un être unique) que d'idem (continuité du sujet dans le temps et l'espace) ; elle se nourrit d'universalité et de personnalité ».[214] Qu'ils soient matériels ou non, les éléments de l'identité numérique sont des représentations de la personne, et leur personnification est indéniable. Malgré l'absence d'une reconnaissance textuelle, il est manifeste que les prérogatives déjà reconnues par la loi en la matière s'apparentent aux droits de la personnalité.

Paragraphe 1. Les prérogatives de l'identité numérique, des droits personnels

En revenant à l'identité numérique dans la définition la plus basique que l'on puisse en donner, il ne s'agit finalement que d'une projection numérique de l'identité personnelle : une reproduction, en quelque sorte. Ce qui la distingue de l'identité matérielle est la projection qui en est faite dans le numérique — cette projection étant parfois enjolivée ou modifiée par les possibilités qu'offre ce dernier. Les diverses utilités des réseaux sociaux ont permis aux individus de se construire eux-mêmes une vision de leur identité, parfois dissimulée de tous, parfois exposée au grand jour, quelquefois même allant jusqu'à la création d'avatars, que le droit reconnaît désormais comme des œuvres de l'esprit, malgré qu'elles n'aient aucune existence physique.[215]

L'identité numérique a développé une ampleur sociale plus conséquente que l'identité traditionnelle, en ce qu'elle permet à l'individu de s'échapper des carcans de sa dénomination quotidienne : à titre d'exemple, prendre un pseudonyme sur un réseau social est bien plus simple que de changer son prénom à l'état civil. Outre les exploitations commerciales qui sont faites des données personnelles de l'individu, celles-ci représentent désormais des parties d'eux-mêmes, plus ou moins concordantes avec la réalité, et qui déterminent ce qu'ils sont, mais également leur place dans la société, et peut-être plus important encore, dans une sphère virtuelle.

Comment renier dès lors que, si droit sur l'identité numérique il existait, celui-ci serait au rang des droits de la personnalité, ces derniers « ayant pour objet de protéger la personnalité dans ses divers aspects », tant ils sont « inhérents à la personne physique » ?[216] À l'image des procédés de reproduction artistique, passés de la lithographie à la photographie, puis à la

---

[214] BIOY (X.), « L'identité de la personne devant le Conseil Constitutionnel », *Revue française de droit constitutionnel*, 2006/1, n°65, pp. 73-95.

[215] MOURON (P.), « L'identité virtuelle et le droit "sur" l'identité », *RLDI*, n°64, 1er oct. 2010, pp. 58-63.

[216] LEPAGE (A.), « Droits de la personnalité », n°151, *in* SAVAUX (É.) [dir.], *Rép. civ.*, 2009, actu. 2018.

captation par caméra, la fixation de l'identité a évolué. De l'oral, à l'écrit, puis à la numérisation, les techniques d'identification ont conduit la notion d'identité elle-même à évoluer.

« Au XIX^e siècle, la reproduction technique avait atteint un niveau tel, que non seulement elle commença à faire de l'ensemble des œuvres d'art traditionnelles son objet et à soumettre leur action aux plus profondes transformations, mais elle acquit elle-même une place parmi les procédés artistiques ».[217]

Ce que démontre Walter Benjamin à propos des procédés de reproduction artistique trouve parfaitement à s'appliquer dans les procédés de projection identitaire. La photographie, technique de représentation d'un portrait, ou d'un paysage, acquérait au fil du temps une valeur d'œuvre d'art à part entière, passant d'une simple reproduction à un chef-d'œuvre. La fixation de l'identité numérique n'est plus un procédé utilitariste, elle est désormais entrée dans les mœurs et fait partie de la vision qu'ont les personnes d'elles-mêmes.

La fixation de l'identité numérique n'est plus simplement un gain de temps ou une rente économique, elle est désormais également un procédé anthropologique qui fait partie de la notion d'identité. En témoigne d'ailleurs l'abstraction des individus pour les nouvelles technologies et l'inter-connectivité. Il existe donc déjà un corpus de droits qui serait à même de protéger l'identité numérique — les droits de la personnalité — puisque les individus le peuvent déjà en les mobilisant séparément.

Les abus de la médiatisation des personnalités dans la presse dite « people », dans les années 1970, ont conduit à protéger des éléments tels que la vie privée ou le droit à l'image. Ces prérogatives juridiques sont des réponses à des comportements peu respectueux de l'intimité de certains. Elles se sont vues renforcées avec l'apparition du numérique, puisque la diffusion de l'information est devenue quasi-instantanée. Ainsi, une photo parue dans un magazine papier ne touche potentiellement que ceux qui l'achèteront en kiosque, et bien que nombreux, ils sont loin d'égaler le nombre de récepteurs potentiels en ligne.

L'apparition de l'identité numérique a engendré les mêmes incertitudes quant à l'efficacité du peu de protection déjà en vigueur et, après l'affaire SAFARI, des prérogatives spéciales ont vu le jour, l'ensemble des données personnelles et des traces numériques étant désormais des moyens d'espionnage et de fichage.[218]

Certains auteurs, tels qu'Emmanuel Derieux, reconnaissent l'existence d'atteintes aux droits des personnes, causées par les nouvelles techniques de communication en ligne et par les médias. Il peut s'agir de la diffusion sans autorisation de l'image des personnes, ce qui pose généralement problème avec les personnalités publiques, dans des cas où il est souvent difficile de délimiter ce qui relève de l'intérêt du public et de la nécessité informationnelle, et ce qui

---

[217] BENJAMIN (W.), *L'œuvre d'art à l'époque de sa reproductibilité technique*, Allia, 2017, p. 17.

[218] DERIEUX (E.), « Droits de la personnalité et protection des données personnelles face aux médias et à leurs usages », *Légicom*, 2009/2, n°43, pp. 123-138.

relève de la sphère privée — ou de la diffusion de l'image des biens, mais également des données personnelles.

En l'espèce, l'article 67 de la loi du 6 janvier 1978 prévoit des exceptions à l'interdiction de l'utilisation des données personnelles, notamment en ce qui concerne les activités journalistiques, ce qui, ici encore, est susceptible de causer des atteintes aux individus. *De facto*, l'ensemble de ces affirmations démontre bien que, si atteintes aux droits des personnes il y a, protection par les droits de la personnalité il devrait y avoir.[219] Or cet encadrement juridique n'existe que par le biais de dispositions éparses qui, bien qu'efficaces et légalement bien construites, ne font que perdre de leur puissance par leur diversité.

Paragraphe 2. L'absence d'uniformité dans la protection législative de l'identité numérique

Pour protéger les éléments de son identité, qu'ils soient immatériels, c'est-à-dire reliés à un sentiment d'identité, ou matériels, comme les données personnelles, l'individu dispose de certains moyens d'actions. Il existe des fondements juridiques permettant de sauvegarder sa réputation digitale. Concernant tout d'abord les éléments immatériels, et s'agissant par exemple des diffamations, la loi du 29 juillet 1881 trouve parfaitement à s'appliquer puisqu'elle punit « toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé ».[220] Il en va de même pour les injures.

Le droit au respect de la vie privée peut également être mobilisée, puisque les dispositions de l'article 9 du Code civil sont également applicables lors de la divulgation sans autorisation de contenus privés. Le droit pénal trouve sa place également, par son article 226- 1, qui punit la captation, l'enregistrement ou la transmission d'images ou de paroles sans l'autorisation de l'intéressé — transmission qui peut totalement s'effectuer sur un support numérique. En outre, comme évoqué ci-dessus, il existe désormais un délit d'usurpation d'identité, puisque l'article L226-4-1 a été enrichi d'un second alinéa, prévoyant la même peine sur tout support « de communication au public en ligne ».

Concernant les éléments matériels, c'est-à-dire les données personnelles, outre les prérogatives d'accès, de rectification et de retrait du consentement, le droit à l'oubli ressemble à s'y méprendre à une disposition tournée vers l'individu. Bien que le règlement européen ne fasse pas taire les hésitations sur la question, l'ayant également nommé droit au déréférencement, son utilité n'est plus un doute depuis le célèbre arrêt Google Spain rendu par

---

[219] DERIEUX (E.), « Droits de la personnalité et protection des données personnelles face aux médias et à leurs usages », *Légicom*, 2009/2, n°43, pp. 123-138.

[220] Art. 29, loi du 29 juillet 1881 sur la liberté de la presse.

la Cour de Justice de l'Union Européenne.[221] Un ressortissant espagnol avait en effet attaqué le moteur de recherche pour avoir indexé à son nom un lien, ancien de plusieurs dizaines d'années, renvoyant à un article le condamnant à des enchères immobilières, à raison de dettes sociales.

Arguant à juste titre qu'un préjudice de réputation lui était infligé, dans la mesure où ce passé financier était derrière lui, le requérant demandait la suppression de ces liens. Après avoir effectué une mise en balance des intérêts fondamentaux en présence, à savoir le droit d'information du public contre le droit au respect de la vie privée, la Cour avait finalement tranché en la faveur du requérant, considérant que l'atteinte était manifeste.[222] Pour autant, bien que cette porte ouverte à d'autres demandes de référencement soit une avancée en la matière, il est nécessaire d'avoir à l'esprit qu'il ne s'agit pas là d'un réel droit à l'oubli. Le contenu existe toujours en ligne et il est possible d'y avoir accès en connaissant son adresse URL directe — il n'est simplement plus affecté à une entrée de recherches précises, en l'occurrence le nom de la personne.

Le problème est que l'ensemble de ces dispositions pourraient, greffées les unes aux autres, générer une protection globale sur l'identité numérique, à compter qu'il existe sans nul doute d'autres moyens juridiques de protection. Mais l'éparpillement de ces garanties leur cause du tort, en ce qu'elles ne permettent pas une harmonisation de la législation — par conséquent, il devient encore plus ardu de protéger une identité elle-même éparse digitalement.

Dès lors, la création d'un réel corpus et d'un droit sur l'identité numérique serait bénéfique, puisqu'elle permettrait une protection globale, pouvant être placée au niveau d'un droit fondamental, voir constitutionnel — l'idéal étant, en outre, que l'individu ait une possibilité de parole ou d'action sur celle-ci, ce qui pourrait se rapprocher de la conception américaine de la vie privée.

---

[221] CJUE, n° C-131/12, 13 mai 2014, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzàlez.

[222] CASTETS-RENARD (C.), « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *RLDI*, n°106, 1er juil. 2014, pp. 68-75.

Section 2. Le droit à l'autodétermination informationnelle

« Le droit à l'autodétermination se situe à un autre niveau : il donne sens à tous ces droits, qui tendent à le garantir, et doivent être interprétés et mis en œuvre à la lumière de cette finalité. Il pourrait donc être inscrit dans les considérants de la proposition de règlement ou dans un article introductif, qui prévoirait que les individus jouissent d'un droit à l'autodétermination informationnelle, c'est-à-dire du droit de décider de la communication et de l'utilisation de leurs données à caractère personnel, dans les conditions et les limites définies par le règlement ».[223]

Plus qu'une prérogative, ce droit, inspiré directement d'une décision de la Cour constitutionnelle allemande, pourrait être requalifié de théorie générale, de modèle, pour la protection des données personnelles. Cette ligne de conduite irriguerait alors toutes les garanties offertes par la loi française et deviendrait en quelque sorte l'esprit d'un droit sur l'identité numérique, à savoir la reconquête des éléments de l'individu.

Bien que le Conseil d'État envisageait déjà la notion dans son étude annuelle de 2014, il n'est toujours pas fait écho à cette notion dans les textes, bien que le règlement européen semble s'en inspirer, tant il apparaît que l'individu est au centre des préoccupations du sujet. Pour autant, la volonté des individus de prendre part à ce combat, et les influences des pays extérieurs en termes de réglementation de la vie privée pourrait faire émerger malgré lui ce concept d'autodétermination.

La séparation doctrinale qu'effectue les juristes américains entre un droit individualiste à la protection de la vie privée et un droit économique au dévoilement de soi peut être aisément rapprochée d'un droit à l'autodétermination informationnelle, qui appert comme un compromis idéal entre la personnification et la patrimonialisation des données personnelles.

Paragraphe 1. L'influence de la vision américaine de la vie privée

La vie privée est une notion sujette à de nombreuses divergences, en témoigne la conception américaine, puisqu'à titre d'exemple, Vint Cerf, directeur évangéliste d'internet de Google et créateur du protocole IT/IP, « privacy may be an anomaly, an artificat construct of the industrial age ». En effet, selon lui, la vie privée n'existe pas dans les petites villes puisque tout le monde se connaît. Il estime que c'est l'expansion civile qui a engendré une étanchéité des informations.

[223] Conseil d'État, *op. cit.,* p. 269.

Le système juridique américain envisage la vie privée en deux axes : le *right to privacy* et le *right to publicy.* La consécration de la vie privée aux États-Unis est le fruit d'un mélange de fondements de droit servant indirectement à la protéger — notamment par le biais de trois amendements de la Constitution, garantissant respectivement le droit de ne pas être recherché sans fondement juridique etla protection de la vie familiale, de l'enfance, ou des relations amoureuses.

Ce droit au respect de la vie privée était prôné pour la première fois par deux célèbres juristes, Louis Brandeis et Samuel Warren, dans un essai de 1890.[224] Leur détermination à démontrer la nécessité de ce qu'ils appellent un « right to be left alone » avait conduit dans un premier temps quatorze États à adopter une législation générale sur la vie privée, jusqu'à ce que l'État de New York s'y adjoigne en 1948. Ce texte visionnaire prouvait d'ailleurs son actualité lors du développement puissant d'Hollywood et de l'émergence de célébrités américaines, constamment exposées médiatiquement, et à la recherche d'intimité face à la presse à scandales. Il demeure encore aujourd'hui l'une des bases de réflexion sur le concept de vie privée et continue d'irriguer les doctrines et les jurisprudences.[225]

La vision de la vie privée américaine repose sur les abus de commercialisation et d'exposition médiatique du nom, de l'image ou des informations personnelles dont les personnalités publiques ont été victimes durant leur passage sur le devant de la scène. Ce fondement trouverait à s'appliquer dans le problème de la réglementation européenne des données personnelles, qui sont constamment utilisées par les responsables de traitement.

Malgré cela, certains auteurs tentent de renverser l'appréhension du concept de la vie privée, au prisme de son contraire : la publicité. Les partisans de cette thèse soulignent à juste titre que, dans le cas précis des personnalités publiques, l'argument leur est régulièrement opposé que leur statut les contraint à accepter qu'une partie de leur vie soit exposée au vu et au su de tous — d'autant qu'au regard de la fédéralité des États-Unis, l'application de la protection n'est pas uniforme sur le territoire.

Cet argument est totalement applicable aux réseaux personnels et aux applications digitales dans la mesure où les utilisateurs ont accepté les conditions générales d'utilisation, et ont par conséquent consenti à l'exploitation de leurs données : comment pourraient-ils alors se prévaloir par la suite d'une atteinte à leur vie privée ?

Le renversement opéré par la doctrine consistant à garantir un droit à la publicité, et non un droit à la vie privée, permet une meilleure adaptation à la réalité économique et juridique du pays. Cette hypothèse soutient que, partant du principe que toutes les informations personnelles sont privées, l'individu détient le droit de dévoiler celles qu'il souhaite, tout en sachant pertinemment qu'elles seront ensuite exploitées commercialement.

---

[224] WARREN (S.), et BRANDEIS (L.), *The Right to Privacy*, 1890.

[225] NIMMER B. (M.), « The Right of Publicity », *Law and Contemporary Problems*, 1954, vol. 19, n°2, p. 203.

Il s'agit d'une action défensive de la part des utilisateurs, qui récupèrent ainsi une partie de leur souveraineté sur leurs données. Ainsi, en cas de préjudice, le fondement juridique sera différent : avec la vie privée, c'est l'atteinte à l'individu qui est mesurée, alors que dans le droit à la publicité, il s'agira de l'estimation de la valeur de l'information divulguée.[226]

Cela permet, de plus, de se rapprocher des tendances sociétales qui emplissent désormais la société, et tout particulièrement l'exposition excessive de soi — puisqu'il s'agirait en fait d'un droit au dévoilement des données. Les informations transmises seraient exploitées en toute légalité sans que ne puissent être engagées d'actions à l'encontre de ces procédés, et, à contrario, l'utilisation de données non dévoilées par l'individu serait légalement punie. Cette séparation permet de s'axer soit sur le versant économique de l'utilisation des données, soit sur le versant individuel. Ce « *right to publicy* » a d'ailleurs été consacré textuellement par certains États, notamment la Californie et New York.

Ce droit a déjà été le fondement d'une décision des juridictions californiennes.[227] Le réseau social Facebook était attaqué par un groupement d'utilisateurs, désireux de voir condamnée la pratique des « sponsorised stories », des publicités commerciales basées sur l'utilisation des informations personnelles, sans aucun consentement préalable des détenteurs des profils concernés. Sur la base de la section 3344 du Code civil de Californie, qui interdit l'exploitation commerciale des informations personnelles sans autorisation, la juridiction américaine était allée en faveur du groupe de consommateurs, leur reconnaissant un « *right to publicy* ». Un accord entre les deux parties avait finalement indemnisé les requérants à hauteur du préjudice subi.[228]

La vision américaine de la vie privée cherche à se rapprocher au mieux de la réalité du numérique, et peut totalement être rapprochée de l'autodétermination informationnelle, un droit consacré récemment par l'Allemagne, et dont la France pourrait s'inspirer, tant il est logique et judicieusement bien pensé.

---

[226] NIMMER B. (M.), « The Right of Publicity », *Law and Contemporary Problems*, 1954, vol. 19, n°2, p. 216.

[227] N. D. Cal., n°11-CV-01726, 4 avr. 2011, Angel Fraley, and al. c. Facebook.

[228] KOEHLER (J.), « Fraley v. Facebook : The Right of Publicity in Online Social Network», *Berkeley Technology Law Journal*, 2013, vol. 28, pp. 963-1002.

Paragraphe 2. L'autodétermination informationnelle, un régime juridique à part entière

La notion d'autodétermination informationnelle a été consacrée par la Cour constitutionnelle allemande, et ce droit peut se définir comme la liberté de décision quant au dévoilement des informations personnelles par un individu. Pour autant, ni la loi française, ni le règlement européen ne le consacrent textuellement, tout comme l'identité numérique d'ailleurs — pour autant, le Conseil d'État en traitait déjà en 2014, lui reconnaissant un sens plus global.

Dans son rapport annuel, la Haute juridiction se penchait sur la conciliation du numérique et des droits fondamentaux. L'une de ses premières propositions était de considérer le droit sur les données personnelles comme un droit à l'autodétermination, et non comme un droit de propriété. Ainsi, le Conseil d'État ne considère pas l'autodétermination informationnelle comme un droit fondamental, mais comme la nature du régime juridique se devant de les encadrer. Il s'oppose par là-même à la patrimonialisation des données.[229]

Cette patrimonialisation des données serait un réel problème pour les pouvoirs publics. Conférer un tel droit de propriété sur les informations personnelles supposerait certaines exceptions, comme il en est régulièrement pour tous les biens appropriables, à compter que les atteintes soient légitimées. Or il y aurait nécessairement des préjudices à cette propriété des données, puisqu'elles sont constamment exploitées — ils se devraient donc d'être examinées et autorisées par le Conseil Constitutionnel et la Cour Européenne des Droits de l'Homme.

L'autodétermination informationnelle semble être une alternative plus que louable, en ce sens, puisque n'impliquant aucune propriété sur les données, mais bien un droit sur l'identité numérique. Le Conseil d'État expose quatre avantages à l'instauration d'un tel régime. Il permettrait de justifier la position de la Charte européenne des droits de l'Homme, qui érige la protection des données personnelles en un droit distinct, et rendrait à l'individu un moyen d'action positif sur son identité, au cœur de la vie numérique.

De plus, si un droit à l'autodétermination informationnelle était instauré, il pourrait également connaître des exceptions, mais permettrait dans sa globalité de protéger également la société démocratique, chacun se voyant désormais maître de la délivrance de ses informations. Enfin, il s'agirait d'un premier pas vers la récupération des données par les individus, processus qui semble bien ambitieux au vu de l'hégémonie indétrônable des entreprises.[230]

L'ensemble de ces questions démontre bien en filigrane le paradoxe constant que soulève l'émergence d'un droit sur l'identité numérique : qui, des individus ou des États, serait le mieux placé pour assurer une protection efficace des données personnelles ?

---

[229] Conseil d'État, *op. cit.,* p. 331.

[230] Conseil d'État, *Le numérique et les droits fondamentaux*, étude annuelle, 2014, pp. 264-268.

Titre second – L'identité numérique, entre souveraineté étatique et contrôle individuel

Face à la numérisation explosive des relations sociales, des procédés technologiques, et même des processus législatifs, la première réponse qu'apporte l'État est une tentative de soumission de cette évolution au droit. « La souveraineté numérique est justement cette volonté de maîtriser ce nouveau destin, afin qu'il réponde des lois de la République et que cette mutation renforce tout autant nos libertés, nos choix que notre prospérité ».[231]

Cette volonté répond d'un constat flagrant pour les gouvernants : la mise en réseau et la numérisation sont des atouts économiques. Les bénéfices dégagés par les entreprises du numérique sont parfois colossaux et leur importance dans les relations économiques n'est pas négligeable — en témoigne la volonté française de moderniser ses entreprises et de favoriser les innovations. Ainsi, il est impensable de laisser ce filon à la dérive sans qu'aucun contrôle ne soit appliqué dessus, tout comme il est délicat pour les États de trouver un régime adapté — tant les entreprises concernées gardent la mainmise sur leur puissance.

Chapitre 1. Les initiatives étatiques d'encadrement de l'identité numérique

Il serait très inefficace pour les États de réguler la protection de l'identité numérique par une surveillance permanente. Cette omniprésence menace au contraire les équilibres de pouvoirs entre les gouvernants et les gouvernés, car dès lors c'est l'État qui porte une atteinte démesurée à la vie privée qu'il est censé garantir.[232] Les tentatives en la matière ont d'ailleurs défrayé la chronique — en témoigne le dévoilement des informations délivrées par Edward Snowden, ancien employé de la NSA et lanceur d'alerte du programme Prism, mis en place par les États-Unis pour surveiller la population.[233]

---

[231] BELLANGER (P.), « Les données personnelles : une question de souveraineté », *Le Débat*, 2015/1, n°183, pp. 14-25.

[232] FINCH (K.), « Welcome to the Metropticon : Protecting Privacy in a Hyperconnected Town », *Fordham Urb. L. J.*, vol. 41, n°5, mars 2016, pp. 1581-1615.

[233] BAUSARDO (T.), « Quel passé pour Prism et Snowden ? », *Vacarme*, 2014/1, n°66, pp. 142-157.

L'État a donc une position délicate en la matière. Il lui appartient de surveiller les individus pour sa sécurité intérieure, tout en respectant les dispositions sur la vie privée — et il doit également trouver les initiatives de protection les plus justes en ce qui concerne les données personnelles et les identités numériques. Face à une évolution constante des technologies, un tel encadrement, avec une efficacité pleine, est très complexe à obtenir. Les gouvernements ont, en outre, des acteurs puissants face à eux, ne leur rendant pas la tâche facile.

Malgré tout, la velléité étatique de garder une assise solide sur la protection des identités ne faiblit pas, et malgré la difficulté de la matière, les initiatives législatives — françaises et européennes — et les projets d'action deviennent de plus en plus nombreux. Face aux entreprises du numérique, les États se dressent peu à peu pour rappeler leur force politique.

Section 1. La difficulté d'un encadrement complet de l'identité numérique

« Il n'y a pas de maîtrise sans possession. Ce droit fondamental[234] doit aujourd'hui s'étendre aux données, prélude d'une véritable propriété de soi sur soi ».[235] Le courant doctrinal qui cherche à revaloriser la donnée personnelle en la rendant monétisable tend à prendre de l'ampleur, comme le démontre la parution de nombreux articles en la matière — articles de partisans mais aussi de détracteurs.

La régulation des données personnelles créées par les identités numériques est un enjeu juridique majeur du XXI^{ème} siècle, tant elles ont de la valeur économique. Les États ont donc une volonté croissante de s'arroger un monopole sur leur contrôle, qui pourtant leur échappe bien souvent. L'endiguement de ce flux d'informations personnelles est un enjeu majeur qui ne peut être effectué par le droit uniquement. Pourtant, de nouvelles contraintes techniques sont apparues avec les technologies.

[234] Sous-entendu le droit de propriété.

[235] KOENIG (G.), Introduction, *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, Génération Libre, rapport numérisé, p.8.

Paragraphe 1. Les contraintes techniques liées à l'identité numérique

Il existe de nombreuses contraintes liées à l'identité numérique — la première et non des moindres étant la territorialité. La réglementation sur les données personnelles diverge selon les pays et les différences de culture par rapport au numérique sont parfois flagrantes. En témoignait d'ailleurs la fameuse affaire opposant la société américaine Yahoo ! à deux associations françaises contre l'antisémitisme, en 2000. Était en cause l'accès à une vente aux enchères d'anciens objets du régime nazi, accessible aux utilisateurs américains mais également français, ce qui posait clairement un problème au regard du passé national.[236] En l'espèce, la loi française ne tolère pas la publication de tels signes, alors que la loi américaine a une vision extensive de la liberté d'expression.[237] Les mêmes problèmes se rencontrent au niveau de la conception des données personnelles.

En outre, il existe des failles techniques, dont témoignent les récents évènements en Inde : un informaticien toulousain au service d'Android a démontré des failles dans la protection informatique du pays en piratant, par cinq méthodes différentes, les cartes d'identité disponibles sur Aadhaar — la plus grande base indienne de données biométriques. Or en Inde les cartes d'identité permettent d'avoir accès aux données bancaires.

Pour prouver que le système n'était vraiment pas adapté, l'ingénieur est allé encore plus loin et s'est lancé le défi de pirater le plus grand nombre de cartes d'identité en trois heures. Le résultat était accablant : 20.000 cartes d'identité sont arrivées en sa possession — soit potentiellement 20.000 comptes bancaires. Une journaliste avait déjà tenté de mettre à jour ce cruel manque de protection mais l'autorité indienne en charge des données personnelles avait préféré la poursuivre en justice.[238]

Bien que cet exemple prouve les lacunes techniques en la matière, il permet malgré tout de relativiser le niveau de protection français, qui semble bien élevé au regard de cet incident. La problématique est ainsi posée : malgré une réglementation européenne et française étoffée, et des textes bien construits qui tentent d'endiguer la régulation des données sous tous les angles, il semble impossible de donner à un ou plusieurs acteurs une souveraineté totale sur ces dernières. Tout porte à penser que cette toute-puissance revienne aux GAFA, et bien que cette affirmation soit en partie vraie, puisque ce sont eux qui totalisent le plus de bénéfices, le droit reste une barrière non négligeable à l'obtention des pleins pouvoirs sur les données.

---

[236] TGI Paris, référé, 22 mai 2000, UEJF et Licra c. Yahoo ! Inc. et Yahoo ! France.

[237] ROJINSKY (C.), « Cyberespace et nouvelles régulations technologiques », *D.*, 2001, pp. 844-847.

[238] FARCIS (S.), « Données biométriques : L'inde le doigt dans l'œillère », *Libération*, 30 mars 2018, pp. 8-9.

Les États sont, bien trop souvent, en retard par rapport aux évolutions technologiques — leur souveraineté n'est que partielle. Quant aux individus, se conscientiser par rapport à l'utilisation faite de leurs données personnelles serait déjà une étape majeure, à laquelle pourrait ensuite succéder la récupération de ces dernières.

Les gouvernements cherchent donc d'ores et déjà des solutions afin d'obtenir plus de contrôle sur ce phénomène de société. La labellisation des firmes ayant un comportement responsable vis-à-vis des données personnelles est une option, qui permettrait d'établir une relation de confiance entre les entreprises et les consommateurs. Les professionnels ont un avantage, à savoir la connaissance de l'usage fait des données personnelles — ce qui reste plutôt vague pour les gouvernants et les gouvernés.

Le contrôle de cette certification serait effectué par les États, qui vérifieraient que les entreprises appliquent bien leur politique de confidentialité. Les entreprises labellisées pourraient avoir une hégémonie supplémentaire, qui permettrait peut-être à terme de contourner l'aura de certains géants tels que Google, à qui une telle certification ne serait pas nécessairement conférée.[239]

Ce procédé existe déjà puisque la CNIL délivre des labels authentifiants. Avec l'entrée en vigueur du règlement européen, à compter du 25 mai 2018, l'autorité de régulation élabore et approuve les procédés de certification qui seront délivrés par un organisme national d'accréditation. Cet indicateur témoigne d'un haut niveau de protection des données et d'un service de qualité, qui permet aux utilisateurs d'avoir confiance. En outre, la CNIL étant une autorité administrative indépendante rattachée au gouvernement, elle permet à l'État français de légitimer son statut de protecteur des individus.

Les gouvernements de tous pays, mais plus particulièrement de l'Union Européenne, font face à ce que l'on pourrait appeler un rééquilibrage des pouvoirs — et cela, bien qu'inexorable, était prévisible. « À l'échelon mondial, l'effet le plus significatif de la banalisation des technologies de la communication sera la redistribution vers l'individu des pouvoirs aujourd'hui détenus par les États et les institutions ».[240]

En effet, les outils technologiques, et plus particulièrement les objets connectés susceptibles de traiter des données personnelles, entrent dans les mœurs — se faisant, les individus commencent à les maitriser parfois mieux que les gouvernants eux-mêmes, instaurant une sorte de légitimité populaire sur ces derniers. C'est la raison pour laquelle les États répressifs sont très peu enclins à l'usage libre de la technologie.

La Chine connaît par exemple une pratique pourtant peu portée au grand public : les *50 cents people*. Une pratique du gouvernement consiste à rémunérer environ 50 centimes le post d'un message sur le net, favorable à la politique du gouvernement, ou en réponse à des opposants politiques. Ces messages constituent évidemment une propagande étatique, qui a été mise en place dès lors que le pays a compris la puissance du numérique.

---

[239] ROCHELANDET (F.), *op. cit.,* pp. 38-66.

[240] SCHMIDT (E.), et COHEN (J.), *À nous d'écrire l'avenir*, éd. Denoël, 2013, pp. 16-18.

Une étude réalisée par les universités d'Harvard, de Stanford et de San Diego estime que le gouvernement chinois fabriquerait chaque année l'équivalent de 488 millions de post sur les réseaux sociaux.[241] L'internet devient donc un espace particulier, prisé pour son influence, mais sur lequel l'État n'a pas les pleins pouvoirs, car de nombreux acteurs le concurrencent.

Paragraphe 2. L'affaiblissement de l'État par des acteurs extérieurs

L'État se trouve affaibli conjointement dans sa position de protecteur, par les GAFA, et par les individus. Il l'est d'abord par les GAFA, car désormais la sécurisation ne passe plus par les mêmes acteurs. Autrefois délivré par les services de la Poste, le courrier l'est aujourd'hui par l'intermédiaire d'une boite mail, et d'un hébergeur. Il y a déjà une transmutation : d'une personne physique, la responsabilité a été transférée à une personne morale. « Les institutions qui, traditionnellement, assurent la confiance et la sécurité des échanges (L'État, la Poste, les banques, etc.) ne sauraient jouer le même rôle sur internet. Ils s'y trouvent en effet supplantés par les grands opérateurs, au premier desquels les "GAFA" ».[242]

En outre, les GAFA sont souvent la cause de préoccupations juridiques entravant la résolution d'affaires complexes. Un réel problème émerge pour les preuves numériques, qui sont parfois la clé de cas délicats, notamment à la suite d'évènements terroristes. En effet, certaines entreprises font barrière à la délivrance de certaines informations : les données de souscription, délivrées à l'inscription, les données de connexion et les données de contenus, c'est-à-dire la teneur des messages. La Commission Européenne travaille d'ailleurs afin de présenter un texte visant une circulation plus rapide des informations entre les États. Les États-Unis sont généralement à l'origine des conflits en la matière, ayant sur leur territoire la majorité des serveurs des applications et des réseaux mis en cause.

La procédure de requête d'informations est très longue et fastueuse, et aucune obligation n'est imposée aux GAFA quant à la délivrance de ces dernières, causant parfois des silences judiciaires et empêchant la résolution d'affaires. En outre, le Sénat américain a adopté en mars dernier un texte, le *Cloud Act*, qui doit permettre la transmission de ces données via une nouvelle plateforme spécialement dédiée à cet effet, pour tout État signataire d'un traité

---

[241] MOZUR (P.), « In China, Government Workers Push Rosy, Diverting Views Online », *The New York Times,* 19 mai 2016, article en ligne.

[242] CARELY (C.)., et MICHELEZ (E.)., « "Ubérisation" et numérisation ne réussiront pas sans confiance », *Dr. et patr.*, n°254, 1er janv. 2016, pp. 12-15.

bilatéral. Le texte interdit pourtant l'accord avec une structure, visant directement ou non l'Union Européenne, qui prépare en ce sens sa riposte. Comment accepter pour la justice française de ne pas obtenir de réponse à ses requêtes directes aux GAFA pour obtenir des données de connexion, dès lors que les entreprises ne sont pas même forcées de motiver leur absence de réponse ?[243]

L'entraide pénale internationale est encore trop ardue à mettre en œuvre, la procédure trop longue et trop complexe, pour une efficacité relative. La territorialité et les divergences de droit posent un réel problème d'efficience du droit, et témoignent des avantages qu'ont les grandes entreprises du digital sur les États — il existe encore peu de textes internationaux permettant une entraide interétatique avec des résultats probants. Ce n'est pas le seul heurt que les législateurs connaîtront.

Le droit à l'oubli, consacré par l'article 17 du RGPD, pourrait également apporter son lot de difficultés. En effet il entraînerait nécessairement un « cahier des charges », inexistant pour le moment, afin de savoir quel type de données supprimer, dans quels cas, et la prévalence de certaines informations sur d'autres. Aucune législation n'existe en la matière et la réalité a montré que, dans le cas des demandes de déréférencement que connaît par exemple Google, il est impossible de connaître les raisons d'un accord ou d'un refus de la société. Sur quels fondements prend-elle sa décision ? Pas sur des fondements juridiques.[244]

Mais l'État est également concurrencé par le développement d'un sens critique des utilisateurs. Face à la facilité de propagande de fausses informations, et la manipulation des masses plus qu'aisée, une certaine méfiance des utilisateurs est née, qui tend à s'amplifier au fil des années. Cela se peut remarquer dans les services et les applications proposées par le numérique, de plus en plus basés sur la confiance inter-individus : les commentaires des uns fondent la confiance des autres, défiant ainsi de plus en plus la légitimité gouvernementale.

Enfin, d'un point de vue plus technique, les gouvernants ont beaucoup de difficultés à entrer dans les écosystèmes fermés que créent les GAFA entre leurs produits et les utilisateurs. Depuis les révélations d'Edward Snowden, Apple se défend de respecter la vie privée de ses clients, puisqu'elle a changé son processus de stockage des informations, contenues désormais dans le smartphone et non dans des serveurs délocalisés.

Ce qui est qualifié d'écosystème fermé est en réalité un lien qui unit l'utilisateur et son produit, à tel point que le droit n'a pas d'effet sur cette proximité. L'aspect ludique de ces produits permet de gagner l'attachement indéfectible du consommateur et de légitimer ainsi la collecte quasi-constante des données.[245]

---

[243] M. (U.), et E (V.), « La guerre discrète de la preuve numérique », *Le Monde*, 17 avr. 2018, p. 10.

[244] MERLAND (L.), « L'identité civile des personnes : "Is big data beautiful ?" », *RLDI*, 1er déc. 2015, n°121, pp. 37-39.

[245] JOUX (A.), « L'intelligence artificielle favorise les écosystèmes contrôlés de terminaux », *La REM*, hiver 2017-2018, n°45, article en ligne.

Les enceintes connectées commencent par exemple à se démocratiser, objets initialement utilisés pour une diffusion musicale, mais dont l'ensemble des fonctions est décliné. Ces outils devenant des interfaces privilégiées, en accès direct avec le consommateur et son habitat, il est très ardu pour le droit de pénétrer dans ces sphères. Le cadre global de protection qu'il pose n'est pas suffisamment à la portée des utilisateurs pour que ceux-ci l'aient à l'esprit lors de l'utilisation de ces objets, malgré des tentatives de sensibilisation croissantes.

Il en va de même dans l'arbitraire des applications. Les systèmes d'exploitation d'Apple ne fonctionnent efficacement qu'avec Safari, là où les systèmes Windows installent internet Explorer. Les smartphones Androïd sont eux aussi assujettis à comprendre la panoplie presque complète des applications mobiles de Google. Tout cet écosystème financier est basé sur la collecte des données personnelles, mais fonctionne en partie parce qu'il a été légitimé et même plébiscité par les individus eux-mêmes, faisant parfois fi des garanties que s'efforcent de maintenir en place les gouvernements. Tous ces éléments de poids freinent la récupération étatique de la souveraineté des États, démunis d'arguments commerciaux pour influencer les citoyens.

Section 2. La récupération étatique progressive de la souveraineté numérique

Les États semblent avoir du mal à récupérer le pouvoir sur leur souveraineté, et pour cause — internet a révolutionné les espaces et les frontières. *De facto*, s'il est si dur pour les gouvernements de réguler cet espace, c'est qu'il est à l'origine d'un principe de liberté. Prenons l'exemple du *deep web*. Ce terme désigne l'ensemble des contenus disponibles en ligne mais non-référencés par les moteurs de recherche traditionnels, car accessibles uniquement par des moyens détournés et par l'utilisation d'un proxy particulier. Connu à tort pour ses dérives criminelles dues à l'anonymat qu'il garantit, sa fonction première était en réalité de sécuriser le web.

En effet, lors de sa création, ses utilisateurs étaient majoritairement des chercheurs désireux de protéger leurs travaux, car le *deep web* garantit un anonymat complet : les adresses IP ne sont pas reconnues, la traçabilité est quasiment impossible et les historiques de recherche ne sont pas enregistrés. Des organismes tels que la NSA et le FBI y mènent également des projets confidentiels. L'espace numérique avait donc pour ambition de créer un espace sécurisé, dans lequel seules les lois des utilisateurs s'appliquaient, qui se réglementait en autonomie et se suffisait à lui-même.[246]

[246] KRAMER (C.), *Deep web, All the mysteries and secret behind the hidden side of the internet*, 2014, Cultura, 1ère éd., p. 14.

Le numérique est un espace différent, qui ne connaît pas de frontières, et qui pose des problèmes de territorialisation — il n'a rien de semblable au territoire étatique sur lequel l'État applique sa puissance juridique en toute légitimité. Il s'agit d'un espace qui s'est créé seul et ce nouveau terrain est inconnu pour les gouvernements et pour les législateurs, ce qui explique la difficulté à réglementer toutes les branches du web.

« Il n'y a rien de commun entre l'internet et l'espace aérien, spatial ou maritime. Le Réseau est une création technique proprement artificielle, dont la nature est directement influencée par le comportement de ses acteurs. Mieux encore, son architecture même est le fruit de choix scientifiques qui conditionnent sa capacité générale à prendre en compte des mécanismes de contrôle ».[247] Malgré cette divergence structurelle, les États semblent bien décidés à trouver des moyens de s'approprier cet espace et à ne pas le laisser hors du droit, d'où le développement de nombreuses initiatives.

Paragraphe 1. Le marché unique numérique : l'initiative européenne

L'une des solutions envisageables afin que les États récupèrent dans la totalité leur souveraineté numérique serait de prendre appui sur les initiatives européennes. Tout d'abord, l'entrée en vigueur du RGPD semble avoir engendré une prise de conscience des acteurs majeurs du numérique — les réseaux sociaux, les applications utilisant la géolocalisation, ou les sites de commerce électronique commencent déjà à informer les utilisateurs de leurs nouvelles obligations —, prise de conscience que les États pourraient ériger en un levier d'action sur ces derniers.

En outre, depuis mai 2015, la Commission Européenne a lancé un projet de marché unique numérique — pour lequel des consultations citoyennes sont toujours d'actualité. Cette stratégie est axée autour de trois piliers : l'accès aux services de commerce électronique au sein de toute l'Union, la sécurisation des réseaux et des services, et l'optimisation économique du numérique.[248] Outre les effets positifs sur le droit, la Commission estime qu'un tel effacement des barrières engendrerait 415 milliards d'euros de bénéfice à l'Union Européenne. L'une des propositions émises estime judicieux de créer un principe de libre-circulation des données non personnelles au sein des membres.[249]

---

[247] ROJINSKY (C.), « Cyberespace et nouvelles régulations technologiques », *D.*, 2001, pp. 844-847.

[248] COSTES (L.) [dir.], « Un marché unique numérique pour l'Europe : 16 initiatives de la Commission », *RLDI*, n°115, 1er mai 2015, p. 25.

[249] Commission Européenne, « Marché unique numérique : supprimer les entraves pour exploiter pleinement les possibilités offertes par internet », article en ligne.

L'idée est intéressante, en ce qu'elle permettrait naturellement d'utiliser à souhait les données personnelles au sein de l'espace commercial uni que forme l'Union, afin d'effacer les barrières entre les acteurs économiques, qui retiennent parfois pour eux leurs bases de données. En 2017, le Conseil national du numérique a pourtant soulevé certaines objections quant à la création d'un tel principe, premièrement quant au terme de « données non-personnelles » — au vu de la difficulté de rendre efficiente l'anonymisation totale des données, il est une éventualité non négligeable où toutes les données finiraient par être échangées sur le territoire européen. De plus, cela pourrait entrouvrir une porte à d'autres accords de libre-échange, afin que ces données non-personnelles transitent vers des pays étrangers : ce qui, *de facto*, contreviendrait à l'esprit même du règlement européen qui cherche à rehausser ce niveau de protection.[250]

Répondant à ces doutes, la Commission présentait en janvier 2018 un rapport sur l'avancement du projet. Selon les rapporteurs, les députés Éric Bothorel et Constance Le Grip, « les restrictions nationales injustifiées à la circulation de ces données, la localisation forcée des données en fonction de considérations stratégiques parfois faussées sont autant d'obstacles à la formation d'ensembles de données susceptibles d'être ensuite traitées par des entreprises européennes et, partant, contribuer à leur croissance ».[251]

Une autre solution possible pourrait être la création d'une institution centralisant les données et supervisant les réglementations en la matière — et qui pourrait avoir comme base de départ en France la CNIL. En effet, pour certains auteurs, ce ne peut être que par ce biais que les États retrouveraient leur souveraineté numérique, car tout part d'une mauvaise définition de la donnée personnelle. Autrefois conçue comme un élément à part, délivrant une information précise sur une personne particulière, elle ne peut être aujourd'hui qu'appréhendée dans son ensemble, c'est-à-dire un réseau de données qui, mises bout à bout, permettent de délivrer un portrait quasi fidèle d'une personne.

Cela engendrerait une nécessité de délivrer des droits individuels, mais également collectifs, sur ces réseaux de données, qui répondraient alors à l'article 714 du Code civil : « Il est des choses qui n'appartiennent à personne et dont l'usage est commun à tous ». Chaque individu disposerait des prérogatives habituelles, telles qu'un droit de retrait, un droit de rectification ou un droit à l'oubli — mais il existerait en sus un « contrôle démocratique et souverain » sur la totalité de ces ensembles.[252]

---

[250] COSTES (L.), « Éclairage », *RLDI*, n°137, 1er mai 2017, p. 9.

[251] COSTES (L.) [dir.], « Assemblée nationale : rapport d'information sur le marché unique numérique », *RLDI*, n°144, 1er jan. 2018, pp. 37-38.

[252] BELLANGER (P.), « Les données personnelles : une question de souveraineté », *Le Débat*, 2015/1, n°183, pp. 14-25.

Paragraphe 2. Les initiatives étatiques commerciales

D'autres possibilités émergent de part et d'autre des esprits juridiques, dont l'une serait de revenir à la privatisation de certains services. La base de l'économie des GAFA repose sur l'accès à un service gratuit contre la monétisation des données — c'est ce qui leur permet de tels bénéfices. Les utilisateurs ne semblent pas prêts à y renoncer à raison de la place qu'ont pris ces services dans leur vie, mais cherchent constamment à récupérer une souveraineté sur leurs données : l'alternative résiderait dans le retour à certains services payants.

Moins de gratuité pour plus de confidentialité : c'est ce que le juriste Lionel Maurel prône. Cela éviterait de retomber dans le modèle publicitaire qui est à la base des problèmes juridiques en la matière. D'un autre côté, ce système montrerait vite ses failles dans la mesure où il créerait des inégalités, car seuls les individus pouvant payer verraient leur vie protégée, et la marchandisation de la vie privée reste présente malgré tout.[253] Dans l'idée, fondamentalement, s'attaquer au modèle économique publicitaire semble être une solution plus judicieuse que de s'attarder sur les données personnelles en tant que des marchandises. Peut-être serait-il bon de revoir tout le processus de rémunération tirée des publicités.

Ces initiatives sont autant d'idées qui ne pourront, malgré tout, pas être mises en œuvre tant qu'un problème majeur ne sera pas corrigé — en témoigne le récent piratage massif de l'Inde et de ses fichiers nationaux. Les autorités étatiques et les législateurs ne prennent pas le soin de s'entourer de professionnels du numérique, ce qui pourrait pourtant grandement leur apporter. La protection des données personnelles par le droit est une chose ; leur protection par la technique en est une autre.

Ces deux domaines que sont l'ingénierie et le droit sont pour le moment trop étanches, l'un ne s'imprégnant pas suffisamment de l'autre. Il est désormais notoire que les États ont du retard par rapport à l'avancée des technologies, rendant plus ardue leur appréhension des véritables problématiques juridiques qui en naissent. L'appui d'une équipe d'ingénieurs pourrait accélérer la création de mécanismes protecteurs, en éludant directement les cas d'impossibilités techniques, et en révélant instantanément des problèmes que des juristes n'auraient pas nécessairement envisagés.

À l'inverse, le bon accompagnement juridique d'un ingénieur, créateur d'une entreprise ou d'une application conduite à traiter des données personnelles, permettrait sans nul doute d'éviter un grand nombre de conflits potentiels. Prenons pour cela l'exemple du créateur d'un objet connecté médical, dont le fonctionnement nécessiterait l'accès à des données de santé, qui sont considérées comme sensibles. Conseillé par un juriste, celui-ci serait averti antérieurement des mesures techniques de protection qu'il doit mettre en œuvre afin qu'aucune atteinte aux personnes ne puisse lui être reprochée.

---

[253] MAUREL (L.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

En outre, il existe un écueil, potentiellement source d'atteinte à la vie privée, et auquel ni les juristes ni les ingénieurs ne semblent sensibilisés : le risque de piratage. À trop projeter l'identité sur des supports totalement dématérialisés, il devient très aisé de les détourner. Il serait par exemple dramatique dans le cadre d'une ville totalement connectée que les données collectées massivement puissent être dérobées, permettant au pirate d'avoir accès aux informations privées d'une population entière. [254]

Le mélange de ces deux domaines aurait pour avantage de diminuer les contentieux en matière d'exploitation des données personnelles, mais également de permettre aux gouvernements de mieux comprendre les enjeux techniques. La science et le droit sont ici étroitement liés, et il apparaît encore une fois que la protection totale de l'identité numérique ne peut se faire en se bornant à l'étude juridique du concept. Elle est un mélange interdisciplinaire qui implique une connaissance technique, juridique, mais également sociale — ce qui peut laisser à penser qu'une régulation par les individus, adeptes de ces technologies, pourrait apporter pour beaucoup à ce problème de droit.

[254] FINCH (K.), « Welcome to the Metropticon : Protecting Privacy in a Hyperconnected Town », *Fordham Urb. L. J.*, vol. 41, n°5, mars 2016, pp. 1590.

Chapitre 2. Les initiatives individuelles de régulation de l'identité numérique

La succession des énigmes juridiques liées aux données personnelles et à l'identité numérique commence à inquiéter l'opinion publique, précisément car elle en est la première génératrice, et donc la première concernée. Les États, loin pourtant d'être défaitistes, ont la volonté mais pas nécessairement l'arsenal nécessaire pour garantir une protection efficiente des données personnelles aux individus. Face aux géants du numérique, il est difficile de voir émerger des barrières politiques, rajoutant en plus sur l'ardoise de l'équation le poids économique non négligeable de ces entreprises pour les États.

Commercialisation abusive des données, souveraineté parfois contestable des algorithmes, fichage massif des informations, harcèlement publicitaire et commercial : il semble malaisé pour un individu de trouver sa place au sein de ce nouveau monde numérique, et de figer une identité personnelle, afin de pouvoir ensuite la défendre. Les craintes des utilisateurs n'iront pas en s'arrangeant : les techniques de vente agressives ont la dent dure. Les cookies — petites lignes de code que le navigateur intègre afin que les sites puissent proposer de la publicité cité — déposés par Amazon « sont conçus pour durer jusqu'en 2037 », et, « en cliquant sur la photo d'un smartphone Samsung, vous déclenchez une nouvelle rafale de 42 cookies provenant de 28 sources : en trois clics, vous voilà fiché 108 fois par une quarantaine de bases de données ».[255]

Face aux failles existantes en matière de protection des données personnelles, et de l'identité numérique de l'individu, pourquoi celui-ci ne trouverait pas sa place au sein d'un écosystème juridique dont il est une partie intégrale, en agissant également de son fait pour se protéger ?

« Toute société fonctionne à coups de réglages entre les différentes dimensions de la vie sociale, de l'économie, de la politique, de la culture, mais aussi de réglages entre l'intégration et l'exclusion, entre la contribution et la rétribution de chacun : c'est au travers de ces réglages que se construisent les notions de justice et d'équité ».[256]

Des initiatives citoyennes et des propositions de réglementation alternatives aux cadres juridiques existants apparaissent alors. Ces évolutions, face aux nouveaux problèmes juridiques apparaissant de jour en jour, démontrent sans qu'il ne soit besoin de le prouver que l'identité juridique est un concept qui tend à prendre de l'expansion dans notre société. Dès lors, pourquoi sa reconnaissance textuelle n'apparaît pas en France ? Peut-être par sa complexité, et par les multiples disciplines qu'elle recouvre. L'identité numérique a une dimension sociologique,

---

[255] EUDES (Y.), « Comment notre ordinateur nous manipule », *Le Monde Culture et Idées*, 10 avr. 2014, article en ligne.

[256] DE TERSSAC (G.), « La théorie de la régulation sociale : repères introductifs », *Revue Interventions économiques*, n°45/2012, 1er mai 2012, p.1.

sociale, anthropologique, juridique, et éthique. Englober tout cela dans un texte en intégrant la régulation citoyenne semble difficile, mais conduirait sans nul doute à améliorer la protection encore fébrile des données personnelles.

Section 1. La collaboration horizontale, nouvelle garantie de protection de l'identité numérique

Serait-il erroné de penser que la protection des données personnelles serait plus efficace si elle était issue des individus eux-mêmes ? La réponse n'est pas formellement négative. En effet, « la régulation se distingue de la réglementation classique, autoritaire, unilatérale et rigide, peu efficace, inadaptée ; elle s'applique à des domaines que l'État ne souhaite pas ou ne peut pas garder exclusivement dans son giron, parce qu'il n'est pas forcément l'acteur déterminant. Le contexte est celui d'un monde ouvert, mondialisé, concurrentiel où s'affrontent des intérêts opposés ou divergents ».[257] À cette rigidité de l'implacable loi s'oppose la souplesse de la régulation horizontale, qui tend inlassablement à se développer.

Les avantages de la régulation horizontale ne sont pas négligeables à l'heure où les technologies se développent plus vite que jamais. Il est en réalité très peu productif de laisser un groupe d'individus travailler sur des projets de façon isolée, là où une communauté pourrait corriger des éventuelles erreurs par la simple utilisation de ces projets. C'est ce qu'explique Éric Raymond dans un essai sur l'open source. Habitué à travailler sur des projets de logiciels de cette façon, sa manière de penser change radicalement en découvrant Linux, un système d'exploitation.

Décelant une collaboration entre les ingénieurs qu'il dirige et les utilisateurs auquel il propose ses services, il réalise que l'éparpillement des idées et des suggestions est beaucoup plus productif et lui permet de corriger beaucoup plus d'erreurs passées inaperçues. Les versions suivantes de ces logiciels ne cessant de s'améliorer, il abandonne l'idée selon laquelle tout projet se doit d'être totalement structuré et pensé en isolement avant d'être soumis au public, sans que celui-ci ne puisse objecter de retour sur celui-ci.[258]

Cette opposition entre un modèle strict et un modèle souple s'applique au droit, et à plus forte raison à la notion d'identité numérique, car qui mieux que les individus peuvent témoigner des obstacles rencontrés dans la protection de celle-ci ? Le législateur ne peut pas, à lui seul, explorer l'ensemble des problématiques juridiques liées aux données personnelles, et à mesure que les choses évolueront, la consultation et l'action citoyenne deviendront des nécessités.

---

[257] FRAYSSINET (J.), « La régulation de la protection des données personnelles », *Légicom*, 2009/1, n°42, p. 5.

[258] RAYMOND (É.), *La Cathédrale et le Bazar*, 1998, essai en libre consultation, p. 2.

Paragraphe 1. L'implication citoyenne dans la sécurisation des données

Depuis quelques années, un fléau sociétal inonde les réseaux sociaux et cause du tort à la presse : les fausses nouvelles, divulguées par des auteurs peu scrupuleux afin de les monétiser et d'en retirer des bénéfices. Pour autant, les initiatives législatives en la matière ne sont pas inexistantes. La Commission Européenne a lancé, depuis 2017, une consultation publique afin d'adopter un texte en la matière. L'Allemagne a adopté, le 1er janvier 2018, une loi imposant aux plateformes telles que les réseaux sociaux de supprimer tous les contenus illégaux signalés, sous peine de se voir imposer une amende.

En France, la loi du 29 juillet 1881 avait déjà créé un délit de fausses nouvelles, dont l'efficacité est aujourd'hui relative face aux nouveaux moyens de communication. Au vu de la réalité du terrain, le Président français annonçait, en janvier 2018, un projet de loi pour la confiance dans l'information, visant dans ses grandes lignes à rendre la propagation de fausses nouvelles très compliquée, et à dévoiler systématiquement les identités des éditeurs ou des hébergeurs en cause. La possibilité de passer par un juge en référé serait également envisageable.[259]

La volonté étatique de légiférer en la matière est plus que louable, mais des interrogations raisonnables pointent sur l'efficacité de telles mesures. L'information digitalisée est plus que rapide et peut se transmettre en une seconde dans le monde — permettre un recours au juge est une hypothèse satisfaisante dans un État de droit, mais l'est moins dans une société en constante évolution. Même si l'action en référé est la plus rapide dans le système juridique français, elle n'endiguera pas complètement la rapidité de diffusion des informations, qui pourra causer en quelques heures seulement une désinformation du public. Quelle serait alors la solution la plus efficace d'un point de vue juridique ?

Le réseau social Facebook a pris en compte les récentes critiques qui lui avaient été adressées en janvier 2018, après la prolifération de *fake news*, dans le contexte politique du scandale Cambridge Analytica — les fausses informations influencent parfois les esprits les moins alertés de leur existence, allant parfois jusqu'à créer des réactions disproportionnées. C'est ce qui s'est produit en France, et cela s'est manifesté par la décision du réseau de s'allier à huit grands quotidiens — tels que Le Monde, Libération, et même l'AFP — afin de réaliser une veille informationnelle.

Cette volonté a trouvé à se concrétiser par la création d'une plateforme, Check News, au travers de laquelle le réseau social fournit les liens d'informations diverses et variées. Aux quotidiens, ensuite, de vérifier celles qu'ils souhaitent, et de les confirmer ou les infirmer, selon trois degrés : l'information est vraie, fausse, ou contient des éléments partiels de vérité. Facebook s'engage à réduire la visibilité des informations erronées et indique le risque aux

[259] COSTES (L.), « Premiers contours du projet de loi sur "la confiance dans l'information" », *RLDI*, n°145, 1er fév. 2015, pp. 3-4.

utilisateurs qui souhaitent les partager.[260] Le réseau rémunère ce travail de vérification, qui ne comporte aucune obligation quantitative, mais nécessite malgré tout du travail : Libération reconnaît que la rédaction a ainsi pu engager deux journalistes supplémentaires.[261]

La vérification par les professionnels de la presse confère aux informations circulant sur les réseaux sociaux une valeur déontologique et éthique que le législateur ne pourrait lui apporter — en outre, elle est plus rapide et plus efficace qu'une action judiciaire. Face aux évolutions sociétales, la régulation par les acteurs du milieu semble plus aisée, grâce à la compréhension du système qu'ils ont, et de leur aisance à corriger les erreurs de parcours. À l'image de ce sujet qu'est l'information, la régulation verticale pourrait fonctionner à pleine efficience dans la protection des données personnelles. En ce sens, de nombreuses initiatives citoyennes ont vu le jour.

En 2005 est créé Faroo, un logiciel à installer directement sur le navigateur internet, donnant accès à un moteur de recherche, un peu différent de ceux utilisés habituellement. En effet, celui-ci propose une architecture technique différente, fonctionnant sur la base du *peer-to-peer*.[262] Ce mode d'organisation est « la dynamique humaine intersubjective à l'œuvre dans les réseaux distribués ».[263] Ces réseaux distribués sont constitués de participants, traditionnellement appelés des « nœuds », mais qui n'ont pas d'obligation d'exister, et sont libres de participer ou non à l'échange.

En outre, il n'existe aucune autorité de contrôle à qui rendre des comptes. L'objectif commun qui réunit les membres d'un tel réseau est la production d'un objet social utile à tous. Traditionnellement, le *peer-to-peer* fait écho aux téléchargements illégaux d'œuvres d'artistes, en audiovisuel ou en audiophonie, alors qu'il recouvre une réalité bien plus large, et pourrait trouver à s'appliquer dans de nombreux autres domaines. Le logiciel Skype fonctionnait d'ailleurs initialement sur la base du *peer-to-peer*, tout comme de nombreuses monnaies virtuelles telles que le Bitcoin.

Les GAFA que nous utilisons traditionnellement utilisent une architecture informatique basée sur une relation entre un client et un serveur, où les ressources des premiers font fonctionner le second. Le *peer-to-peer*, à l'inverse, est un système de mise en relation des individus, qui se partagent entre eux des contenus ou des informations. C'est une architecture différente et moins connue, mais qui gagnerait pourtant à l'être plus.

---

[260] DELCAMBRE (A.), « Huit médias français s'allient à Facebook contre les "fake news", *Le Monde*, 6 fév. 2017, article en ligne.

[261] MATHIOT (C.), « Est-il vrai que Facebook rémunère "Le Monde" et "Libération" pour aider à trier les fake news ? », *Libération*, 8 jan. 2010, article en ligne.

[262] NEEDLEMAN (R.), « Faroo makes your PC a searchbot », *Cnet*, 17 sept. 2017, article en ligne.

[263] BAUWENS (M.), et SUSSAN (R.), « Le *peer-to-peer* : nouvelle formation sociale, nouveau modèle civilisationnel », *Revue du MAUSS*, 2005/2, n°26, p. 194.

En effet, l'utiliser dans un service internet, tel que le moteur de recherche, permettrait de modifier les rapports habituels existant entre les opérateurs de réseaux et les utilisateurs — c'est ce qu'a tenté de démontrer Edward Snowden en dénonçant les failles informatiques de la sécurité nationale américaine, car il était trop facile d'accéder aux données des utilisateurs.[264]

Le logiciel Faroo fonctionne ainsi, en proposant aux individus de partager entre eux les informations. Cette architecture permet également d'intégrer directement la *privacy by design*, « principe techno-juridique selon lequel toute technologie exploitant les données personnelles doit intégrer la protection de la vie privée à partir des premières phases de sa conception, et s'y conformer tout au long de son cycle de vie » — et en poussant la construction plus loin, il pourrait même devenir un *privacy by architecture.*[265]

D'autres initiatives ont vu le jour en ce sens, à l'image du réseau social diaspora*, permettant les mêmes fonctionnalités que Facebook — partage de contenus, portefeuille de contenus, lien avec les autres comptes sociaux — mais sans revendre les informations des utilisateurs. Les serveurs sont délocalisés, c'est-à-dire qu'au lieu de contraindre l'utilisateur à accéder au site par un serveur unique — twitter.com, par exemple —, celui-ci est libre d'en choisir un qui lui soit propre, et qu'il sait éthique en matière de données personnelles.

Cette proposition architecturale et organisationnelle est intéressante en ce qu'elle répondrait naturellement à l'exigence du RGPD, qui prévoit en son article 25 que « le responsable de traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des donnée ». L'usager récupère une partie de sa force et de son utilité, puisqu'il est désormais acteur du réseau.

Si d'autres recherchent les mêmes choses que lui, il pourra apporter ses réponses. Ainsi, l'on évite d'enregistrer les préférences des gens, pour aller vers un partage massif et communautaire des recherches et des solutions. Cela évite « d'encrypter l'information » sur l'individu. Mieux encore, cela supprime l'intérêt principal des GAFA : connaître les préférences des personnes afin de leur proposer des services ou des informations. La donnée personnelle perdrait sa valeur économique et le marché qui en est né n'aurait plus de raison d'être.[266]

En outre, l'absence d'unité de contrôle qui centraliserait les informations, et rendrait la conservation des informations impossibles, semble être un argument supplémentaire quant au développement de tels services. Pour autant, il existe peu de sensibilisation à ces modèles, donc

---

[264] MUSIANI (F.), « Les architectures P2P : une solution européenne originale pour la protection des données personnelles ? », *Réseaux*, 2015/1, n°189, pp. 50-52.

[265] MUSIANI (F.), *op. cit.,* p. 56.

[266] MUSIANI (F.), *op. cit.,* p. 59.

leur utilisation reste très faible, et il demeure compliqué de concurrencer les GAFA, dont l'usage est rentré massivement dans les mœurs.

Qui plus est, il ne faudrait pas tomber dans la problématique inverse, à savoir l'inexploitation des données personnelles qui, utilisées avec éthique et dans le respect de la loi, conduisent parfois à la création de services et d'applications plébiscités par le grand public et utiles au quotidien. Néanmoins, la décentralisation des services numériques pourrait être envisagée comme une solution, tant au niveau français qu'au niveau européen.[267]

Enfin, argument final en faveur d'une consécration du *peer-to-peer* : l'absence de serveurs délocalisés à l'étranger répondrait à une problématique environnementale trop souvent oubliée dans les questionnements liés au digital. Le stockage en nuage, ou *cloud computing*, est bien réel, et les centres de données de plus en plus grands deviennent de plus en plus énergivores. Le secteur du numérique représentait, en 2015, 10% de la production électrique mondiale. 50% de la dépense énergétique des centres de données est liée au refroidissement constant des serveurs, et le streaming n'est pas en reste : la consommation de vidéo en ligne très plébiscitée, comme un succès sur YouTube, peut consommer l'équivalent de la production d'une petite centrale électrique.[268]

[267] MUSIANI (F.), *op.cit.,* pp. 65-68.

[268] SERMONDADAZ (S.), « Numérique et écologie : les data centers, des gouffres énergétiques ? », *Sciences et avenir*, 9 mars 2018, article en ligne.

Paragraphe 2. L'émergence d'actions de consommateurs

Une autre solution, moins juridique, mais qui pourrait porter ses fruits, vise à atteindre l'e-réputation des grands acteurs du numérique. Il émerge une véritable rébellion des consommateurs qui s'unissent et utilisent le digital pour faire valoir leurs droits. L'utilisation des bloqueurs de publicité — petites extensions du navigateur qui permettent de ne plus afficher les sollicitations commerciales — a augmenté de 20% en 2016.[269] Certaines marques font désormais face à des offensives groupées sur leurs pages réseaux, ou sur les pages réservées aux avis des consommateurs.

Il est désormais une réalité que les grands groupes ne peuvent éviter, et pour laquelle il n'est pas rare de voir des employés attitrés à la réponse au consommateur et au service après-vente en ligne. La e-réputation est devenue essentielle et les avis sur le web pouvant vite devenir viraux, il est essentiel pour une entreprise de les endiguer ou d'avoir une réponse à amener aux clients mécontents. L'avis d'une personne ayant eu un souci n'importe que lorsqu'elle rencontre d'autres clients dans son cas, et le rapport de force entre la plateforme et les clients s'en trouve immédiatement redistribué.[270]

« Dans l'espace globalisé contemporain, où disparaissent les souverainetés nationales et émergent des pouvoirs incontrôlables, les droits fondamentaux représentent le seul contrepoids visible dont disposent les citoyens ».[271] Les frontières tendent à s'effacer avec l'apparition des technologies et c'est une chance pour les individus que de récupérer un peu de leur légitimité à agir. Utiliser la liberté d'expression pour dénoncer les abus des entreprises en position de force devient donc un nouvel atout pour l'individu. Ce mouvement pourrait être qualifié « d'interconnexion collaborative », puisque les individus travaillent de concert afin de ne plus laisser régner les médias ou l'État. « Contestation de l'expertise, compétence des incompétents, sagesse des foules : nos doubles numériques réclament l'instauration d'un Nouveau Régime, ou qu'on repose à tout le moins la question de la démocratie ».[272]

Ce pouvoir d'expression a déjà fait ses preuves en matière juridique, plus précisément sur les traitements de données — preuve d'une certaine conscientisation émergeante. En 2008

---

[269] PEZ-PÉRARD (V.), LANDREAU (I.), et LÉGER (L.), « Les aspects socio-économiques et éthiques des données personnelles », Partie 1, p. 36, *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, GénérationLibre, rapport numérisé, janv. 2018, 148p.

[270] ROUBAUDI (K.), « E-réputation : quels risques pour les entreprises et les particuliers ? », *Rev. Lamy. dr. aff.*, n°87, 1er nov. 2013, pp. 113-115.

[271] RODOTA (S.), *op. cit.,* pp. 38-66.

[272] MERZEAU (L.), « Habiter l'hypersphère », *Documentaliste-Sciences de l'Information* 2010, vol. 47, pp. 30- 31.

intervient une réforme démantelant les Renseignements généraux français. Pour centraliser les informations sur les personnes déjà collectées, deux fichiers sont créés : EDVIGE et CRISTINA. Le premier était de libre accès au public qui, après avoir été lu, avait entraîné une mobilisation massive : 328 associations et plus de 46.000 personnes signaient une pétition pour que le fichier soit retiré — le Gouvernement avait cédé.

Le texte prévoyait notamment de « centraliser et d'analyser les informations relatives aux personnes physiques ou morales ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif, sous condition que ces informations soient nécessaires au Gouvernement ou à ses représentants pour l'exercice de leurs responsabilités ».[273]

Une telle formulation aurait permis de faire figurer au sein de ce fichier des informations de santé, ou d'orientation sexuelle, sans que n'y soit pour autant développée la question de la protection de celles-ci. La CNIL elle-même avait émis des objections quant à la clarté du texte, qui fut modifié et adopté un an plus tard, après qu'elle eût vérifié la présence de garanties nécessaires aux individus. Le fichier CRISTINA, en revanche, ne sera pas l'objet de contestations et pour cause : il a bénéficié d'une exemption de publication.

En effet, ce fichier est classé secret défense, comme le prévoit l'article 26. III de la loi du 6 janvier 1978, qui dispose que : « certains traitements […] peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission ».

Pourtant, ce fichier est bien plus contrôlant sur les données personnelles que ne l'était son homologue : aucun organisme, pas même la CNIL, n'a de droit regard sur celui-ci. Mais, abstraction faite de cette exception, justifiée par la sécurité nationale, le pouvoir des individus regroupés peut être parfois une influence considérable pour un Gouvernement.

Ces actions de groupe abouties prouvent bien qu'il y a désormais une dimension sociale dans la protection des données personnelles, que le système juridique doit pouvoir accueillir. Selon la présidente de la CNIL, Isabelle Falque-Perrotin, la dimension collective des données personnelles n'est pas suffisante. Il est nécessaire que les droits d'accès et de portabilité soient, par exemple, plus mobilisés par les citoyens.[274]

Le RGPD contient en lui les prémices d'éléments de gestion orientée vers les actions sociales. L'article 80 dispose en effet qu'il est possible de « mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et est actif dans le domaine de la protection des droits et libertés des personnes concernées […]

---

[273] MANDRAUD (I)., « Edvige, Cristina, Ardoise : la difficile mobilisation contre les fichiers de police », *Le Monde*, 24 juil. 2008, article en ligne.

[274] FALQUE-PIERROTIN (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

pour qu'il introduise une réclamation en son nom, exerce en son nom les droits visés aux articles 77, 78 et 79 et exerce en son nom le droit d'obtenir réparation ».

Cette possibilité semble à première vue intéressante du point de vue de l'efficacité du droit, tant les actions en la matière sont peu portées par les individus isolés — l'encadrement par une association ou par un organisme reconnu pourrait conduire à une protection récurrente en cas de litige. Mais le règlement n'impose aux États que de garantir la possibilité pour une association de « déposer une réclamation » — le pouvoir de demander réparation du préjudice ou d'agir sans mandat échouera au bon vouloir des Gouvernements, ce qui créera nécessairement des disparités à l'échelle européenne.[275]

Il existe en outre une forme de volonté européenne émergeante, au vu de certaines actions, et tout particulièrement dans la mouvance de Maximilian Schrems, qui ne s'est pas arrêté à l'invalidation du *Safe Harbour* — décision adoptée en 2000 par la Commission Européenne, qui reconnaissait un niveau de protection suffisant aux États-Unis pour accepter que les données des résidents européens y soient transférées, et remplacée en 2016 par le *Privacy Shield*. En effet, Max Schrems, résident autrichien et doctorant sur le sujet, se trouve opposé dans un litige au commissaire à la protection des données, qui avait refusé de donner suite à une plainte concernant l'envoi des données personnelles sur des serveurs américains.

De ce litige était née une question préjudicielle posée à la Cour de Justice de l'Union Européenne quant à la réelle efficacité du *Safe Harbour*, au regard notamment des évènements qui venaient à peined'être dénoncés par Edward Snowden. Face à la réalité technique et au manque de garanties protectrices, la Cour avait déclaré l'accord invalide au sens du droit européen.[276]

En janvier 2018, le combat juridique contre le réseau social prenait une nouvelle tournure : Maximilian Schrems s'attaque à Facebook Ireland Limited, afin que lui soit reconnue la qualification de consommateur dans sa relation contractuelle avec l'entreprise — et ce afin que sa juridiction étatique ait vocation à devenir la juridiction internationale en cas de conflit. En effet, l'article 16 du règlement « Bruxelles I » dispose que « l'action intentée par un consommateur contre l'autre partie au contrat peut être portée soit devant les tribunaux de l'État membre sur le territoire duquel est domiciliée cette partie, soit devant le tribunal du lieu où le consommateur est domicilié ».[277]

La qualification de consommateur lui a été reconnue par la Cour de Justice, qui considère que le fait d'utiliser sa page Facebook personnelle comme un levier de diffusion de ses activités et de ses actions ne suffisait pas à prouver une utilisation professionnelle. Cette avancée majeure permettra à d'autres individus de se voir attribuer la qualité de consommateur,

---

[275] MATTATIA (F.), et MORDELET (F.), « La mise en œuvre du RGPD au prisme du risque juridique », *RLDI*, n°140, 1er août 2017, p. 61.

[276] CJUE, Gr. Ch., n°C-362/14, 6 oct. 2015, Maximilian Schrems KG c. Data Protection Commissioner.

[277] Art. 16, Règlement (CE) n°44/2001, 22 déc. 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.

afin de résoudre peut-être plus aisément les litiges avec l'entreprise. En revanche, la seconde prétention de Maximilian Schrems, qui tenait à la reconnaissance de cette même qualité à sept personnes lui ayant cédé leurs droits pour cette action, a été rejetée par la Haute juridiction, et pour cause : la protection du consommateur ne se peut faire qu'individuellement, et pas par le biais d'un recours collectif.[278]

Malgré cette victoire en demi-teinte, il est louable qu'une telle reconnaissance ait eu lieu de la part des instances juridiques européennes, car il existe désormais un modèle pour les potentiels individus amenés à se retrouver dans une telle situation. L'existence de droits et d'un arsenal juridique pour les défendre n'implique pas nécessairement que celui-ci soit utilisé, et c'est ici que le bât blesse — les droits d'accès, de portabilité, de rectification, sont encore très peu mobilisés par les citoyens. Pour renforcer ce courant d'action individuelle qui tend à s'intensifier, Maximilian Schrems a également créé une association, NOYD,[279] afin de dénoncer les pratiques illégales de certaines entreprises.

Composée d'experts de la protection de la vie privée, le collectif vise à résoudre la plupart des conflits par des moyens extra-juridiques tels que la médiation ou l'arbitrage, mais se dit prêt à s'engager devant les tribunaux dès que la situation géographique le permet. Ce changement de paradigme illustre bien que désormais, l'individu qui a conscience de ces droits se fédère pour les défendre.[280]

---

[278] PIRONON (V.), « *Maximilan Schrems contre Facebook* : acte II », *AJ Contrat*, 2018, p. 124.

[279] litt. None of your business.

[280] FALQUE-PIERROTIN (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

Section 2. La pluridisciplinarité d'un droit sur l'identité numérique

La question des sources de droit a été, et demeure, une base de réflexion pour les philosophes du droit, mais son étude permet de comprendre en quoi l'identité numérique ne peut être définie qu'à partir d'une seule et unique orientation juridique. Étymologiquement, le mot « source » vient de « sorse », en français médiéval, qui signifie « prendre sa source en ». L'ensemble des sources de droit équivaut aux origines et aux légitimations du droit.

Toutes les sources ne sont pas acceptables et l'on connaît traditionnellement la loi, la coutume, la jurisprudence, et la doctrine. L'ajout d'une nouvelle source peut être considéré comme une argumentation à prouver l'impact de cette dernière sur des cas d'espèces. En outre, les sources du droit sont intrinsèquement liées à sa conception : définir le droit comme étatique exclut par exemple les sources telles que les usages ou la coutume.[281]

La définition textuelle d'un droit sur l'identité numérique étant pour l'instant inexistante, il est tout à fait envisageable d'explorer les contours des sources qui le composeront. Or au vu des évolutions technologiques et sociales qui accompagnent le développement de telles projections digitales, ces sources seront nécessairement diverses. La rigidité dont le droit fait parfois preuve se verra contrainte de s'assouplir car en la matière, une réglementation efficace ne pourra l'être qu'avec une ouverture d'esprit. De nombreuses branches du droit impactent la notion d'identité, et elles ne doivent pas être mises de côté, afin d'aboutir à un droit construit et profitable à tous.

Paragraphe 1. La dimension sociale d'un droit sur l'identité numérique

L'identité numérique ne deviendrait-elle pas une protection sociale ? Il semble que le développement progressif de ces mobilisations citoyennes s'apparente aux modèles existant déjà en droit du travail. Traditionnellement, c'est la situation des employés qui pose souvent des problèmes, auxquels le droit social a apporté un mécanisme de protection qu'est la convention collective : pour protéger l'individuel, pourquoi ne pas passer par le collectif ? L'idéal juridique serait de pouvoir négocier avec les entreprises telles que Facebook, mais, dans l'attente de cet idylle, l'action collective pourrait être une solution.[282]

---

[281] GOLTZBERG (S.), *Les sources du droit*, 2016, PUF, pp. 7-14.

[282] MAUREL (L.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

L'opinion publique collective devient une réelle arme à l'ère du numérique, capable de mettre à mal même les plus grands à l'hégémonie d'apparence inébranlable. En témoigne la tourmente dans laquelle se trouvent, depuis mars 2018, Facebook et son créateur Mark Zuckerberg. Un lanceur d'alerte dénonçait en effet l'extraction illégale de millions de données des utilisateurs, par la société Cambridge Analytica, lors des dernières élections présidentielles américaines et de la campagne pour le Brexit — en vue de prédire les votes et de les influencer.[283]

La société, censée travailler sur la numérisation de ces évènements politiques, est qui plus est attaquée en justice par un professeur américain, afin de la contraindre à révéler l'ensemble des données que la société possède sur lui — et, se faisant, pourrait bien constituer un précédent juridique pour des centaines d'autres utilisateurs bafoués.[284] Le tollé provoqué par cette révélation et le choc pour les utilisateurs a entraîné des réactions inattendues : Mark Zuckerberg se retrouvant, en avril dernier, à rendre des comptes devant le Sénat américain. Malgré les excuses maintes fois répétées quant à la collecte totalement illégale des données, et sa responsabilité assumée pour l'insécurité engendrée sur le réseau, remonter la pente semble compliquée tant la situation est particulière.

À l'heure de l'entrée en vigueur imminente du RGPD, l'entrepreneur a avoué à demi-mot que le modèle européen pouvait en effet garantir une efficience de la protection à laquelle il a échoué.[285] Malgré la réticence des États-Unis à adhérer au modèle de l'Union Européenne, un projet de « *consent act* » va être voté, afin d'imposer un consentement préalable de l'utilisateur à la collecte de ses données.[286] Véritable processus de transformation du droit existant, ou nécessité de réagir rapidement et efficacement face à la colère grondante des utilisateurs bafoués ? Dans les deux cas, l'opinion publique a joué un rôle non négligeable, prouvant bien que désormais, la régulation de l'identité ne peut se faire qu'en intégrant l'avis des premiers concernés dans les relations qu'existaient déjà entre les États et ses grandes entreprises.

En outre, envisager l'aspect social de la protection des données personnelles aurait de nombreux avantages. Certains auteurs considèrent que cet aspect ne peut être écarté, tant il pourrait apporter de solutions aux problèmes actuels. La critique principale qui est adressée au système en vigueur est de ne prendre en compte l'individu que dans son unicité, et non dans un ensemble général qu'est la société.

---

[283] CADWALLADR (C.), et GRAHAM-HARRISON (E.), « Revealed : 50 million Facebook profiles harvested for Cambridge Analytica in major data breech », *The Guardian*, 17 mars 2018, article en ligne.

[284] ALBERT (É.), « Cambridge Analytica : au cœur de la tempête politique, médiatique et judiciaire », *Le Monde*, 23 mars 2018, article en ligne.

[285] HANNE (I.), « Zuckerberg au Sénat : un mea culpa et des questions sans réponses », *Libération*, 11 avr. 2018, article en ligne.

[286] PIQUARD (A.), « Audition du PDG de Facebook, Mark Zuckerberg : une discrète revanche de l'Europe », 11 avr. 2018, *Le Monde,* article en ligne.

S'inspirant du droit de travail et des négociations collectives qui résultent de la cohésion formée par les salariés, les partisans d'une socialisation des données personnelles estiment que « si négociation collective de la vie privée il y a, celle-ci doit être le fait d'une société civile collectivement organisée ».[287] Cela ne semble pas dénué de sens au regard des actions de groupes et des consommateurs qui se multiplient. Il ne manque que de la sensibilisation juridique pour que les utilisateurs se sentent réellement tous concernés par la question des données personnelles.

En outre, les mêmes partisans considèrent qu'il existe un lien plus qu'évident de subordination entre les exploitants des données personnelles et les utilisateurs qui les créent, au regard des déséquilibres conséquents entre la puissance des premiers et l'inanité des seconds. Cette thèse s'appuie en outre sur le critère de la dépendance économique, qui pourrait être démontrée en la matière, auquel cas les négociations collectives permettraient de réajuster ces différends.[288]

Rappelons que l'article 1143 du Code civil dispose qu'il y a « également violence lorsqu'une partie, abusant de l'état de dépendance dans lequel se trouve son cocontractant, obtient de lui un engagement qu'il n'aurait pas souscrit en l'absence d'une telle contrainte et en tire un avantage manifestement excessif ». Quelques doutes peuvent être émis quant à l'applicabilité par un juge d'une telle disposition aux exploitations des données personnelles et pourtant la démonstration des conditions remplies serait possible.

Le consommateur se trouve effectivement dans une situation de dépendance puisqu'il profite d'un service gratuit dont il ne peut se passer — qu'elles qu'en soient les raisons anthropologiques —, et peut-être que si les conditions générales d'utilisation étaient plus claires et moins ardues à lire et à déchiffrer, les utilisateurs les liraient et de fait, n'auraient jamais plébiscité des services tels que Facebook. Quant à l'avantage manifestement excessif, nul besoin est de rappeler les chiffres d'affaires des GAFA, contre les revenus que tirent les individus de leurs données — ce montant étant nul.

La théorie d'une approche sociale des données personnelles ne semble pas si incohérente dans la mesure où il s'agit ici de défendre des droits inhérents aux individus et impactant leur quotidien de manière assez importante, tout comme peut le faire la situation professionnelle. Mais en réalité, déterminer si le droit sur l'identité numérique devrait être un droit social, contractuel, de la consommation, économique, ou même pénal, est une erreur. *Per se*, l'identité numérique est une notion pluridisciplinaire — et par conséquent, le régime de droit qui doit lui être rattaché le sera également.

---

[287] MAUREL (L.), et AUFRÈRE (L.), « Pour une protection sociale des données personnelles », p. 5., article numérique en libre accès.

[288] MAUREL (L.), et AUFRÈRE (L.), *op. cit.,* p. 6.

Paragraphe 2. Vers l'émergence nécessaire d'un droit sur l'identité pluridisciplinaire

Lorsque l'identité est née de la parole des hommes, dans son apparat le plus ancestral, elle n'était qu'un nom. Enrichie au fur et à mesure du temps de nouvelles caractéristiques, elle est devenue progressivement une partie de l'individu, pour en devenir une projection numérique dans la société du XXI^{ème} siècle. Cette projection a connu diverses utilités, et elle est aujourd'hui irriguée et influencée par de nombreuses branches du droit.

La donnée en tant que bien ou objet de droit pose déjà une question fondamentale qui reste pour l'instant ouverte à débat. Elle monopolise ainsi une partie de la doctrine sur la propriété privée, et plus largement encore, sur la *summa divisio* entre les personnes et les choses. Ce volet des questions juridiques en la matière est tellement important qu'il conduit même les critiques de la propriété privée traditionnelle à s'en servir, afin de démontrer son insuffisance.

Les questions économiques relatives à l'exploitation des données posent des problèmes en termes de consommation, puisque la relation qui unit les acteurs du numérique et les individus est souvent déséquilibrée — or il s'agit du but de cette discipline que de réajuster le lien contractuel, trop souvent en défaveur du consommateur. L'ensemble de cette problématique est en adéquation totale avec le développement d'actions de groupes, de mobilisations citoyennes, et la consécration d'une action collective par le règlement européen.

Mais la problématique des données personnelles ne s'arrête pas là. Le droit pénal est également concerné, puisque la loi du 6 janvier 1978 a inclus des dispositions précises dans le Code. Le droit du travail l'est également, puisque, comme évoqué précédemment, la question de la protection des données personnelles peut s'envisager sous un angle social.

Il ne s'agit là pour autant que des potentielles branches du droit ayant trait à la protection des données personnelles, qui, elles, ne sont qu'un élément de l'identité numérique. À l'échelle supérieure, la question de cette notion émergente entraîne des réflexions quant à sa nature. Droit constitutionnel, droit ou liberté fondamentale, droit de l'Homme ? Il existe déjà des composantes de l'identité qui sont protégées par ces catégories souveraines, telles que la vie privée, le droit à l'image, ou le droit à la réputation.

Enfin, de manière plus générale, la notion d'identité ne fait pas appel qu'au domaine juridique. Elle est avant tout une notion sociale, puisqu'elle est intrinsèquement liée à l'individu, et politique, puisqu'elle a permis la constitution des États, par le regroupement des hommes en communautés symbiotiques. L'identité fait appel également à une certaine philosophie, en ce qu'elle n'est pas qu'un caractère descriptif, mais également une vision, un regard extérieur de l'individu sur ce qu'il est. Enfin, son exploitation commerciale et le développement des pratiques qui l'entourent ne sont pas détachables de certaines notions d'économie.

Le Conseil d'État, dans son rapport annuel de 2017, faisait preuve d'une certaine souplesse en prenant en compte des évolutions technologiques n'ayant pas de prime abord d'impact sur le droit, et en s'inspirant de certaines disciplines étrangères au droit administratif,

mais dont l'étude avait permis d'éclairer des questions juridiques sans réponses. À l'instar de la réflexion de la Haute juridiction, il serait sans nul doute judicieux qu'à l'aune de l'émergence d'un droit sur l'identité numérique, celui-ci se voit imprégné de diverses disciplines et d'influences variées. La technologie est un domaine dans lequel il est difficile d'anticiper, et il y est donc nécessaire de se baser sur des constatations de fait — le droit ne se suffisant plus à lui-même dans la lutte pour la protection des identités, la prise en compte de réalités sociales ne sera qu'un bénéfice de taille pour l'élaboration de garanties individuelles performantes.

CONCLUSION

Les gardiens des données personnelles, détenteurs exclusifs et omnipotents de ce pétrole contemporain, que sont aujourd'hui les grandes entreprises du numérique, ont assis leur pouvoir avec force techniques commerciales et tentent désormais quotidiennement d'outrepasser les lois. Force est de constater qu'ils ont à tout le moins permis d'appréhender ce phénomène de société qu'est l'exposition numérique des éléments de la personnalité. Face aux tendances de dévoilement de soi, sont apparues des problématiques sociales, du regard que le sujet de droit se porte, avec bienveillance ou non.

Tout changement de mœurs et d'habitudes a nécessairement des implications juridiques, et l'apparition de telles pratiques a fait émerger un concept social qu'est l'identité numérique, auquel le législateur français ne fait aucune allusion. Or celle-ci est le contenant de nombreuses problématiques juridiques naissantes, puisque s'y rapportent des thèmes d'actualité, tels que les données personnelles ou la protection des libertés fondamentales dans la société numérique.

Il est désormais évident que tout questionnement lié à l'exploitation des données personnelles, à leur commercialisation, mais également à la protection de la vie privée, de l'intimité, du secret — et même de l'utilisation des algorithmes, de l'apparition de la robotique, de l'émergence de quartiers connectés — est intrinsèquement relié à la perception de l'identité dans un espace numérisé.

Par conséquent, chaque préjudice, chaque litige, chaque défaut de définition juridique d'un concept dans l'un ou dans l'autre de ces domaines impliquera nécessairement une facette de l'identité juridique. Pour autant, son absence de reconnaissance textuelle empêche que les prérogatives déjà existantes soient réellement efficaces, tant elles sont éparses — alors que, rassemblées sous la coupe de l'identité numérique, elles pourraient devenir un corpus de droits efficient et puissant.

L'identité numérique et ses agrégats, les données personnelles, sont aujourd'hui le fruit d'une mixité entre diverses sciences humaines, sociales, et mathématiques, d'une conception résultant d'une pluralité d'acteurs, et d'une diversité normative. La consécration d'une telle notion dans le système juridique français impliquerait de prendre en considération ces spécificités afin que le régime qui en découle soit au mieux adapté.

Il n'est plus qu'à espérer qu'une telle reconnaissance voie le jour, mais elle implique une certaine renonciation de la part du législateur et du gouvernement français, tant elle ébranlerait les codes juridiques. Les puissantes firmes du numérique ont déjà pris trop de pouvoir sur les données personnelles, et les États trop de retard et d'inanité face à ces colosses. Il est temps d'y remédier en organisant un corpus de garanties législatives adaptées à ces problématiques émergentes.

Errare humanum est, perseverare diabolicum.

B I B L I O G R A P H I E

I – Ouvrages généraux et spécialisés

- ABBOTT (B.) *Travelling Law-School and Famous Trials (First Lessons in Government and Law)*, Boston, D. Lothrop, 1884, 116p.

- ABOUT (I.), et DENIS (V.), *Histoire de l'identification des personnes*, La Découverte, « Repères », 2010, 128p.

- ANTIPPAS (J.), et BEIGNIER (B.), *La protection de la vie privée*, Hors collection Dalloz, mai 2017, 1062p.

- ATIAS (C.), *Droit civil, Les biens*, 11ème éd., Litec, 2011, 386p.

- ATIAS (C.), *Le droit civil*, 2004/2161, 7ème éd., PUF, 128p.

- BENJAMIN (W.), *L'œuvre d'art à l'époque de sa reproductibilité technique*, Allia, 2017, 94p.

- BOISTEL (A.), *Philosophie du droit*, 1889, t. 1, n° 131 et s., 451p.

- BOLLÉE (S.), et PATAUT (É.), [dir], *L'identité à l'épreuve de la mondialisation*, IRJS Éditions, 2016, 268p.

- BOUT (R.) [dir.], *Lamy Droit économique*, 2018.

- CABRILLAC (R.), *Libertés et droits fondamentaux 2017*, Hors collection Dalloz, mai 2017, 1062p.

- COSTES (L.), et MARCELLIN (S.) [dir.], *Lamy Droit du numérique (Guide)*, 2009.

- CRARY (J.), 24/7 - *Le capitalisme à l'assaut du sommeil*, éd. La Découverte, mai 2014, 180p.

- DE TERSSAC (G.), *La théorie de la régulation sociale de Jean-Daniel Reynaud*, éd. La Découverte, 2003, 448p.

- FINKIELKRAUT (A.), et SORIANO (P.), *Internet, l'inquiétante extase*, Éd. Mille et une nuits, 2001, 93p.

- GOLTZBERG (S.), *Les sources du droit*, 2016, PUF, 128p.

- HERNET (P.), *Les algorithmes*, 2002/2928, 2ème éd., PUF, 128 p.

- KAPLAN (D.)., *Informatique et libertés 2.0*, éd. FYP., 2010, 142p.

- KERDELLANT (C.), *Dans la Google du loup,* Plon, 2017, 226p.

- KRAMER (C.), *Deep web, All the mysteries and secret behind the hidden side of the internet*, 2014, Cultura, 1ère éd., 48p.

- LALOUETTE (J.), *L'État et les cultes, 1789-1905-2005*, 2005, La Découverte, 128p.

- MERCKLÉ (P.), *Sociologie des réseaux sociaux*, 2016, La Découverte, 128p.

- MOURON (P.), et PICCIO (C.) [dir.], *L'ordre public numérique : libertés, propriétés, identités*, 2015, PUAM, 168p.

- RAYMOND (É.), *La Cathédrale et le Bazar*, 1998, essai en libre consultation, 20p.

- REBOUL-MAUPIN (N.), *Droit des biens*, 6ème éd., Dalloz, Hypercours, 764p.

- ROCHELANDET (F.), *Économie des données personnelles et de la vie privée*, La Découverte, 2010, 128p.

- SAVAUX (É.) [dir.], *Rép. civ.*, 2009, actu. 2018, 9444p.

- SCHMIDT (E.), et COHEN (J.), *À nous d'écrire l'avenir*, éd. Denoël, 2013, 384p.

- SIMONNET (D.), *Les 100 mots de l'entreprise*, 2016, PUF, 128p.

- VIVANT (M.) [dir.], *Lamy Droit du numérique,* 2017.

II – Articles, interventions, contributions et dossiers

- ALBERT (É.), « Cambridge Analytica : au cœur de la tempête politique, médiatique et judiciaire », *Le Monde*, 23 mars 2018, article en ligne.

- ANDRÉ (S.), et LALLEMAND (C.), « *Facebook* contre le consommateur français : l'hallali de la clause attributive », *Dalloz IP/IT*, 2016, pp. 214-215.

- ANGWIN (J.), LARSON (J.), MATTU (S.), et KIRCHNER (L.), « Machine Bias », *ProPublica*,23 mai 2016, étude en ligne.

- « An open letter to the United Nations Convention on certain conventional weapons », lettre ouverte, *Future Institute of Life*, disponible en ligne.

- Avis de l'ANSES, « Exposition de la population aux champs électromagnétiques émis par les "compteurs communicants", Rapport d'expertise collective, juin 2017, éd. scientifique, version révisée de l'avis de déc. 2015, 124p.

- BARRAUD (B.) : « Le coup de data permanent : la loi des algorithmes », *RDLF*, chron. n°35, 2017.

- BAUSARDO (T.), « Quel passé pour Prism et Snowden ? », *Vacarme*, 2014/1, n°66, pp. 142- 157.

- BAUWENS (M.), et SUSSAN (R.), « Le *peer-to-peer* : nouvelle formation sociale, nouveau modèle civilisationnel », *Revue du MAUSS*, 2005/2, n°26, pp. 193-210.

- BELLANGER (P.), « Les données personnelles : une question de souveraineté », *Le Débat*, 2015/1, n°183, pp. 14-25.

- BENSOUSSAN (G.), « Éditorial », *Revue d'Histoire de la Shoah*, 2005, n° 183, pp. 5-15.

- BEMBARON (E.), « Axa s'associe à Withings dans la santé connectée », *Le Figaro*, 2 juin 2014, article en ligne.

- BIOY (X.), « L'identité de la personne devant le Conseil Constitutionnel », *Revue française de droit constitutionnel*, 2006/1, n°65, pp. 73-95.

- BLÉRY (C.), « SECURIGREFFE : l'identité numérique judiciaire opposable est née », *JCP G*, n°9-10, 29 févr. 2016, p. 256.

- BOULLAND (P.), « Récolte et usages des données personnelles dans les recherches socio-biographiques du Maitron », *La Gazette des archives*, n°215, 2009, résumé du colloque « Archives et coopération européenne : enjeux, projets et perspectives » et « Les données personnelles, entre fichiers nominatifs et jungle Internet ». pp. 161-168.

- BUAT-MÉNARD (E.), et GIAMBIASI (P.), « La mémoire numérique des décisions judiciaires », *D.*, 2017, pp. 1483-1489.

- CADWALLADR (C.), et GRAHAM-HARRISON (E.), « Revealed : 50 million Facebook profiles harvested for Cambridge Analytica in major data brec », *The Guardian*, 17 mars 2018, article en ligne.

- Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

- CARELY (C.)., et MICHELEZ (E.)., « "Ubérisation" et numérisation ne réussiront pas sans confiance », *Dr. et patr.*, n°254, 1er janv. 2016, pp. 12-15.

- CASTETS-RENARD (C.), « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *RLDI*, n°106, 1er juil. 2014, pp. 68-75.

- CERUZZI (E.), « Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté », *Le temps des médias*, 2012/1, n°18, pp. 15-28.

- CHAMPEAU (G.), « Reconnaître un droit d'auteur aux robots ? L'idée fait son chemin… », *Numérama*, 23 juin 2016, article en ligne.

- CHASTAGNOL (A.), « L'onomastique de type pérégrin dans les cités de la Gaule Narbonnaise », *Mélanges de l'École française de Rome*, 1990, n°2, vol. 2, pp. 573-593.

- CHERIF (A.), « Introduction des nouvelles technologies et changements organisationnels au sein du ministère français des Finances : l'exemple de la mécanographie (des années 1930 aux années 1970) », *Entreprises et Histoires*, 2014/2, n° 75, pp. 24-41.

- CLÉMENT (J-M.), BOUILLIÉ (A.), et FOURÈS (M.), *BDEI*, n°73, 1er jan. 2018, p. 34, note sous TA Montreuil, 7 déc. 2017, n°1700278, *Préfet de la Seine-Saint-Denis.*

- *CNIL, fiche thématique, « Qu'est-ce qu'une donnée de santé ? », article en ligne.*

- COJEAN (A.), « Mychal Bell, rescapé de la justice sudiste », *Le Monde*, 1er oct. 2007, article en ligne.

- Commission Européenne, « Marché unique numérique : supprimer les entraves pour exploiter pleinement les possibilités offertes par internet », article en ligne.

- Conseil d'État, *Le numérique et les droits fondamentaux*, étude annuelle, 2014, 446p.

- COSTES (L.) :

  * « La Silicon Valley vent debout contre le "MuslimBan" », *RLDI*, n° 134, 1er févr. 2017, p. 3.

  * « Premiers contours du projet de loi sur "la confiance dans l'information" », *RLDI*, n°145, 1er fév. 2015, pp. 3-4.

  * « Éclairage », *RLDI*, n°137, 1er mai 2017, p. 9.

  * « Apple vs FBI : confidentialité vs sécurité… », *RLDI*, n°125, 1er avril 2016, p. 3.

  * [dir.], « Un marché unique numérique pour l'Europe : 16 initiatives de la Commission », *RLDI*, n°115, 1er mai 2015, p. 25.

  * [dir.], « Assemblée nationale : rapport d'information sur le marché unique numérique », *RLDI*, n°144, 1er jan. 2018, pp. 37-38.

- D. (L.), *in* Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

- DAOUD (E.), TROUVÉ (M.), et CHAUVIÈRE (E.), « Libertés fondamentales et protection des données personnelles », *Lamy dr. aff.*, n°87, 1er nov. 2013, p. 87.

- DE GROËR (S.), « Condamnation de Facebook par le Tribunal de grande instance de Berlin », *RLDI*, n°146, 1er mars 2018, pp. 62-63.

- DELCAMBRE (A.), « Huit médias français s'allient à Facebook contre les "fake news", *Le Monde*, 6 fév. 2017, article en ligne.

- DENOUËL (J.), et GRANJON (F,) « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie*, vol. 1, n°1, 2010, pp. 25-43.

- Dépêche AFP et Reuters, « Facebook boucle l'achat d'Instagram », *Le Monde*, 23 août 2012, article en ligne.

- Dépêche 6Médias, « GAFA : l'étonnante proposition de Julien Dray », *Le Point*, 14 janv. 2018, article en ligne.

- Dépêche 6Médias, « Facebook : le chiffre d'affaires bondit malgré une baisse du temps d'utilisation », *L'Opinion*, 1er fév. 2018, article en ligne.

- DERIEUX (E.), « Droits de la personnalité et protection des données personnelles face aux médias et à leurs usages », *Légicom*, 2009/2, n°43, pp. 123-138.

- DE TERSSAC (G.), « La théorie de la régulation sociale : repères introductifs », *Revue Interventions économiques*, n°45/2012, 1er mai 2012, pp. 1-18.

- DONDERO (B.), « La justice prédictive : la fin de l'aléa judiciaire ? », *D.*, 2017, pp. 532-538.

- DOWEK (G.), Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

- DUBEY (G.), « Sur quelques enjeux sociaux de l'identification biométrique », *Mouvements*, 2010/2, n° 62, pp. 71-79.

- DUBUC (D.), « Les nudges : incitations vertueuses ou flicage invisible ? », *Usbek & Rica*, 10 oct. 2017, article en ligne.

- DUCOURTIEUX (C.), « L'Union Européenne punit Google d'une amende record de 2,42 milliards d'euros », *Le Monde*, 27 juin 2017, article en ligne.

- ERTZSCHEID (O.), « L'homme, un document comme les autres », *Hermès, La Revue* 2009/1, n° 53, pp. 33-40.

- ESCANDE (P.), « Les taxis autonomes de Google sur la grille de départ », *Le Monde Économie*, 20 déc. 2017, article en ligne.

- EUDES (Y.) :

  * « PredPol, le Big Data au service de la police », *Le Monde*, 22 avr. 2015, article en ligne.

  * « Comment notre ordinateur nous manipule », *Le Monde Culture et Idées*, 10 avr. 2014, article en ligne.

  * Cahier du « Monde », p. 5., *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

- FAGOT (V.), et TUAL (M.), « Intelligence artificielle : ce qu'il faut retenir du rapport de Cédric Villani », *Le Monde*, 28 mars 2018, article en ligne.

- FALQUE-PIERROTIN (I.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

- FARCIS (S.), « Données biométriques : L'inde le doigt dans l'œillère », *Libération*, 30 mars 2018.

- Fiche thématique « Les droits de l'enfant : le droit à l'identité », Unicef, contenu en ligne.

- FIÉVET (C.), « Une vie numérique éternelle en 2067 ? », *Inria*, 12 nov. 2017, article en ligne.

- FINCH (K.), « Welcome to the Metropticon : Protecting Privacy in a Hyperconnected Town », *Fordham Urb. L. J.*, vol. 41, n°5, mars 2016, pp. 1581-1615.

- FORCADE (O.), « Objets, approches et problématiques d'une histoire française du renseignement : un champ historiographique en construction », *Histoire, économie & société,*

2012/2 (31ème année), p. 99-110.

- FORÊT (É.), « Il y aura bientôt plus de morts que de vivants sur Facebook », *France Inter*, 31 oct. 2017, article en ligne.

- FRAYSSINET (J.), « La régulation de la protection des données personnelles », *Légicom*, 2009/1, n°42, p. 5.

- GALLMEISTER (I.), « État et capacité des personnes », *Rép. Civ.*, juin 2016, rub. 38-54.

- GEFFRAY (E.), « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », *Les nouveaux Cahiers du Conseil Constitutionnel*, 1er juin 2016, n°52, p. 7.

- GEORGES (B.), « Macron annonce 1,5 milliards d'euros pour développer l'intelligence artificielle », *Les* Échos, 29 mars 2018, article en ligne.

- GEORGES (F.), « L'identité numérique dans le web 2.0 », *Le mensuel de l'Université,* n°27, juin 2008, article en ligne.

- GODEFROY (L.), « Les algorithmes : quel statut juridique pour quelles responsabilités ? », *Comm. com. élec.*, n°11, nov. 2017, pp. 18-22.

- GIUSTI (J.), NDIAYE (A.), « L'identité numérique, monnaie d'aujourd'hui et rente de demain… », *RLDI*, 1er août 2017, n°140, pp. 56-60.

- GROS (M.), « Polisis, du deep learning pour comprendre les CGU » *Le Monde informatique*, 19 fév. 2018, article en ligne.

- GUITON (A.), « Le scandaleux logiciel espion vendu pour "savoir si son fils est gay" », *Libération*, 22 août 2017, article en ligne.

- GUYADER (A.), « Les enjeux du grand bouleversement », *Pouvoirs*, 2018/1, n°164, éd. Le Seuil, pp. 7-18.

- HANNE (I.), « Zuckerberg au Sénat : un mea culpa et des questions sans réponses », *Libération*, 11 avr. 2018, article en ligne.

- HOURCADE (B.), « Une filiale de Google construit un quartier entier à Toronto », *Usbek & Rica*, 21 oct. 2017, article en ligne.

- ISAAC (H.), « La donnée numérique, bien public ou instrument de profit », *Pouvoirs*, 2018/1, éd. Le Seuil, pp. 75-86.

- JOUX (A.), « L'intelligence artificielle favorise les écosystèmes contrôlés de terminaux », *La REM*, hiver 2017-2018, n°45, article en ligne.

- JUNEAU (S.), « La cyberdépendance : un phénomène en construction », *Déviance et Société*, 2014/3, vol n°38, p. 285.

- KOEHLER (J.), « Fraley v. Facebook : The Right of Publicity in Online Social Network», *Berkeley Technology Law Journal*, 2013, vol. 28, pp. 963-1002.

- KOENIG (G.), « Nous ne voulons pas être de la chair à algorithme ! », *Les Échos*, 27 jan. 2016, article en ligne.

- KOENIG (G.), Introduction, *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, Génération Libre, rapport numérisé.

- LANDREAU (I.) :

* « Pour une approche éthique de la valorisation des données du citoyen », *RLDI*, n° 124, 1er mars 2016, pp. 33-36.

* « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

- LE BILLON (V.), « Compteurs Linky : une bonne affaire pour Enedis », *Les Échos*, 7 fév. 2018, article en ligne.

- LEBRET (M.), « Notre manque de connaissances des algorithmes nous nuit », *Slate*, 24 mars 2015, article en ligne.

- LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, Génération Libre, jan. 2018, rapport numérisé, 148p.

- LEPAGE (A.), « Droits de la personnalité », *Rép. civ,* 2009, actu. 2018.

- LEQUILLERIER (C.), « L'"ubérisation" de la santé », *Dalloz IP/IT*, 2017, p. 155.

- LEVENSON (C.), « Un logiciel censé prédire le risque de récidive aux États-Unis a un problème de racisme », *Slate*, 24 mai 2016, article en ligne.

- LUCAS (A.), et SIRINELLI (P.), « L'originalité en droit d'auteur », *JCP*, n°23, 9 juin 1993, doctr. 3681.

- MANDRAUD (I)., « Edvige, Cristina, Ardoise : la difficile mobilisation contre les fichiers de police », *Le Monde*, 24 juil. 2008, article en ligne.

- MARIN (J.), « L'assureur américain Aetna prévoit d'offrir 500.000 Apple Watch », *Le Monde*, 12 fév. 2018, article en ligne.

- MATHIOT (C.), « Est-il vrai que Facebook rémunère "Le Monde" et "Libération" pour aider à trier les fake news ? », *Libération*, 8 jan. 2010, article en ligne.

- MATTATIA (F.), et MORDELET (F.), « La mise en œuvre du RGPD au prisme du risque juridique », *RLDI*, n°140, 1er août 2017, pp. 61-64.

- MATTATIA (F.), et YAÏCHE (M.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *RLDI*, n°114, 1er avr. 2015, pp. 60- 63.

- MAZEAUD (V.), « La constitutionnalisation du droit au respect de la vie privée », *Nouveaux cahiers du Conseil constitutionnel*, n° 48, juin 2015, pp. 7-20.

- MERLAND (L.), « L'identité civile des personnes : "Is big data beautiful ?" », *RLDI*, 1er déc. 2015, n°121, pp. 37-39.

- MEURIS-GUERRERO (F.), « L'attrait croissant des plateformes numériques », *Comm. com. électr.*, n°9, sept. 2016, p. 52.

- MERZEAU (L.), « Habiter l'hypersphère », *Documentaliste-Sciences de l'Information* 2010, vol. 47, pp. 30-31.

- MAUREL (L.), « À qui confier notre portefeuille de données personnelles ? », Du grain à moudre, *France Inter*, 19 fév. 2018, intervention orale.

- MAUREL (L.), et AUFRÈRE (L.), « Pour une protection sociale des données personnelles », article numérique en libre accès.

- MORIN (V.), « Sophia, robot saoudienne et citoyenne », *Le Monde*, 4 nov. 2017, article en ligne.

- MOUREN (L.), « Des intelligences artificielles ont créé un langage pour communiquer entre elles », *L'Express*, 8 oct. 2016, article en ligne..

- MOURON (P.), « L'identité virtuelle et le droit "sur" l'identité », *RLDI*, n°64, 1er oct. 2010, pp. 58-63.

- MOZUR (P.), « In China, Government Workers Push Rosy, Diverting Views Online », 19 mai 2016, *The New York Times,* article en ligne.

- M. (U.), et E (V.), « La guerre discrète de la preuve numérique », *Le Monde*, 17 avr. 2018, p. 10.

- MUIR WATT (H.), « Gutmann (Daniel) : Le sentiment d'identité (Étude de droit des personnes et de la famille », *Rev. crit. DIP*, 2000, pp. 947-950.

- MUSIANI (F.), « Les architectures P2P : une solution européenne originale pour la protection des données personnelles ? », *Réseaux*, 2015/1, n°189, pp. 47-75.

- NEEDLEMAN (R.), « Faroo makes your PC a searchbot », *Cnet*, 17 sept. 2017, article en ligne.

- NEUER (L.), « Alain Bensoussan : "Il faut construire un droit spécifique aux robots" », *Le Point*, 20 nov. 2017, article en ligne.

- NIENTUS (Z.), « Humans 2.0 : meet the entrepreneur who wants to put a chip in your brain », *The Guardian*, 14 déc. 2017, article en ligne.

- NIMMER B. (M.), « The Right of Publicity », *Law and Contemporary Problems*, 1954, vol. 19, n°2, pp. 203- 223.

- NORA (D.), « Micro-États, villes flottantes : le projet fou des nouveaux maîtres du monde », *Nouvel Obs*, 13 avr. 2014, article en ligne.

- *Notoriété et attentes vis-à-vis des algorithmes*, Sondage IFOP pour la CNIL, jan. 2017.

- OCHOA (N.), « Pour en finir avec l'idée d'un droit de propriété sur les données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, pp. 1157-1174.

- ORSINI (A.), « Au Japon, une start-up lance le paiement par QR Code », *Numerama*, 11 fév. 2017, article en ligne.

- PEDROLETTI (B.), « En Chine, le fichage high-tech des citoyens », *Le Monde*, 11 avr. 2018, article en ligne.

- PEZ-PÉRARD (V.), LANDREAU (I.), et LÉGER (L.), « Les aspects socio-économiques et éthiques des données personnelles », Partie 1, *in* LÉGER (L.) [dir.], *Mes data sont à moi – Pour une patrimonialité des données personnelles*, GénérationLibre, jan. 2018, rapport numérisé, 148p.

- Press release, « Apple Reports First Quarter », 1er fév. 2018, rapport en ligne.

- PIERRE (J.), « Génétique de l'identité numérique », *Les Cahiers du numérique*, 2011/1, vol. 7, pp. 15-19.

- PIRONON (V.), « *Maximilan Schrems contre Facebook* : acte II », *AJ Contrat*, 2018, p. 124.

- PIQUARD (A.), « Audition du PDG de Facebook, Mark Zuckerberg : une discrète revanche de l'Europe », 11 avr. 2018, *Le Monde,* article en ligne.

- PUYUELO (R.), « Journaux "extimes" et communauté de l'anonyme », *EMPAN*, n°176, 2009, pp. 30-36.

- RODOTA (S.), « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements*, 2010, n° 62, pp. 55-70.

- ROJINSKY (C.), « Cyberespace et nouvelles régulations technologiques », *D.*, 2001, pp. 844- 847.

- ROUBAUDI (K.), « E-réputation : quels risques pour les entreprises et les particuliers ? », *Rev. Lamy. dr. aff.*, n°87, 1er nov. 2013, pp. 113-115.

- SAENKO (L.), « Le nouveau délit d'usurpation d'identité numérique », RLDI, n°72, 1er juin 2011, pp. 63-69.

- SERMONDADAZ (S.), « Numérique et écologie : les data centers, des gouffres énergétiques ? », *Sciences et avenir*, 9 mars 2018, article en ligne.

- SMITH (A.), et ANDERSON (M.), « Social Media Use in 2018 », *Pew Research Center*, 1er mars 2018, étude en ligne.

- STEEL (E.), LOCKE (C.), CADMAN (E.), et FREESE (B.), « How much is your personal data worth ? », *Financial Times*, 12 juin 2013, m.à.j 15 juil. 2017, article en ligne.

- THEVENIN (L.), « Santé : Generali va récompenser les bons comportements », *Les Échos*, 6 sept. 2016, article en ligne.

- TRUJILLO (E.), « En Chine, le grand bond en avant de la reconnaissance faciale », *Le Figaro*, 13 déc. 2017, article en ligne.

- TUAL (M.), et LAROUSSERIE (D.), *in* Cahier du « Monde », *Intelligence artificielles : promesses et périls*, n°22696, 31 déc. 2017, 1er et 2 janv. 2018, *Le Monde*, 9p.

- TURRETTINI (É.), « Des "chatbots" pour parler avec les morts », *Le Temps*, 26 fév. 2017, article en ligne.

- TURGIS (S.), « Le "Guide des droits de l'homme pour les utilisateurs d'Internet" du Comité des ministres du Conseil de l'Europe : Vademecum du droit européen de l'internet », *LPA*, 29 août 2014, n°173, p. 7.

- VATICAN (A.) « Le fichier de la surveillance administrative de la ville de Bordeaux, 1945-1995 », *La Gazette des archives*, n°215, 2009, résumé du colloque « Archives et coopération européenne : enjeux, projets et perspectives » et « Les données personnelles, entre fichiers nominatifs et jungle Internet ». pp. 139-148.

- VULBEAU (A.)., « Contrepoint – La Compagnie des machines Bull, de la mécanographie à l'informatique », *Informations sociales*, 2015/3, 144p.

- WAKIM (N.), « Linky : Corinne Lepage et un groupe d'avocats lancent une action collective contre le compteur électrique », *Le Monde*, 11 avr. 2018, article en ligne.

- Anonyme, « Images, lettres et sons », *Vingtième Siècle, Revue d'histoire*, 2012/2, n° 114, pp. 215-231.

- Anonyme, « #NO #SEX – Les mots clefs interdits par Instagram », *Le Monde*, 3 sept. 2013, en ligne.

- Anonyme, « Les 37 projets d'Elon Musk contre les dangers de l'intelligence artificielle », Pixels, *Le Monde*, 6 juil. 2015, article en ligne.

- Anonyme, « La discrimination raciale et le système juridique aux États-Unis : les leçons récentes de la Louisiane », Chronique de l'ONU, *Le magazine des Nations Unies*, vol. XLIV, n°3, sept. 2007.

- Anonyme, « Combien de temps faut-il pour lire les règles de confidentialité ? », *Slate*, 6 mars 2012, article en ligne.

- Anonyme, « HapiFORK, la fourchette qui vous dit comment manger », *Les Échos*, 12 avr. 2013, article en ligne.

III – Notes, observations, commentaires et chroniques de jurisprudence

- BRUGUIERE (J-M.), « Un moteur de recherche est bien "une personne" susceptible de remédier aux atteintes aux droits d'auteur et droits voisins sur l'internet », note sous CA Paris, Pôle 5, Ch. 1., n°14/01359, 15 mars 2016, Syndicats APC, FNDF, SEVN, UPF, et SPI contre Orange, SFR, YAHOO ! Darty, Bouygues télécom, Free, Google, Microsoft, Numéricâble, *PI*, 1er juillet 2016, n°60, pp. 344-346.

- Note d'information sur la jurisprudence de la Cour n°149, greffe de la Cour, n° 60641/08, 7 fév. 2012, Von Hannover c. Allemagne (n°2).

- PAUTROT (B.), « Adresse IP : victoire du relativisme sur les dogmatismes quant à la qualification de données à caractère personnel », *RLDI*, n°134, 1er fév. 2017, com. de CJUE, 2ème Ch., C-582/14, 19 oct. 2016, Patrick Breyer c. Bundesrepublick Deutschland.

- PÉRONNE (G.), « L'adresse IP est bien une donnée à caractère personnel », obs. sous CJUE, n° C-582/14, 19 oct. 2016, Patrick Breyer c. Bundesrepublik Deutschland et C. Cass., 1ère Ch. civ., n°15-22.595, 3 nov. 2016, *Dalloz IP/IT*, 2017, pp. 120-123.

- VOORHOOF (D.), note sous CEDH, n°59320/00, 24 juin 2004, Affaire Von Hannover c. Allemagne, *IRIS.*

- WALTER (J-B.), « La protection du droit au respect de la vie privée : entre texte et prétextes (Retour sur les arrêts Van Hannover…) », *RLDI*, n° 98, 1er nov. 2013, pp. 34-40.

IV – Jurisprudence

- CEDH, 2ème sec., requête n° 58148/00, 18 mai 2014, Affaire Éditions Plon c. France.

- Supreme Court of the United States, 18 déc. 1967, Charles Katz c. United States.

- CJUE, Gr. Ch., n°C-362/14, 6 oct. 2015, Maximilian Schrems KG c. Data Protection Commissioner.

- CJUE, n° C-582/14, 19 oct. 2016, Patrick Breyer c. Bundesrepublik Deutschland.

- CJUE, n° C-131/12., 13 mai 2014, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzàlez.

- C. Constit, n° 76-75 DC, 12 jan. 1977, sur la loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales.

- C. Constit, n° 94-352 DC, 18 jan. 1995, sur la loi d'orientation et de programmation relative à la sécurité.

- C. Constit, n°99-416, 23 juil. 1999, sur la loi portant création d'une couverture maladie universelle.

- C. Constit., décision n°81-132 DC, 16 jan. 1982, sur la loi de nationalisation.

- C. Cass. 1ère Ch. civ., n°15-22.595, 3 nov. 2016.

- C. Cass., Ch. cr., n° 05-83.423,14 mars 2006.

- CE., 10ème et 9ème sec., n°306173, 30 déc. 2009, *Leb.*

- CE., 10ème et 9ème sec., n°301178, 21 mai 2008, *Leb.*

- CNIL, Décision n°2018-007, 5 mars 2018, mettant en demeure la société DIRECT ENERGIE.

- N. D. Cal., n°11-CV-01726, 4 avr. 2011, Angel Fraley, and al. c. Facebook.

- CA Paris, Pôle 5, Ch. 1., n°14/01359, 15 mars 2016, Syndicats APC, FNDF, SEVN, UPF, et SPI contre Orange, SFR, YAHOO ! Darty, Bouygues télécom, Free, Google, Microsoft, Numéricâble.

- CA Paris, n° 15/08624, 12 fév. 2016,

- TGI Paris, référé, 22 mai 2000, UEJF et Licra c. Yahoo ! Inc. et Yahoo ! France.

- TA Montreuil, n°1700278, 7 déc. 2017, Préfet de la Seine-Saint-Denis.

V – Textes officiels

- Loi n° 2004-801, 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, Dossiers législatifs – Exposé des motifs.

- Loi n°89-1009 du 31 décembre 1989 renforçant les garanties offertes aux personnes assurées contre certains risques.

- Loi du 29 juillet 1881 sur la liberté de la presse.

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

- 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 à la protection des données).

- Règlement (CE) n°44/2001, 22 déc. 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.

T A B L E D E S M A T I È R E S