AIX-MARSEILLE UNIVERSITÉ
FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE D'AIX-MARSEILLE
INSTITUT DE RECHERCHE ET D'ETUDES EN DROIT DE L'INFORMATION ET DE LA COMMUNICATION

LA PATRIMONIALISATION DES DONNEES PERSONNELLES

MÉMOIRE POUR L'OBTENTION DU MASTER « DROIT DES MEDIAS ET DES TELECOMMUNICATIONS »

PRÉSENTÉ PAR

RAMAGE Manon

Sous la direction de Monsieur Philippe MOURON, Maître de conférences en droit privé

Année universitaire

2014/2015

TABLE DES ABREVIATIONS

- **AEPD** : agencia espagnola de proteccion de datos.
- **CEDH** : Convention européenne des droits de l'Homme et du citoyen.
- **CJUE** : Cour de Justice de l'Union européenne.
- **CNIL** : Commission nationale de l'informatique et des libertés.
- **CNNum** : Conseil National du Numérique.
- **GAFA** : Google, Apple, Facebook, Amazone.
- **GC** : grande chambre.
- **LIBE** : Libertés civiles, justice et affaires intérieures.
- **NSA** : National Security Agency
- **OCDE** : Organisation de coopération et de développement économique.
- **RTD Civ.** : Revue trimestrielle de droit civil.
- **SAFARI** :

SOMMAIRE

Introduction

Une étude menée par une entreprise spécialisée dans la cybercriminalité a révélé qu'en 2014 plus d'un milliard vingt trois millions de données à caractère personnel ont été volées[1]. Ce chiffre démontre que chaque jour, dans l'Europe et dans le monde entier, transite un nombre extrêmement élevé de données et donne une explication à la préoccupation croissante des européens vis-à-vis de leurs données.

En effet, les données à caractère personnel sont un sujet qui crée le débat en Europe tant du côté des particuliers que de celui des politiques ou encore des législateurs… Cela est du principalement à l'expansion croissante et considérable d'internet. Aujourd'hui tout le monde utilise internet quotidiennement à partir de terminaux prenant des formes différentes: tablettes, téléphone, ordinateur, objets. Internet fait partie intégrante de notre quotidien de façon beaucoup plus importante qu'il y a une dizaine d'années. Sur internet, nombreux sont les services dont l'accès est gratuit mais où il est nécessaire en contrepartie de renseigner ses données personnelles. C'est le cas pour les réseaux sociaux tels que Facebook par exemple. Internet sert également à mettre en ligne un certain nombre d'informations personnelles qui pourront être récupérées par les entreprises à des fins commerciales[2]. Ainsi, certaines sociétés ont bâti leur modèle économique sur l'utilisation de nos données personnelles. Les européens sont de plus en plus sensibles aux sort et à l'utilisation qui est réservée à leurs données personnelles.

Plus encore, l'actualité ne cesse de relancer le débat à travers différentes affaires qui ont pu faire grand bruit dans l'opinion publique. C'est notamment le cas avec l'affaire Snowden. Les révélations d'Edward Snowden qui ont démontré que des collectes massives d'informations réalisées par la NSA concernaient pour 90% des citoyens ordinaires et dépassaient largement le cadre de lutte contre le terrorisme ont choqué et inquiété les citoyens de nombreux pays[3].

Cette affaire a déclenché un débat en France sur le Big Data, c'est à dire la production massive de données via le net, qui serait considérée par certains comme le futur Big Brother qui surveillerait tout le monde[4]. Enfin, le projet de loi renseignement remet une fois de plus en avant le sujet des données personnelles puisqu'il prévoit afin de renforcer les dispositifs de surveillance dans le cadre

[1] ANONYME, « Les chiffres du vol des données en 2014, cil.cnrs.fr, 20 février 2015.
[2] DESGENS-PASANAU (G.), *La protection des données à caractère personnel La loi « informatique et libertés »*, LexisNexis, Paris, 2012, p. 11.
[3] ANONYME, « 90% des citoyens espionnés par la NSA sont des « gens ordinaires » », lexpress.fr, 07 juillet 2014.
[4] ANONYME, « Quand « Big Data » menace de devenir « Big Brother » », laquadrature.net, 06 janvier 2014.

de la lutte contre le terrorisme, la possibilité de mettre en place des dispositifs permettant une surveillance générale d'internet, ce qui a été vivement critiqué de toute part[5].

Nous voyons donc que c'est un des sujets qui donne lieu au nombre le plus élevé de débats, ce qui prouve que les données personnelles sont au coeur des préoccupations des citoyens européens. C'est un problème qui touche chaque citoyen personnellement, d'où l'intérêt croissant qui leur est porté.

Paradoxalement, les internautes fournissent tous les jours certaines de leurs données personnelles sans forcément s'en rendre compte, car lorsqu'on utilise le terme « données personnelles » on ne sait pas de prime abord ce que cela désigne et l'on pourrait être tenté de le prendre à la légère. D'où la nécessité de définir les données personnelles de manière claire et précise.

L'article 2 de la loi Informatique et liberté sur la protection des données personnelles définit ces dernières comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». Cet article précise également que l'on détermine si une personne est identifiable aux vus des moyens dont dispose le responsable de traitement ou toute autre personne permettant son identification. Cette définition couvre un champ très large puisqu'elle couvre les fichiers numérisés mais également les fichiers papiers. De plus, il suffit que la personne soit identifiable pour que cela rentre dans la catégorie des données personnelles. Ainsi, l'adresse, le nom ou encore les données de connexion seront considérées comme des données personnelles. Il suffit d'avoir une information quelle qu'en soit sa nature qui concerne une personne physique identifiée ou identifiable[6]. Ces données sont traitées par de nombreuses sociétés c'est à dire qu'elles font l'objet de « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »[7]. On appelle personne concernée la personne à laquelle se rapportent les données qui font l'objet du traitement. Ces données de toutes sortes sont de plus en plus exploitées par les entreprises, ce qui conduit à penser qu'un mouvement

[5] RONFAUT (L.), « Qu'est-ce que la loi renseignement ? », lefigaro.fr, 25 juin 2015
[6] EYNARD (J.), *Les données personnelles : quelle définition pour un régime de protection efficace ?*, Michalon, Paris, 2013, p. 33.
[7] Article 2 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.

de patrimonialisation de ces données est en marche. La patrimonialisation se définit comme le fait pour un attribut de la personnalité qui à la base est par nature extrapatrimonial, de se charger d'une valeur qu'il est possible d'apprécier en argent. La conséquence est le passage de la catégorie des droits extrapatrimoniaux à celle des droits patrimoniaux. Cette valeur économique est issue de la valeur propre de la personne et c'est seulement cette dernière qui est en droit de l'exploiter[8].

Dans les réflexions qui seront proposées nous nous concentrerons sur cet aspect patrimonial des données. Nous présenterons rapidement les règles en vigueur en matière de protection des données mais nous nous focaliserons surtout sur l'aspect patrimonial des données qui pourrait influer sur cette protection.

En effet, aujourd'hui, la protection des données à caractère personnel semble être l'enjeux majeur de notre époque car on en produit énormément chaque jour et il faut que l'on puisse permettre la progression de la technologie et d'internet et à la fois protéger efficacement les citoyens. C'est bien le droit qui viendra essayer de trouver une balance équitable entre les deux.

L'idée d'une protection efficace des données à caractère personnel n'est pas nouvelle pour autant. Même à l'épode des fichiers papiers, la crainte du sort des données personnelles était bien présente chez les citoyens et notamment chez les français. En effet la France s'est dotée d'une loi de protection des données personnelles avec la loi du 6 janvier 1978 alors que l'informatique n'en était qu'à ses balbutiements et qu'internet n'existait pas. Cette loi a été votée suite à deux scandales: l'affaire SAFARI et l'affaire du numéro Carmille qui ont fait craindre aux français la mise en place d'un Big Brother et d'un fichage généralisé[9]. Il en est de même pour l'Allemagne qui en adoptant une loi fédérale a été le premier pays à se doter d'un texte sur la protection des données personnelles[10]. Par la suite, l'Union européenne dans les années 1990 a pris conscience qu'il était nécessaire de réguler ce phénomène à l'échelle européenne et elle a adopté une directive en 1995. Cependant, celle-ci a été adoptée lorsque internet n'existait pas encore ou très peu, ce qui fait qu'aujourd'hui il serait nécessaire de modifier le droit européen applicable. C'est pour cette raison qu'un projet de règlement est en cours d'élaboration. Ce projet pourrait faire évoluer un certain nombre de choses puisqu'il évoque la possibilité de prendre en compte la patrimonialsation des données. En effet, le droit européen est aujourd'hui très protecteur des données personnelles et moins permissif en terme de commercialisation de ces données.

[8] CORNU (G.), *Vocabulaire juridique*, Puf, 8e éd., Paris, 2009, p. 667.
[9] DESGENS-PASANAU (G.), *op. cit.*, p. 5.
[10] ANONYME, « La protection des données personnelles », http://www.senat.fr, 12 février 2014.

Ce n'est pas le cas dans tous les pays puisque certains sont très permissifs et on parle même de paradis des données. Ces derniers correspondent en général aux paradis fiscaux. Dans ces pays ,les traitements de données sont libres. Par exemple aux Etats Unis, on se rend compte que les choses sont beaucoup plus simples. Pour le moment il est possible de récolter et de vendre les données librement.

Ce phénomène de commercialisation est aujourd'hui mondialisé et existe réellement. Ainsi, nous nous demanderons en quoi la patrimonialisation des données personnelles peut justifier l'instauration d'un droit de propriété sur ces données.

Nous nous pencherons sur la patrimonialisation des données personnelles (I) avant d'étudier la possible instauration d'un droit de propriété sur les données personnelles (II).

I) La patrimonialisation du droit des données personnelles.

Il conviendra de prendre conscience de l'existence d'une patrimonialisation réelle en dépit des dispositions législatives (A) avant d'étudier l'existence d'une patrimonialisation potentielle dans le projet de règlement européen pour la protection des données personnelles (B).

A) Une patrimonialisation réelle en dépit des dispositions législatives.

En France, c'est la loi du 6 janvier 1978 relative à l'informatique aux fichiers et aux liberté dite Informatique et Liberté qui règle la question de la protection des données personnelles. Cette loi a conféré à la France une position avant-gardiste sur la protection des données personnelles. En effet, peu nombreux sont les pays qui se sont préoccupés du sort des données personnelles dans le milieu des années 1970. Des lois ont commencé à se mettre en place en Allemagne puis en Suède et la France s'est placée dans le sillage de ces deux pays et s'est penchée sur l'adoption d'une loi dans ce domaine. La France est donc en avance sur la question de la protection des données personnelles. La preuve en est que la législation européenne en la matière qui n'apparaitra que dans les années 2000 s'inspirera de cette loi de 1978. Cette avance de la France s'explique d'abord par une prise de conscience des français concernant le développement de l'informatique. La fin des années 1970 accueille le passage du fichier papier au fichier informatisé et les français réalisent que ce nouvel outil pourrait avoir des conséquences néfastes[11]. Cette crainte des français est accentuée par une

[11] DESGENS-PASANAU (G.), *op. cit.*, p. 3.

succession de scandales concernant les données personnelles dans les années 1970 et notamment par le projet SAFARI[12].

C'est le ministère de l'intérieur qui en 1974 avait créé un système informatique baptisé système automatisé pour les fichiers administratifs et le répertoire des individus (SAFARI). Le but était d'interconnecter les fichiers nominatifs des administrations françaises. Il s'agissait d'une base de données centralisée de la population et c'était le fichier de sécurité sociale qui devait servir d'identifiant commun à tous les fichiers administratifs[13]. Le but était de créer un seul identifiant pour les fichiers de toutes les administrations publiques ainsi que pour la sécurité sociale. Il était également prévu la mise en place d'un ordinateur permettant de centraliser toutes les bases de données[14] des différents services comme ceux de police, du ministère public, des armées ou encore de la banque par exemple. Une simple interrogation de fichiers informatiques aurait pu permettre à l'administration française d'avoir accès à toutes les informations enregistrées sur une personne[15]. Le risque de ce fichier était la création de profils permettant de ficher les français et pouvant les gêner dans certaines de leurs démarches. Par exemple, un client reconnu comme insolvable aurait pu être gêné lors de la réalisation de certaines démarches administratives en raison de cette ancienne insolvabilité qui aurait été une donnée centralisée par le gouvernement. Cela aurait contribué à enfermer le citoyen dans une situation en lui apposant une certaine étiquette dont il aurait eu beaucoup de mal à se défaire[16]. Ce projet a été révélé aux français par le journal Le Monde en 1974 dans un article intitulé « Safari ou la chasse aux Français ». Cet article a immédiatement suscité une vive émotion et c'est une réelle polémique qui va s'installer. En effet, à cette époque la guerre de 1940 est encore dans tous les esprits. Or, sous le régime de Vichy, un numéro spécifique avait été attribué au juifs et aux étrangers par l'administration. Par conséquent, ce qui effraye certains citoyens, outre le fait d'être fiché, c'est l'utilisation qui pourrait être faite d'un tel fichier en cas de prise de contrôle de l'administration par un régime comme celui qui a été mis en place en France pendant la seconde guerre mondiale[17]. A cette époque, on était en effet encore persuadé que le numéro de sécurité sociale avait été créé pour réaliser un fichage ethnique, ce qui n'a en réalité pas été le cas[18].

---

[12] FRAYSSINET (J.), Droit des TIC approfondi, cours du Master 2 droit des médias et des télécommunications, IREDIC, 2014-2015, p. 3.
[13] ANONYME, « 1977 - 1978 : le Sénat invente les autorités administratives indépendantes », http://www.senat.fr, 20 juin 2008.
[14] BOUCHER (P.), « A l'origine de la CNIL : « Safari » ou la chasse aux Français », http://ldh-toulon.net, 1er octobre 2008.
[15] DESGENS-PASANAU (G.), *ibid*.
[16] ANONYME, « Origine de la loi Informatique et Liberté », cil.cnrs.fr, le 15 novembre 2012.
[17] BOUCHER (P.), *op. cit.*
[18] DESGENS-PASANAU (G.), *op. cit.*, p. 4.

Il convient de préciser que suite au développement très important de la technologie ces dernières années, la loi « Informatique et liberté » a subi une réforme le 6 août 2004 car pour tenter de faire face aux nouvelles problématiques concernant les données personnelles, l'Europe avait adopté une directive dans ce domaine le 24 Octobre 1995 qu'il était devenu nécessaire de transposer en droit français[19].

Parallèlement à la règlementation française, les organismes internationaux ont eux aussi réfléchi à la question des données personnelles en des termes moins précis que la loi française mais ils ont réussi à dégager de grands principes de protection. Ainsi l'OCDE a adopté le 23 septembre 1980 la Recommandation du conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, et le 28 janvier 1981, c'est le Conseil de l'Europe qui a adopté la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel plus connu sous le nom de Convention 108. La valeur normative de ces textes est quelque peu amoindrie puisque les lignes directrices ne sont qu'une recommandation et que la Convention 108 n'est qu'applicable aux Etats ayant décidé de la signer. Ces textes n'ont donc qu'une faible valeur contraignante. La France est signataire de la Convention 108, elle est entrée en vigueur en France en 1983, par conséquent la France se doit de la respecter[20]. Il existe 8 grands principes qui ont été dégagés dans ces deux textes. Tout d'abord celui selon lequel toute personne physique doit avoir un droit d'accès, de modification et d'opposition sur ses données personnelles. Ensuite, il y a la règle de la finalité selon laquelle le traitement d'une donnée doit être fait pour la finalité qui a été précisée au moment de sa collecte et pas pour une autre finalité. Il est également nécessaire que toute personne physique soit informée du traitement que vont subir ses données et qu'elle donne son consentement. Le traitement doit également porter sur des données exactes complètes et mises à jour. Lorsqu'il s'agit de données dites sensibles, celles-ci doivent faire l'objet d'un traitement spécifique. Les données ne peuvent pas être conservées à vie, elles doivent être conservées pendant la durée nécessaire à la durée de la finalité. Selon ces textes, des mesures pour protéger les données de leur destruction ou de leur divulgation non autorisée et enfin ces données ne peuvent pas être exportées vers des pays qui ne garantissent pas un niveau de protection équivalent à la protection en vigueur dans leur pays d'origine[21].

[19] DESGENS-PASANAU (G.), *op. cit.*, p. 2.

[20] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, jurisprudence*, Eyrolles, Paris, 2013, p. 13.

[21] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op. cit.*, p. 15.

Dans la loi française, on retrouve la plupart de ces grands principes mais de façon plus précise et parfois même des principes plus sévères. En effet, la France a fait le choix d'adopter un régime protecteur pour celui dont les données sont exploitées, ce qui n'est pas le cas dans tous les pays puisque par exemple aux Etats Unis il existe une grande liberté d'utilisation des données personnelles par les entreprises.

Toujours dans ce souci d'obtenir un niveau de protection élevé dans la loi Informatique et liberté, le droit de la protection des données personnelles est posé de telle manière que cela conduit à placer ce droit dans la catégorie des droits dits extrapatrimoniaux.

En effet, que ce soit dans la conception française ou dans la conception européenne, l'idée principale est que les informations relatives aux personnes relèvent des droits de la personnalité[22]. C'est à dire de droits inhérents, attachés à la personne humaine qui appartiennent à toute personne physique dans le but de protéger ses intérêts principaux[23]. Ce droit est tellement consubstantiel à la personne que celle-ci ne peut pas choisir de disposer librement de ces informations[24]. Fait partie notamment de ces droits de la personnalité le droit à la vie ou encore le droit au respect de la vie privée. Or, dans la loi Informatique et libertés, les données à caractère personnel sont définies comme toute information relative à une personne physique identifiée ou identifiable. A partir du moment où la loi de 1978 a qualifié les données personnelles d'informations relatives aux personnes, on peut en déduire que le législateur a entendu faire entrer ces données dans les droits de la personnalité et donc a fortiori dans la catégorie des droits extrapatrimoniaux dont relèvent les droits de la personnalité. Ces droits extrapatrimoniaux sont ceux qui n'entrent pas dans le patrimoine et qui touchent à la personne. Par conséquent, ils n'ont pas la qualification de bien et sont normalement hors du commerce[25]. Ces droits sont incessibles, imprescriptibles et perpétuels. De toute évidence il semblait plus pratique de classer le droit à la protection des données personnelles dans la catégorie des droits extrapatrimoniaux tout d'abord en raison de leur essence même et ensuite afin d'avoir la possibilité de mettre en en place un régime protecteur des données. De plus, lorsqu'on pense à ses données personnelles (telles que le nom, le numéro de téléphone, les goûts), il est difficile d'imaginer dans un premier temps que des données aussi attachées à la personne et à sa vie privée soient considérées comme des biens et puissent bénéficier d'une facilité d'utilisation par les tiers.

[22] FRAYSSINET (J.), *op. cit.*, p. 1.
[23] CORNU (G.), *op. cit.*, p. 679.
[24] FRAYSSINET (J.), *op. cit.*, p. 2.
[25] CORNU (G.), *op. cit.*, p. 395.

Par conséquent, la loi Informatique et liberté a tenté de poser un régime de protection des données à la hauteur de ce nouveau droit de la personnalité. C'est en effet certainement en raison de ce rattachement aux droits extrapatrimoniaux qu'un certain nombre de règles de protection ont été posées.

Bien que la loi s'applique aux traitements automatisés et aux traitements manuels[26] le premier article de la loi donne le ton en précisant que « 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. »[27]. Ici le législateur sous entend que ce n'est pas l'homme qui est au service de l'informatique mais bien l'inverse, l'informatique doit donc rester un outil permettant d'aider l'homme et dès cet article on précise que cela ne doit pas porter atteintes aux droits de la personnalité de l'homme. Par cette énumération de droits devant être respectés, on voit qu'il y a une volonté du législateur d'assurer un large champ de protection pour les données personnelles car les termes choisis tels que vie privée, libertés individuelles ou publiques sont volontairement très larges[28]. Cet article permet également de souligner que dans la protection des données à caractère personnels la vie privée n'est pas le seul élément protégé, car bien souvent on a tendance a réduire la protection des données personnelles à la protection de la vie privée alors qu'elle n'est qu'un des éléments protégé par le droit de la protection des données personnelles[29]. Il est vrai qu'il est tentant d'associer les deux, cependant, la loi, en énumérant d'autres droits, nous montre bien que le droit à la protection des données à caractère personnel est un droit à part entière assimilé aux droits de la personnalités. La vie privée est donc un des éléments protégés par ce droit mais ce n'est pas le seul.

C'est aussi certainement ce rattachement à la catégorie des droits extrapatrimoniaux qui a poussé le législateur français à adopter une définition des données à caractère personnel plus large qu'en droit européen. En effet, l'article 2 de la loi précise qu'une donnée personnelle est toute information relative à une personne physique identifiée ou identifiable et élargit le caractère identifiable à « l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou tout autre personne. ». Là encore il y a une volonté du législateur d'englober un maximum d'informations dans la catégorie des données personnelles. Une donnée anonyme sur laquelle l'anonymat peut être levée sera toujours considérée comme une données

[26] Article 2 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.
[27] Article 1 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.
[28] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op. cit.*, p. 30.
[29] FRAYSSINET (J.), *op.cit.*, p. 4.

personnelle et pas seulement quand l'anonymat sera levé par le responsable de traitement mais aussi lorsque il sera levé par les autorités judiciaires à l'occasion d'enquête ou par les services de renseignements étatiques par exemple[30]. Cela pourra d'ailleurs poser problème à ces autorités qui devront alors certainement se soumettre aux obligations pesant sur le responsable du traitement des données à caractère personnel.

Ce dernier sera « la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens »[31]. Le responsable de traitement est d'ailleurs soumis à des obligations permettant de garantir une protection efficace des données personnelles et donc de données pouvant toucher des éléments de la personnalité. Ce responsable doit tout d'abord s'occuper de la déclaration des traitements automatisés de données à caractère personnel à la Commission nationale de l'informatique et des libertés. La CNIL est un un organisme spécialisé mis en place par la loi informatique et liberté dans le but de faire respecter les droits et obligations existants dans la loi. Cela permet là encore d'avoir une protection accrue des données personnelles qui peut s'expliquer par leur rattachement aux droits extrapatrimaniaux. De plus, avec la révision de la loi informatique et liberté en 2004, la CNIL a obtenu en plus de sa mission de surveillance et d'information des personnes concernées un pouvoir de sanction s'apparentant à un pouvoir de contrôle a posteriori[32]. Ainsi, la CNIL a d'abord une mission de sensibilisation importante permettant d'informer les destinataires des traitements de données de leurs droits et de conseiller les responsables de traitement de données à caractère personnel afin que ceux-ci puissent effectuer ce traitement en conformité avec les dispositions légales. De plus, il n'est pas toujours évident de comprendre la façon dont le traitement doit être mis en oeuvre. Ainsi, les responsables de traitement peuvent s'adresser à la CNIL afin que celle-ci leur indique la marche à suivre[33].

Cette mission montre que la loi veut éviter au maximum les entraves aux règles qu'elle pose et donc éviter que suite à un mauvais traitement des données personnelles, il soit porté atteinte à un droit de la personnalité comme la vie privée par exemple. Cela prouve l'importance attachée à la protection de ces données. On veut éviter par la mission de conseil une atteinte aux donnée personnelles car on sait que si une telle atteinte a lieu, même si le responsable de traitement est sanctionné, le mal sera fait pour la personne dont les données sont exploitées contre son gré ou révélées. Cela peut avoir

[30] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op. cit.*, p. 31.
[31] Article 3 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.
[32] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op. cit.*, p. 55.
[33] ANONYME, *Informatique et liberté mode d'emploi*, Groupe Revue Fiduciaire, Paris, 2007, p 57.

pour la personne qui fait l'objet de l'atteinte un côté effrayant voir traumatisant lorsque des données qui sont éminemment personnelles se retrouvent dévoilées ou utilisées par des entreprises sans qu'elle ait donné son autorisation. C'est certainement de là qu'il est apparu nécessaire de rattacher les données personnelles aux droits extrapatrimoniaux. La loi pour protéger au mieux ces données semble donc plus partisane d'une prévention et d'un conseil accru afin d'éviter au mieux les atteintes que de la partie sanction. Le pouvoir de sanction a d'ailleurs été instauré mais il rend surtout d'autant plus efficace la mission de conseil. En effet, lorsque la CNIL est informée d'un manquement aux obligations imposées par la loi (notamment lorsqu'elle reçoit une plainte d'un particulier par exemple) elle peut prononcer un avertissement et mettre en demeure le responsable de traitement de faire cesser l'atteinte. C'est seulement si le responsable de traitement ne respecte pas la mise en demeure que la CNIL pourra prononcer des sanctions administratives[34] qui se divisent en deux catégories : une sanction pécuniaire (150 000 euros pour un premier manquement, 300 000 euros si il y a réitération dans les cinq ans) et une injonction de cesser le traitement ou le retrait de l'autorisation de traitement. La CNIL peut ordonner que ces sanctions soient publiées[35]. Parfois, les entreprises préfèrent payer l'amende car la publication d'une telle sanction peut entrainer une perte de confiance des destinataires du traitement ainsi que de ses partenaires. C'est d'ailleurs ainsi que ce pouvoir de sanction rend la mission de sensibilisation efficace. Ces sanctions qui peuvent être lourdes pourraient inciter les responsables de traitement à vouloir se conformer à la loi et ainsi préférer demander conseil à la CNIL avant de mettre en oeuvre un traitement. Ainsi, les responsables de traitements qui craignent les représailles seraient moins enclins à réaliser un traitement frauduleux des données personnelles, ce qui éviterait les erreurs de traitements et ainsi les atteintes à ces données. C'est le but recherché par la loi informatique et liberté. Cette volonté de faire primer la prévention sur la sanction est visible dans les chiffres puisque sur plus de 11 000 demandes individuelles adressées à la CNIL en 2014 seules 18 sanctions ont été prononcées par cette dernière, sur lesquelles on trouve 3 relaxes et seulement 8 sanctions financières, les 7 autres étant des avertissements[36].

La responsabilité qui est recherchée est celle du responsable de traitement, c'est à dire que c'est celui sur qui pèse les obligations imposées par la loi, qui risque d'être sanctionné. La protection est accrue par le fait qu'en cas de recours à un sous-traitant pour les opérations de traitement, le réel responsable de traitement ne sera pas exonéré car le sous-traitant ne décide pas des finalités ni des

[34] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op cit.*, p 55.
[35] ANONYME, *Informatique et liberté mode d'emploi*, *op. cit.*, p 60.
[36] « Conférence de presse 16 avril 2015, présentation du 35ème rapport d'activité 2014 », Rapport de la CNIL, 16 avril 2015, disponible sur cnil.fr, p 4.

moyens contrairement au responsable[37]. Cependant, le sous-traitant doit respecter les obligations imposées par le responsable de traitement. Cette responsabilité constante du responsable peut encore l'inviter à rester dans le droit chemin et à veiller à ce que ses sous-traitants traitent les données sans porter atteintes aux droits des personnes concernées car en cas de mauvais traitement il ne pourra pas rejeter la faute sur le sous-traitant.

Comme nous l'avons précisé plus haut, le responsable de traitement doit effectuer une déclaration à la CNIL, déclaration qui est encore révélatrice d'une volonté de protection efficace en raison de la nature extrapatrimoniale des données. En raison de leur qualité extrapatrimoniale les données personnelles ne peuvent pas être traitées par n'importe qui et n'importe comment. C'est là l'importance de cette déclaration préalable à la CNIL. Elle permet qu'aucun traitement de données à caractère personnel puisse avoir lieu sans en avoir demandé l'autorisation au préalable. Pour traiter des données à caractère personnel il est donc nécessaire de se déclarer à la CNIL. Cette étape permet à la CNIL de vérifier d'emblée certains éléments essentiels dont notamment la finalité du traitement et la catégorie de données concernées. En effet, lors de la déclaration, un des éléments à fournir est la finalité du traitement et cela est déterminant car une fois cette finalité déclarée, le responsable de traitement ne pourra pas utiliser les données qu'il a en sa possession pour une autre finalité. Cela est protecteur car le traitement d'une donnée personnelle ne peut avoir lieu sans le consentement de la personne à laquelle appartient les données. Ainsi, la personne donne son consentement pour une certaine finalité et ses données ne pourront pas être exploitées pour une autre finalité sans son consentement. Afin d'alléger les procédures, pour certaines catégories de données, il existe en dehors de la procédure normale de déclaration, des procédures simplifiées de déclaration et même des dispenses[38]. Par exemple, des dispenses ont été accordées pour les traitements réalisés par des organismes à but non lucratifs ou encore pour les sites web réalisés par des particuliers et collectant des données à caractère personnel dans le cadre d'une activité personnelle[39]. Au contraire, il y a des cas listés dans la loi où le responsable de traitement devra obtenir l'autorisation de la CNIL avant de le mettre en oeuvre. C'est le cas par exemple des traitements de données dites sensibles, les traitements concernant les données génétiques, sauf ceux réalisés par les médecins dans le but d'exercer leur profession, ou encore le transfert de données personnelles vers un pays n'ayant pas un niveau de protection équivalent à celui de la France[40].

---

[37] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op. cit.*, p 33.
[38] ANONYME, *Informatique et liberté mode d'emploi, op. cit.*, p. 89 et p. 90.
[39] DESGENS-PASANAU (G.), *op. cit.*, p. 19 et p. 20.
[40] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op. cit.*, p 60.

De la même façon, ce ne sont pas n'importe quelles données qui peuvent faire l'objet de n'importe quel traitement. En effet la phase de collecte des données est primordiale car pour assurer un niveau de protection suffisant il ne faut pas une collecte sans limite, sans consentement de la personne ou en lui indiquant de fausses conditions de traitement[41]. Ainsi, pour être régulière, la collecte doit d'abord être loyale et licite[42]. Une collecte licite signifie que cette dernière doit respecter les exigences posées par la loi. Mais une condition supplémentaire est posée: celle de la loyauté qui signifie de ne pas utiliser des manœuvres détournées ou de respecter les règles normales d'honnêteté. La collecte doit donc respecter la loi et en plus elle doit être faite de façon loyale et honnête. Une autre exigence posée par la loi est que la collecte doit être faite dans un but précis et déterminé d'où la nécessité lors de la déclaration de préciser la finalité de traitement. Il ne sera pas possible d'utiliser par la suite les données collectés dans un autre but que celui pour lequel elle a été réalisé sauf accord de la personne concernée ou de la CNIL[43]. Il y a ensuite une exigence de proportionnalité selon laquelle les données « sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs »[44]. Le responsable de traitement doit garantir une proportionnalité par rapport à la finalité poursuivie mais également par rapport à la catégorie de donnée faisant l'objet du traitement[45]. De la même façon, les données doivent être exactes, complètes et mises à jour[46]. Les données ne peuvent pas être conservées ad vitam aeternam. La durée de conservation ne doit pas excéder la durée pour laquelle les données ont été collectés[47].

Enfin, la loi donne à celui à qui appartient les données le rôle central. Tout d'abord, le consentement de la personne dont les données sont recueillies doit être donné sauf cas exceptionnels prévus par la loi[48]. Ensuite, selon l'article 32 de la loi de 1978, la personne dont les données sont collectées doit être informée d'un certain nombre de choses comme l'identité du responsable de traitement, la finalité du traitement ou encore des destinataires de ces données et des droits dont elle dispose. Ces droits sont au nombre de trois : droit d'accès aux données, droit de rectification et droit d'opposition. Le droit d'accès au données signifie que toute personne peut demander au responsable

[41] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op. cit.*, p 48.
[42] Article 6 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.
[43] MATTATIA, *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL,* op. cit., p 49.
[44] Article 6, 3° de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.
[45] DESGENS-PASANAU (G.), *op. cit.*, p. 38.
[46] Article 6 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.
[47] Article 6 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.
[48] Article 6 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.

de traitement s'il traite des données la concernant et si oui de lui donner des informations sur ce traitement ainsi que de lui communiquer la liste des données personnelles dont il dispose. Le responsable ne pourra s'y opposer qu'en cas de demande abusive ou ayant un caractère systématique. Le droit de rectification permet à toute personne de demander au responsable de modifier, rectifier, de mettre à jour ou d'effacer les données à caractère personnel la concernant qui seraient inexactes, incomplètes, périmées ou équivoques. Le responsable devra alors informer les tiers auxquels les données ont été transmises de la modification qui a été effectuée. Enfin, le droit d'opposition va permettre a toue personne de s'opposer à la collecte de ses données si celle-ci justifie d'un intérêt légitime. Ce n'est donc pas un droit absolu et il devra être concilié avec les intérêts légitimes du responsable de traitement qui peut dans certains cas particuliers se passer du consentement des personnes pour effectuer la collecte[49].

Suite à cette présentation de la loi, on peut dire que celle-ci est très protectrice en raison du rattachement aux droits extrapatrimoniaux du droit à la protection des données à caractère personnel. Malgré tout, on constate que le nombre de plaintes augmente sans cesse de la part des particuliers. En 2014, il y a eu une hausse de 3% des plaintes adressées à la CNIL, c'est à dire qu'elles ont été au nombre de 5825[50]. La protection des données personnelles est au coeur du débat public et il y a une inquiétude croissante des personnes concernant leurs données. On peut donner plusieurs explications à cela. La loi de 1978 n'est pas infaillible car bien qu'elle ait été rédigée de façon à donner une protection élevée c'est à de nouveaux enjeux de protection qu'elle est confrontée aujourd'hui. En effet, depuis quelques années, on assiste a une internationalisation des flux de données[51] alors qu'en France la loi ne s'applique qu'aux responsables de traitement établis sur le sol français ou à ceux établis hors de France et de l'Union européenne mais recourant à des moyens de traitements situés en France[52]. En outre, il existe désormais une délocalisation des traitements informatiques qui sont situés en Afrique du Nord ou en Inde afin de profiter de coûts moins élevés. Dans une période récente, nous avons aussi connu une explosion technologique, notamment avec les objets connectés et cette nouvelle technologie est de plus en plus gourmande en données personnelles. Tout est allé si vite ces dernières années qu'il était impossible pour la loi de 1978 de prévoir une telle évolution et une telle mondialisation. Nous verrons plus tard que le droit européen a tenté d'apporter une solu-

[49] MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, op cit.*, p. 47 et p. 48.
[50] « Conférence de presse 16 avril 2015, présentation du 35ème rapport d'activité 2014 », Rapport de la CNIL, 16 avril 2015, disponible sur cnil.fr, p. 7.
[51] DESGENS-PASANAU (G.), *op. cit.*, p. 11.
[52] Article 5 de la loi n°78-17 du 6 janvier 1978, loi relative à l'informatique aux fichiers et aux libertés.

tion à ce problème de champ d'application de la loi qui ne permet pas d'apporter une protection optimale aux données sortant du territoire français ou européen.

Tout ceci fait que même si la loi a entendu classer les données personnelles dans le champ extrapatrimonial, lorsqu'on se penche sur les pratiques existantes, on peut dire qu'il existe une patrimonialisation de fait de ces données. Il semblerait même que cette patrimonialisation soit inévitable et même nécessaire. En 2020, le marché de la donnée en Europe représentera plus de 1000 milliards d'euros[53]. On parle parfois de nouveau pétrole ou de ruée vers l'or de la part des entreprises qui commercialisent ces données. Et pour cause, certains géants ont fondé leur modèle sur la vente de ces données tel est le cas des GAFA : Google, Apple, Facebook et Amazone. C'est par la vente de nos données qu'ils s'enrichissent en collectant de plus en plus d'informations, ce qui leur permet d'avoir un suivi de plus en plus personnalisé des utilisateurs et ainsi de proposer des publicités adaptés aux gouts de chaque client.

Traditionnellement, on considère que les droits extrapatrimaniaux ne sont pas susceptibles de faire l'objet d'une évaluation pécuniaire contrairement aux droits patrimoniaux qui peuvent être évalués en argent et échangés. Ainsi, le critère permettant de passer de l'extrapatrimonialité à la patrimonialité serait la possibilité d'avouer la valeur du bien en question et sa capacité à être échangé. Si le bien remplit les deux conditions, il peut alors faire partie de la catégorie des droits patrimoniaux[54]. Si on prend les données personnelles en pratique il y a toute une économie qui s'est créée autour de la vente de ces données. Finalement, après avoir étudié la loi de 1978 rien n'interdit la commercialisation de ces données, l'essentiel étant d'obtenir préalablement l'accord de l'intéressé pour la collecte de ses données. Par conséquent, le législateur qui a voulu rattacher ce droit de la protection des données personnelles à la catégorie des droits extrapatrimoniaux n'a pas clairement exclu la possibilité de les faire passer dans la catégorie des droits patrimoniaux. La possibilité d'une patrimonialisation n'est pas prévue dans la loi mais existe bel et bien dans les faits. Les données ont en effet une réelle valeur économique pour les entreprises qui les vendent. Il y a donc en plus échange de ces données. A partir du moment où ces données se chargent d'une valeur marchande il est possible de les apparenter à un bien immatériel qui est susceptible de rentrer dans le patrimoine d'une personne et d'être échangé en contrepartie d'une rémunération. Nous sommes donc bien en présence d'une parimonialisation de fait puisqu'elle n'est pas prévue par la loi mais a bien lieu en réalité.

[53] MEHN (A.), « Peut-on vraiment contrôler ses données personnelles ? », france5.fr, le 15 janvier 2015.
[54] SERIAUX (A.), « la notion juridique de patrimoine », *RTD Civ.*, décembre 1994, n°4, p. 801.

Cela ne serait pas le seul droit à acquérir une dimension patrimoniale puisque certains auteurs aujourd'hui parlent même d'une patrimonialisation des droits extrapatrimoniaux[55]. C'est notamment le cas avec le droit à l'image qui fait l'objet de nombreux débats. Pour Hassler c'est l'évolution de la société qui a rendu inévitable la patrimonialisation de certains droits patrimoniaux. Si on prend le droit à l'image, il est très courant qu'une photo d'une célébrité soit vendue en exclusivité à un journal ou bien lorsqu'elle est de nature à intéresser le public et donc à faire vendre le journal en question à être simplement vendue. De plus, l'image entière des célébrités permet de faire commerce[56]. Le côté marchand est évident ici puisque c'est l'image de la personne qui permet de faire vendre et que cette image est évaluable en argent. Pour certains, cette tolérance de l'exploitation de l'image permet simplement à la personne célèbre de retirer les fruits et de tirer profit de sa notoriété. Il serait même préférable pour certains auteurs de reconnaitre cette patrimonialisation puisque une action en réparation du préjudice subi du fait d'une exploitation non autorisée de l'image d'un individu permettrait d'obtenir réparation. Certains ont même imaginé un régime hybride, c'est à dire de faire des droits extrapatrimoniaux susceptibles d'avoir une valeur marchande des droits patrimoniaux à caractère personnel. Il s'agirait d'appliquer la qualification de droits extrapatrimoniaux pour protéger l'individu des atteintes extrapatrimoniales et d'ajouter la possibilité d'exploiter ce droit en lui conférant le statut de droit personnel[57].

Une telle solution appliquée aux données personnelles permettrait de protéger les personnes auxquelles appartiennent ces données des différentes atteintes pouvant être faites et notamment à leur vie privée tout en leur permettant de profiter de l'exploitation de ces données. Cela permettrait en outre, de prendre en compte une réalité évidente aujourd'hui qui est la patrimonialisation de ces données qui ont acquis une véritable valeur marchande. On peut cependant noter une particularité dans la patrimonialisation des données personnelles. En effet, dans ce domaine la patrimonialisation se fait au bénéfice des entreprises sans que l'émetteur ou le créateur de ces données y participe. Habituellement la patrimonialisation profite à la personne qui vend un attribut de sa personnalité, ce qui n'est pas le cas ici.

Avec le développement des smartphones et applications, ainsi que l'apparition des objets connectés, tous les jours nous sommes confrontés à la marchandisation de nos données et donc à leur patrimonilisation. Prenons Facebook par exemple. Au dernier trimestre 2014, ce sont en moyenne 1,393 milliards d'utilisateurs qui se sont connectés à ce réseau social. Rien qu'en France, on compte 28

[55] HASSLER (T.), « La patrimonialisation des droits extrapatrimoniaux », *Petites affiches*, décembre 2004, n°244, p.3.
[56] HASSLER (T.), « La patrimonialisation des droits extrapatrimoniaux », *ibid*.
[57] HASSLER (T.), « Contriburion à la nature juridique du droit « patrimonial » à l'image, *RLDI*, 2010, n° 59, p. 72.

millions d'utilisateurs qui se connectent à Facebook tous les mois, et en Europe on en compte 307 millions. L'entreprise à la base n'a pas été conçue dans un but marchand ou commercial, pourtant en 2014 c'est un bénéfice de 2,93 milliards qu'elle a réalisé[58]. Facebook est donc une réelle entreprise ayant une vraie stratégie commerciale et dont le patron est milliardaire avec une prospérité basée sur l'exploitation de nos données.

En effet, Facebook est gratuit, pourtant il génère d'énormes profits. Ce succès vient de la récolte par le réseau social de l'ensemble des informations que les utilisateurs laissent lors de leur utilisation de Facebook et surtout de leur revente aux annonceurs[59]. Cela permet à ces derniers de réaliser par la suite de la publicité ciblée et ainsi de récupérer plus de clients. Ces données sont donc vendues et achetées à prix d'or. De plus, une étude a démontré que des données confidentielles pouvaient être déduites en observant l'utilisation du bouton « j'aime » par les utilisateurs de Facebook. Il serait possible de retrouver la religion, les origines géographiques ou encore les orientations sexuelles des utilisateurs. Grace à cela Facebook gagnerait environ 5 dollars par profil d'utilisateur. De manière plus générale les données personnelles d'un européen représenteraient environs 600 euros de nos jours. Cela n'a rien d'étonnant puisque Facebook est loin d'être le seul à collecter nos données pour les revendre. C'est données représentent une matière première qui doit ensuite être valorisée. Apple et Amazone se servent des données qu'ils collectent pour vendre leurs produits de manière ciblée. De plus, avec ces deux géants, il est possible de créer des comptes (Itunes par exemple) ce qui leur permet de conserver nos données bancaires entre autre. Enfin, Google lui aussi grâce à son moteur de recherche récolte beaucoup de données personnelles qu'il utilise à des fins commerciales, ce qui lui permet notamment de suggérer des activités à faire à ses utilisateurs en fonction des lieux où ils se trouvent[60].

Un autre exemple de ce phénomène de patrimonialisation est l'apparition en Europe d'entreprises qui proposent aux internautes de vendre eux-mêmes leurs données personnelles. C'est le cas en Angleterre avec la Start-up « Allow » qui propose de vendre ces données et de recevoir de l'argent en contrepartie.

La plupart des français et des européens sont des utilisateurs des GAFA. Or, malgré la loi protectrice de 1978 les français sont confrontés à cette vente et à l'utilisation de leurs données person-

[58] HOTTOT (K.), « Facebook en 2014 : 1,39 milliard d'utilisateurs et 2,93 milliards de bénéfices », nextinpact.com, 29 janvier 2015.
[59] CASTEX (F.), « Mes données personnelles ne sont pas à vendre ! », liberation.fr, 18 mars 2013.
[60] VINCENT (C.), « La ruée vers l'or des données personnelles », lesechos.fr, 7 mars 2013.

nelles. Ainsi, cette loi, bien que rédigée de manière très protectrice, est aujourd'hui confrontée à des situations auxquelles le législateur n'était pas préparé. Le législateur n'aurait pas pu non plus imaginer que les données personnelles se patrimonialiseraient.

Même la jurisprudence semble accepter et reconnaitre cette patrimonialisation de fait. En effet, la Cour de cassation a jugé dans un arrêt du 25 juin 2013 qu'un fichier de clientèle non déclaré à la CNIL constituait une chose hors commerce et par conséquent ne pouvait faire l'objet d'une cession à titre onéreux[61]. En raisonnant dans le sens inverse, on pourrait déduire de cette solution qu'un fichier de clientèle, lorsqu'il est déclaré à la CNIL, est dans le commerce et peut donc faire l'objet d'une cession à titre onéreux. En effet, cet arrêt semble vouloir considérer le régime juridique des données personnelles sous un angle marchand. Par cette décision, la Cour de cassation semble accepter et reconnaitre la réalité de la patrimonialisation en rendant sa décision en se basant sur le côté mercantile des données personnelles. En insinuant que la déclaration à la CNIL est la condition de forme qui permettrait de faire commerce des données personnelles, la Cour semble redonner aux données leur véritables nature et reconnaitre ce qu'elles sont vraiment : des données entrées dans le commerce[62]. La Cour pose une condition à respecter : la déclaration à la CNIL qui est une manière de protéger les personnes dont les données sont collectées puisqu'elle examinera les déclarations et veillera à ce qu'il ne soit pas porté atteinte aux droits de ces personnes. Cependant, dès que cette condition est remplie, elle semble vouloir reconnaitre que les données peuvent faire l'objet d'une vente, ce qui montre qu'elle leur reconnait leur valeur patrimoniale[63].

Enfin, le Conseil National du numérique aussi prend en compte cette évolution. Dans un rapport de 2014, le Conseil reconnaissait que les données étaient un vecteur clé de l'économie actuelle et constituaient une véritable chaîne de valeur. Le Conseil prend en compte l'augmentation croissante du nombre de données et les modèles économiques des plates-formes qui revendent ce type de données. A ce tire, il évoque la nécessité d'une réorganisation européenne afin de concilier la patrimonialisation des données aujourd'hui devenue une réalité et la protection des droits des personnes dont proviennent les données[64].

---

[61] C. Cass., Ch. Comm., 25 juin 2013, n° 12-17.037, FS-P+B+I

[62] STORRER (P.), « Pour un droit commercial des données à caractère personnel », *RTD Civ.*, juillet 2013, n°27, pp. 1845.

[63] MOURON (P.), « Non commercialité d'un fichier de données non déclaré à la CNIL », paru dans l'ouvrage *Droit commercial - Sociétés commerciales 2014 - Un an de jurisprudence commentée*, p. 318

[64] « Neutralité des plateformes : Réunir les conditions d'un environnement numérique ouvert et soutenable », Rapport du Conseil National du numérique, mai 2014, disponible sur www.cnnumerique.fr, p. 11.

Consciente elle aussi de cette nouvelle réalité, l'Union européenne a décidé de réformer la directive applicable en matière de protection des données afin de faire face aux nouveaux problèmes existants et de mettre en place un régime en adéquation avec les utilisations qui sont faites des données personnelles.

B) Une patrimonialisation potentielle dans le projet de règlement européen pour la protection des données personnelles.

Le droit de l'Union Européen en matière de protection des données à caractère personnel est largement inspiré du droit français et notamment de la loi Informatique et liberté de 1978, du fait qu'il est intervenu postérieurement à cette loi. Le Conseil de l'Europe aussi a élaboré des règles en matière de protection des données. C'est par le biais de l'article 8 de la Convention européenne des droits de l'Homme et des libertés fondamentales du 4 novembre 1950, qui énonce le droit à la protection de la vie privée et familiale, que les données à caractère personnel sont protégées par le

Conseil de l'Europe[65]. Ici, les données personnelles sont rattachées à la vie privée et familiale ce qui laisse penser qu'il y a une volonté de rattacher le droit de la protection des données a un droit de la personnalité qui aurait par conséquent une nature extrapatrimoniale. L'avantage du Conseil de l'Europe est qu'il comprend 47 Etats membres dont 28 pays sont déjà membres de l'Union européenne[66]. Par conséquent, la CEDH a un champ d'application plutôt large puisque tous les membres sont obligés de respecter les dispositions de la Convention. De plus, la Cour européenne des droits de l'Homme a été créée afin de faire appliquer et respecter les obligations de la CEDH. En étant insérée dans cette Convention, la protection des données personnelles devrait donc s'appliquer aux 47 Etats membres, ce qui permet à tous d'avoir un texte de référence en matière de protection des données.

Il y a également la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dite convention 108 du Conseil de l'Europe qui est le seul texte dans le domaine de la protection des données à avoir une force juridique obligatoire internationale. Cette convention oblige les Etats signataires à prendre des mesures dans leurs législations nationales afin d'obtenir une législation respectant les grands principes de la protection des données tels que la collecte licite et loyale des données ou encore l'exactitude des données collectées ou conservées. L'avantage ici est que sa signature est ouverte aux pays non membres du Conseil de l'Europe et qu'il s'agit d'une norme universelle qui peut servir de vitrine à la protection des données dans le monde. Il est prévu que cette convention soit modernisée afin de prendre en compte les évolutions technologiques rendant la collecte des données de plus en plus importante[67].

Dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, le droit à la protection des données personnelles a été reconnu dans son article 8. La charte traite notamment de la loyauté du traitement et de l'importance de l'accord de la personne concernée par le traitement et prévoit l'importance de la mise en place d'autorités indépendantes chargées de veiller à l'application des règles en matière de protection des données. Cette charte a été intégrée au traité de Lisbonne de 2007, ce qui lui a donné la valeur de traité et lui permet d'avoir un poids plus important au niveau européen[68].

---

[65] HAAS (G.) et COHEN-HADRIA (Y.), *Guide juridique informatique et libertés : collecte, traitement et sécurité des données dans l'univers numérique : ce que vous devez savoir*, ENI, St Herblain, 2012, p. 17.

[66] *Manuel de droit européen en matière de protection des données*, office des publications de l'Union européenne, Luxembourg, 2014, p. 15.

[67] *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 16.

[68] HAAS (G.) et COHEN-HADRIA (Y.), *op. cit.*, p. 19.

Malgré cette multiplicité de sources en droit européen, un besoin d'harmonisation s'est fait sentir au niveau de l'Union européenne. Le 24 octobre 1995 a donc été adoptée la directive n° 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Cette directive intervient à un moment où les pays de l'Union européenne ont pour la plupart adopté une législation en matière de protection des données personnelles et son but premier est d'harmoniser l'ensemble des droits existants afin d'obtenir une meilleure efficacité de protection. Le but a également été d'obtenir une protection de haut niveau dans l'Union européenne et d'en élargir le cadre. Enfin, cette harmonisation était indispensable afin de mettre en place la libre circulation des données au sein de l'union européenne. Cette libre circulation des données était elle même devenue indispensable à mettre en place. Elle était en effet rendue nécessaire par la libre circulation qui existait déjà en matière de marchandises, de capitaux, de services et de personnes au sein de l'Union européenne[69]. La liberté de circulation étant la règle dans l'union européenne, les données se devaient de subir le même sort si l'Europe voulait avancer avec son temps et ne pas prendre de retard. Sans harmonisation, il n'était pas possible de faire circuler les données entre différents Etats en favorisant la protection des personnes concernées et ne pas faire circuler les données du tout seraient devenu impossible à l'heure actuelle. La solution était donc de prévoir un cadre de circulation sain et favorisant la protection des données en circulation. La directive européenne à donc tenté de poser un cadre général permettant de protéger les données tout en les laissant circuler librement dans l'Union Européenne.

Avec ce double objectif à atteindre, le droit de l'Union européenne ouvre la porte à une double conception possible des données à caractère personnel. Le fait que le directive prévoit de mettre en place une protection accrue en matière de protection des données et qu'elle ait été construite dans le but de donner du poids au principe du droit à la vie privée[70] permet de rapprocher les données des droits de la personnalité. A l'inverse, le fait que la directive mette en place la libre circulation des données à caractère personnel permet d'assimiler les données à des biens, puisque celles-ci peuvent circuler librement de la même façon que les biens dans l'Union européenne. A fortiori, cela permettrait là encore de laisser une porte ouverte pour donner la qualification de droits extrapatrimoniaux aux données[71]. Cette possibilité de double qualification a sans doute été mise en place pour tenter de correspondre au maximum aux différentes conceptions existantes en droit européen.

[69] *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 18.
[70] *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 19.
[71] FRAYSSINET (J.), *op. cit.*, p. 4.

Si la liberté de circulation des données est la règle en Europe et cela sans qu'il soit nécéssaire pour le responsable de traitement d'accomplir des formalités spécifiques, la directive a entendu protéger les européens contre les exportations de données dans des pays qui n'auraient pas un droit équivalent en matière de protection des données. Cependant, l'exportation des données hors Union européenne n'ayant pas un niveau reconnu équivalent par la Commission européenne reste possible du moment où des accords entre pays sont conclus dans le respect de la loi. Par exemple, il y a le Safe Harbor conclu entre les autorités américaines et la Commission européenne en 2001. Il s'agit d'une convention internationale qui comprend la liste des entreprises américaines qui s'engagent volontairement à respecter le Safe Harbour qui comprend un ensemble de principes concernant la protection des données personnelles[72].

La directive européenne a donc une forte volonté de protection des données personnelles et même à l'extérieur de l'Union européenne. Cela peut montrer que les données peuvent être rattachées aux droits de la personnalité puisqu'elles font l'objet d'une protection élevée. En même temps, la circulation des données est rendue possible dès lors que certaines conditions sont remplies, ce qui montre que la double qualification droits de la personnalité/bien peut correspondre aux données en droit européen.

Par conséquent, le droit à la protection des données n'est pas un droit absolu et il doit être concilié avec d'autres droits comme la liberté d'expression, l'accès aux documents, ou encore le droit de propriété et notamment le droit de propriété intellectuelle.

Bien que la directive soit satisfaisante en ce qui concerne les grands principes et les objectifs de protection, elle ne suffit pas aujourd'hui à protéger les citoyens européens contre des utilisations massives et parfois illicites de leurs données. La Commission européenne a donc mis en avant le fait qu'il fallait faire évoluer la règlementation en matière de protection des données. En effet, lorsque la directive a été adoptée en 1995, internet n'existait pas. Par conséquent, la directive ne pouvait pas envisager l'ampleur que prendrait la collecte des données[73]. De plus, bien que la directive était ouverte à une double qualification, à savoir droit de la personnalité et bien donc qui s'apparenterait plus à des droits patrimoniaux, la valeur économique des données n'était pas clairement reconnue dans la directive. La raison est que dans les années 1995 le phénomène de commercialisation des données n'existait pas ou très peu, celui-ci s'étant surtout développé avec

[72] DESGENS-PASANAU (G.), *op cit.*, p. 47 et p. 48.
[73] ANONYME, « la nécessité d'une refonte en profondeur », *Lamy droit des médias et de la communication*, tome 1, Lamy, étude 479-30, mai 2015.

l'apparition d'internet. Une liberté de circulation est reconnue dans la directive de 1995, ce qui laisse penser qu'un rattachement aux droits patrimoniaux est possible. Cependant, la valeur économique n'étant pas clairement reconnue, le doute de la qualification subsiste.

En 2011, le Parlement européen a lui aussi pris conscience de la nécessité d'engager une réforme de la protection des données. Le 25 janvier 2012 a ainsi été proposé un projet de règlement 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 (règlement sur la protection des données personnelles). En décidant de mettre en place un règlement, il y a une volonté de l'Europe d'éviter d'avoir une transposition différente dans chaque Etat de l'Union. Un règlement communautaire sera d'application immédiate dans les différents Etats. Le but est d'éviter que les nouvelles règles issues du règlement soient transposées plusieurs années après son entrée en vigueur. De plus, avec la directive de 1995, il y a dans chaque pays des interprétations très différentes des notions clés de cette directive, ce qui conduit à une application différente du droit à la protection des données. La mise en place du règlement limiterait ces interprétations et permettrait une réelle uniformisation du territoire européen et a fortiori une meilleure protection des données personnelles des européens[74].

Ce projet a été adopté en première lecture au Parlement européen en mars 2014[75]. A la lecture de la proposition de règlement, on voit qu'il y a de la part du législateur européen une reconnaissance des faiblesses du sytème en place actuellement et une volonté de prendre en compte les évolutions ayant eu lieu ces dernière années. Il y a une prise de conscience que les nouvelles technologies ont modifié les rapports économiques puisqu'elles permettent à tout le monde de partager des flux de données et permettent au secteur privé comme au secteur public d'utiliser ces données[76]. En reconnaissant cette utilisation des données par les entreprises ou par les pouvoirs public, cela permet de faire un pas en avant vers la reconnaissance de l'utilisation commerciale de ces données. En effet, le nouveau texte a vocation à prendre en compte cette situation de fait existant de façon massive en Europe aujourd'hui.

Le but de ce texte est également de mettre en place un climat de confiance dans le numérique. Or, cette confiance ne passera que par la reconnaissance de la réelle utilisation des données. Rien ne sert de se voiler la face, il est préférable de prendre en compte cette commercialisation des données

[74] FRAYSSINET (J.), op. cit., p. 5.

[75] POIDEVIN (B.), « Les apports du projet de règlement européen du 25 janvier 2012 relatif aux données personnelles », http://www.village-justice.com, 1er avril 2015.

[76] « Proposition de règlement du Parlement européen et du Conseil 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 », Commission européenne, le 25 janvier 2012, disponible sur ec.europa.eu, p1.

conduisant à une réelle patrimonialisation de celles-ci afin que l'Europe ne reste pas arriérée dans le monde du numérique.

L'Europe semble avoir compris qu'il est nécessaire de trouver des solutions de protection des données tout en reconnaissant leur utilisation commerciale. Mettre en confiance l'utilisateur ou le consommateur de technologie quant à ses données personnelles est essentiel pour favoriser le développement économique européen dans ce domaine[77]. Il est important pour l'Europe que les européens aient confiance en l'économie numérique afin qu'il n'y ait pas de frein à l'utilisation des nouvelles technologies due à une mauvaise protection données personnelles.

De plus, l'instauration d'une telle confiance par le biais de la protection des données personnelles permettrait de développer l'innovation en Europe. Les données personnelles sont les piliers sur lesquels repose l'innovation numérique. Certains pensent que la protection des données est un frein au développement de ces technologies mais c'est le contraire car comme le reconnaissent les autorités européennes, l'innovation et la protection des données sont aujourd'hui étroitement liées. La bonne santé de l'économie liée au numérique dépend du degré de confiance des consommateurs dans la technologie et donc de l'importance accordée à la protection des données personnelles lors de l'utilisation de ces technologies[78].

Cette prise de conscience européenne concernant l'impact de la protection des données sur l'économie numérique montre que l'Europe prend en compte la dimension économique des données. Les autorités européennes reconnaissent que les données sont une véritable manne financière autant du fait de la commercialisation dont elles font l'objet que du fait que leur protection peut être très bénéfique pour l'économie numérique. C'est sur cette base que le projet a été élaboré. Par conséquent, il semblerait que l'Europe prenne le chemin d'une qualification en faveur des droits extarpatrimoniaux concernant la nature des données personnelles. En effet, le texte devra concilier cette dimension économique des données avec un niveau de protection élevé.
Le but serait de rapprocher notre système du système américain en terme de commercialisation des données tout en augmentant le niveau de protection en y ajoutant de nouveaux droits: projet ambitieux mais qui semble efficace. Pourtant, cela fait des années que des discussions ont lieu sur le projet qui subit les pressions d'un puissant lobbying. Il est effectivement difficile de convenir à tout le

[77] « Proposition de règlement du Parlement européen et du Conseil 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 », *ibid*.
[78] ANONYME, « Enjeux 2015 (2) : la protection des données, clé de voûte de l'innovation », http://www.cnil.fr, 16 avril 2015.

monde. En ce qui concerne les pays européens, ils ont des avis partagés, certains comme l'Allemagne sont favorables à une protection élevée, tandis que d'autres préfèreraient un abaissement du niveau de protection comme le Royaume Uni. La Commission européenne serait sensible au système plus laxiste existant aux Etats Unis alors que le Parlement européen est partisan d'un niveau de protection élevé. S'ajoute à tout cela une activité extrêmement forte des groupes de pressions, ce qui fait qu'aujourd'hui le règlement européen est toujours en discussion. Certains espèrent qu'il soit adopté avant la fin 2015, pendant que d'autres essayent encore de retarder sa sortie[79].

Un des points épineux du règlement concerne la définition des données personnelles. En effet, il existe un débat sur les catégories d'informations devant rentrer ou non dans la définition des données personnelles. Il existe deux catégories de données. Il y a celles qui permettent directement ou raisonnablement d'identifier un individu[80] comme par exemple celles faisant apparaitre le nom ou le prénom, le numéro d'immatriculation ou le numéro de téléphone, ou encore l'adresse électronique qui font l'objet d'une protection. Pour celles-ci il n'y a pas de doute, elles rentrent bien dans la définition des données à caractère personnel puisqu'il s'agit de données portant sur des personnes identifiées ou identifiables et que grâce à ces données, les personnes sont identifiables et que des informations supplémentaires sur ces personnes peuvent être obtenues sans avoir besoin de réaliser un effort déraisonné[81]. Bien qu'une évolution de la notion de données à caractère personnel soit prévue dans le projet de règlement européen, le but est de renforcer la protection des individus par rapport à ses données donc il est nécessaire que cette catégories de données permettant d'identifier la personne restent dans la définition et il ne fait pas de doute qu'elles feront partie de cette définition dans le nouveau règlement. En revanche il y a une autre catégorie de données sur laquelle il y a un débat afin de savoir si elles doivent ou non rentrer dans la définition des données personnelles. Ce sont celles qui n'ont qu'un lien indirect avec l'individu ou bien celles qui seraient anonymisées comme les données de connexion par exemple qui ne permettent un rattachement à l'individu que par rapport à ses préférences et son parcours de navigation sur internet. Cela reste donc plutôt éloigné de la réelle identité de l'individu et certains souhaiteraient que cette catégorie de données ne rentre pas dans la définition des données à caractère personnel et ainsi ne bénéficie pas du même niveau de protection. Ce désaccord sur les éléments devant ou non renter dans la définition des données personnelles est une des raisons pour lesquelles le règlement européen n'a toujours pas été adopté. Il faut dire que cette question est essentielle. En effet, la qualification de cette deuxième

[79] FRAYSSINET (J.), *op. cit.*, p. 6.
[80] MOURON (P.), « Perspective sur le droit à l'identité numérique », L'ordre public numérique - Libertés, propriété, identité, Presses universitaires d'Aix-Marseille, 2015, p. 116.
[81] *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 38.

catégorie de données est essentielle et déterminera la voie que prendra l'Europe en matière de protection des données personnelles. L'Europe pourrait décider d'inclure les deux catégories de données pré-citées dans la définition des données à caractère personnel, ce qui reviendrait à avoir un droit de la protection des données à caractère personnel vraiment élargie et donc choisir la primauté de la personne sur la dimension économique. En revanche, choisir d'exclure les données n'ayant qu'un lien indirect avec la personne concernée reviendrait à rétrécir le domaine de protection et donc favoriser l'exploitation économique plutôt que la personne[82].

On voit qu'avec cette question de définition on en revient toujours à la nécessité de choisir entre la qualification de droit de la personnalité ou celle de droits patrimoniaux pour les données personnelles. La définition qui sera élaborée en droit européen sera déterminante quant au régime applicable aux données personnelles et quant à la détermination de leur nature. Si l'on choisit d'englober les données permettant un rattachement raisonnable à la personne ainsi que celles n'ayant qu'un lien indirect avec la personne concernée, on choisit une protection vraiment élevée et par conséquent plutôt un rattachement aux droits extarpatrimoniaux puisque l'ensemble de ces données seront soumises aux obligations à respecter en cas de traitement par un responsable. Celles-ci ne pourront pas être exploitées librement, cette exploitation sera soumise à autorisation. En revanche, si le choix est fait de n'intégrer dans la définition que les données ayant un lien avec la personne et permettant raisonnablement de l'identifier, cela conduirait à restreindre le champ de protection et de pencher plus vers un rattachement aux droits extrapatrimoniaux et d'autoriser sur cette catégorie de données l'exploitation commerciale. En effet, il serait possible d'exploiter sans autorisation et de façon commerciale l'ensemble des données ne permettant pas d'identifier directement la personne ou l'ensemble des données anonymisées d'une personne. Or, ces données chaque individu en possède énormément. Rien que les données de connexion sont de plus en plus importantes avec l'apparition des objets connectés. L'apparition des réseaux sociaux tels que Facebook augmente considérablement les données faisant apparaître les préférences des individus. Ne pas inclure ce type de données dans la définition du futur règlement conduirait à une acceptation de commercialisation de masse et sans contrôle de ces données. La dimension choisie serait donc plus la dimension patrimoniale étant donné que ces données pourraient alors être vendues et échangées de la même façon que n'importe quel bien.

Par conséquent, de ce choix de définition découlera le choix de nature des données personnelles et ainsi déterminera le niveau de protection dont bénéficieront les européens. La question de la défi-

[82] MOURON (P.), « Perspective sur le droit à l'identité numérique », *op. cit.*, p. 115.

nition des données personnelles dans le futur règlement européen est primordiale et déterminante pour le futur du droit à la protection de ces données. En même temps cette question peut s'apparenter a un cercle vicieux car faire une définition des données personnelles sans avoir clairement décidé de la nature que l'on devait leur donner est difficile. C'est la raison pour laquelle le règlement européen n'a toujours pas été adopté.

De plus, pour certains, les mots employés dans les ébauches de définition des données personnelles seraient trop vagues. En effet, la personne concernée dans le projet initial de règlement européen devait être définie comme « une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[83]. On avait une définition des données à caractère personnel qui était intégrée dans la définition de la personne concernée. Le lien entre les deux pouvait laisser penser que l'on choisissait un rattachement à la personne et donc aux droits extrapatrimoniaux. Cependant, le fait que les termes employés restaient très vagues permettaient d'avoir un doute sur ce choix. Par l'utilisation du terme « raisonnablement » étaient exclues de la protection un certains nombre de données à savoir celles qui ne permettaient pas raisonnablement d'identifier la personne. Ce n'est pas le choix d'un régime très protecteur puisque de nombreuses données peuvent entrer dans cette catégorie. D'autant plus que le terme « raisonnablement » s'il n'est pas clairement défini peut vouloir tout ou rien dire. Il n'y avait aucune indication sur ce que le terme « raisonnablement » englobait ou non. Or, le danger était que soit tiré de cette définition un champ d'application de la protection des données ne s'appliquant qu'à une catégorie restreinte de données, à savoir celles permettant d'identifier clairement la personne. Toute une catégorie de données ne permettant pas d'identifier clairement la personne n'aurait pas bénéficié de la protection. Par conséquent, il est important de clarifier ce que signifie le terme « raisonnablement » ou bien de trouver une définition plus claire qui n'aura pas besoin de donner lieu à des tas d'interprétations par les tribunaux. Il serait préférable d'avoir une définition claire, précise quant au régime et à la nature des données personnelles qui ainsi n'aurait pas besoin de donner lieu à interprétation et permettrait une application unifiée du droit à la protection des données en Europe.

[83] MARTIAL-BRAZ (N.), ROCHFELD (J.) et GATTONE (E.), « Quel avenir pour la protection des données à caractère personnel en Europe ? » , *Recueil Dalloz*, 2013, p. 2789.

Le G29 a donc tenté de poser des critères afin d'étendre le champ de la protection et de préciser les incertitudes existant sur ce terme de « raisonnablement identifiable ». Le premier critère est celui de la singularité selon lequel une donnée à caractère personnel serait toute donnée permettant de singulariser l'individu parmi les autres. Cela signifie que serait considérée comme une donnée à caractère personnel toute donnée permettant de distinguer un individu en particulier par rapport au groupe d'individus. Il y a ensuite le critère de la finalité du traitement réalisé. Grâce à ce critère, serait une donnée personnelle bénéficiant de la protection toute donnée qui subirait un traitement dont le but est d'identifier la personne ou bien de la rendre identifiable. Concernant les moyens permettant « raisonnablement » d'identifier une personne, ce serait ceux existants au moment de l'appréciation et qui permettraient de rendre identifiable une personne[84].

Avec cette définition et ces précisions qui interviennent en parallèle, on aboutit à quelque chose de plutôt complexe, car il faut trop interpréter, chercher et préciser le sens des mots. Par conséquent, l'objectif de simplification qui est portant essentiel si on veut une bonne application du droit et une bonne protection des données personnelles n'est pas rempli.

Une proposition de la Commission LIBE fait disparaitre la définition de la personne concernée et divise les données personnelles en deux catégories : d'un côté les données classiques ou ordinaires et celles dites pseudonymisées ou encryptées. Le problème est que ces termes ne sont pas clairs et ne sont pas accessibles à tous. On aboutirait là encore à une complexification du droit de la protection des données qui serait difficilement lisible, que cela soit pour les professionnels du droit ou pour les individus concernés par la collecte de données[85].

Ces problèmes paralysent en partie l'adoption du texte. Un autre débat existe en Europe concernant le consentement des personnes à un traitement de leurs données. Le but du projet de règlement européen était de renforcer ce consentement. Dans la législation actuelle, un traitement n'est mis en oeuvre que dans le but pour lequel le consentement a été donné, sauf exceptions énoncées par les textes. Dans le projet de règlement, un traitement peut être réalisé dans un autre but que l'objectif initial et notamment si le responsable de traitement y voit un intérêt légitime. Là encore le terme « intérêt légitime » reste vague car tout et n'importe quoi peut être présenté comme un intérêt légitime. Cela ouvre la porte à une liberté dans la réalisation de traitements qui pourront être faits sans le consentement des personnes. L'intérêt légitime du responsable de traitement pourrait très bien

[84] MARTIAL-BRAZ (N.), ROCHFELD (J.) et GATTONE (E.), op. cit, p. 2791.
[85] MARTIAL-BRAZ (N.), ROCHFELD (J.) et GATTONE (E.), *op. cit.*, p 2793.

être un intérêt économique comme par exemple l'exploitation ou la récolte des données à des fins publicitaires, la revente de telles données à des entreprises par les réseaux sociaux afin que celles-ci réalisent de la publicité ciblée. Or, là on serait bel et bien dans une dimension patrimoniale des données personnelles[86]. Cela reviendrait à accepter implicitement une reconnaissance patrimoniale des données personnelles puisque on ne doute pas du fait que les responsables de traitement invoqueront l'intérêt économique comme intérêt légitime pour exploiter les données personnelles des individus sans leur consentement direct pour cette utilisation spécifique.

De plus, la façon dont le consentement est recueilli peut aussi être critiquable. Il n'est rien prévu dans le projet de règlement pour régler ce problème. En effet, la plupart du temps la demande de consentement se manifeste par une case à cocher par l'internaute qui n'est pas forcément bien averti des conséquences que pourraient avoir son choix. D'autant plus qu'il est parfois nécessaire d'autoriser la collecte de données pour accéder à certains sites, les internautes acceptent alors sans connaitre forcément les conséquences. Même lorsqu'il est possible de ne pas accepter une telle collecte, l'internaute n'est pas toujours informé du fait qu'il a la possibilité de refuser. Il faut aussi souvent accepter des conditions générales que l'internaute ne lit pas car elles sont trop longues et complexes. Ce manque d'information du public à propos du consentement n'est pas réglé dans le projet de règlement tout comme les techniques que l'on peut qualifier de légères en ce qui concerne le recueil du consentement[87].

Finalement, on hésite beaucoup, l'Europe a du mal à qualifier les données à caractère personnel de droits patrimoniaux car il y a une crainte que cela fasse un tolet auprès du public et que cela amène vers une faible protection de ces données. Or, aujourd'hui, la patrimonialisation des données ne semble plus discutable[88] et bien réelle et c'est le manque de précision et l'absence de choix de nature pour les données personnelles dans leur définition qui paralyse le droit de la protection et empêche d'avoir une protection réellement efficace. Il vaudrait peut être mieux évoluer avec la technologie et avec son temps en reconnaissant explicitement et juridiquement cette patrimonialisation de fait des données personnelles. Il vaudrait en effet mieux coller à la réalité, cela offrirait un droit plus clair, plus accessible et donc a fortiori une meilleure application du droit et une meilleure protection des données personnelles.

[86] MOURON (P.), « Perspective sur le droit à l'identité numérique », *op.cit.*, p. 119.
[87] MARTIAL-BRAZ (N.), ROCHFELD (J.) et GATTONE (E.), *op. cit.*, p 2791.
[88] MOURON (P.), « Perspective sur le droit à l'identité numérique », *ibid.*

Il convient également de préciser que le droit à la portabilité des données ne sera certainement plus considéré comme un droit mais comme une simple incitation. Ainsi, les responsables de traitement seraient simplement incités à mettre en place des formats interopérables permettant un échange facilité des données[89]. Cette disposition pourrait laisser penser que l'on favorise l'individu plutôt que la libre circulation et la dimension économique puisqu'une telle disposition pourrait freiner quelque peu la libre circulation des données. Une incitation n'est pas aussi forte qu'une obligation. Cependant, les choses ne sont pas aussi simples que cela, et au fil des dispositions présentes dans le projet de règlement, il est difficile de voir de quel côté l'Europe voudrait pencher.

Mise à part ces importants problèmes de définition, le projet de règlement prévoit un certain nombre de règles innovantes. Un des objectifs est notamment d'alléger les procédures administratives. Pour cela, le projet prévoit une innovation majeure en remplaçant les procédures classiques de déclaration administrative auprès des autorités de protection nationale par la mise en place par les responsables de traitement d'une analyse de risque. Grâce à cette analyse, seuls les projets qui seront jugés comme représentant un risque devront être soumis aux formalités administratives devant les institutions de protection nationale. Le responsable du traitement devra ainsi comparer les répercussions que pourra avoir le traitement des données en question sur les libertés des personnes concernées par le traitement. Cette analyse permettra d'identifier si le traitement comporte un risque ou non. Le projet de règlement prévoit également une liste des traitements susceptibles de présenter des risques afin d'aider les responsables de traitement dans leur analyse[90]. Cette nouvelle procédure permettrait de responsabiliser davantage les entreprises et les responsables de traitement dans leur collecte et traitement de données.

Dans la même idée de responsabilisation des entreprises, le projet de règlement prévoit que lorsqu'une violation des données personnelles a lieu, cela sera au responsable de traitement d'en informer l'Autorité nationale de contrôle (par exemple la CNIL en France). De la même manière, si cette violation est susceptible de porter atteinte aux droits ou aux intérêts légitimes de la personne victime du traitement, le responsable de celui-ci devra lui-même informer la personne concernée de ce manquement[91].

[89] REES (M.), « Droit à l'oubli, etc. Les eurodéputés votent le Règlement Données personnelles », http://www.nextinpact.com, 13 mars 2014.
[90] POIDEVIN (B.), « Les apports du projet de règlement européen du 25 janvier 2012 relatif aux données personnelles », http://www.village-justice.com, 1er avril 2015.
[91] POIDEVIN (B.), *op. cit.*

Il y a donc une réelle volonté de responsabiliser et d'impliquer le responsable de traitement. Il y a une sorte d'échange qui est prévu : d'un côté le travail du responsable de traitement est facilité en Europe car il y a moins de lourdeur administrative et que les échanges de données entre les pays européens sont facilités et en contrepartie il doit s'investir davantage dans l'étude des traitements. Il y a une responsabilisation dans le sens où il n'est pas dans l'intérêt des entreprises de perdre la confiance de leur client en raison d'un problème qui serait survenu lors du traitement de leurs données. Par conséquent, elles ont intérêt de se conformer à la loi et d'effectuer un traitement loyal des données. Cette nécessité est donc accentuée par ces nouvelles règles prévues par le projet de règlement puisque cela sera désormais les entreprises qui effectueront les analyses afin de voir si un traitement ne porte pas atteinte au droit des personnes et en cas de problème elle devront en personne avertir leur client. Cela peut les placer en position délicate car elles ne pourront plus se cacher derrière les institutions nationales, elles seront directement jugées par leur clients. Les entreprises traitant des données personnelles seront donc incitées à réaliser un traitement bien en conformité avec le droit en vigueur.

Cette volonté de responsabilisation se manifeste également par l'apparition de deux concepts d'origine anglosaxonne dans le projet de règlement. Tout d'abord c'est celui de l'accountability qui consiste pour l'entreprise à avoir une analyse de ses bonnes pratiques ou de ses failles en matière de protection des données. L'entreprise devra alors analyser ses forces et ses failles et ensuite tout mettre en oeuvre pour augmenter les actions positives et diminuer les failles en matière de protection. Le deuxième concept est celui du privacy by design qui a pour but d'instaurer des obligations à la charge du responsable de traitement. Ce concept peut rendre obligatoire la mise en place d'un règlement interne afin de mieux respecter le droit en matière de protection des données[92]. Les entreprises seront vraiment responsabilisées à l'issu du nouveau règlement et deviendront de véritables acteurs de la protection des données. Si l'on demande aux entreprises de s'investir autant, c'est peut être que l'on veut les responsabiliser afin de concilier protection des données et exploitations économiques de celles-ci.

Un des points positifs est également le renforcement du droit à l'effacement puisque toute personne pourrait obtenir l'effacement de lien menant à ses données personnelles dès lors qu'un tribunal ou une décision d'une autorité règlementaire de l'Union européenne ayant considéré que les données

[92] MOHAMED (R.), « Données personnelles : les impacts du futur règlement européen » : une conférence au sommet pour l'AFDIT », http://www.linkipit.com, 16 avril 2014.

devaient être effacées a acquis force de chose jugée ou dès lors que les données font l'objet d'un traitement illicite[93].

Le droit à l'oubli ne serait pas en reste lui non plus puisque le texte entend le consacrer pleinement. Les eurodéputés souhaitent consacrer ce nouveau droit dégagé par la jurisprudence afin qu'il connaisse une application vraiment efficace. Ces mesures devraient concerner au premier chef les moteurs de recherche. Cependant, les destinataires des demandes d'effacement pourront opposer le droit à la liberté d'expression ou une mission de recherche scientifique, historique ou statistique et selon les cas, auront la possibilité de simplement rendre l'accès plus difficile aux données[94].

Les sanctions financières pouvant être prononcées en cas de violation du droit de la protection des données ou de traitement illégal de données devraient également être augmentées[95]. En cas de manquement aux obligations posées par le règlement, il a été proposé que l'amende puisse atteindre 100 millions d'euros ou au minimum 5% du chiffre d'affaire annuel mondial[96]. Ces sanctions administratives restent plutôt sévères, ce qui montre une volonté de l'Union européenne qu'il y ait un vrai respect de la protection des données personnelles et qui donne une idée de l'importance du respect de cette protection.

Il faut préciser que les collectivités européennes sont critiques voire opposées au renforcement de la protection des données personnelles. Elles réclament qu'une distinction entre le secteur privé et le secteur public soit intégrée dans le règlement afin de leur faciliter la tâche. De plus, elles craignent une surcharge administrative et par conséquent demandent à ce que le droit à l'oubli ne s'applique qu'aux GAFA. Elles craignent une surcharge de travail et de coûts pour pas grand chose puisque pour elles l'impact sur les droits des citoyens ne serait pas révolutionnaire. Les pays eux-mêmes sont « frileux » par rapport à l'adoption de ce texte. La Grande Bretagne reste hostile au projet, certains pays tentent de retarder l'adoption du texte[97]. D'autres sont plus favorables à son entrée en vigueur, la France par exemple. La CNIL a même créé un label sur la gouvernance informatique et

[93] POIDEVIN (B.), *op. cit.*
[94] REES (M.), *op. cit.*
[95] AUFFRAY (C.), « Données personnelles : nous aurons le règlement européen en 2015 », http://www.zdnet.fr, 28 janvier 2015.
[96] POIDEVIN (B.), *op. cit.*
[97] VANDYSTADZT (N.), « Les collectivités européennes opposées au renforcement de la protection des données personnelles », http://www.lagazettedescommunes.com, 18 novembre 2014.

liberté qui permettrait en amont de mettre les responsables de traitement en conformité avec le futur règlement européen[98].

Ce que l'on peut dire c'est que ce projet contient de bonnes initiatives qui semblent vouloir trouver un équilibre entre l'exploitation commerciale des données et la protection de ces données. Cependant, il semblera difficile de les rendre efficaces tant que l'Europe n'aura pas fait un choix entre d'un côté la primauté de la personne sur la dimension économique et de l'autre la libre exploitation économique de ces données, du moins dans la définition de la notion de données personnelles[99]. Même en lisant le règlement, le fait d'y retrouver des points d'avance en matière de protection et en même temps des domaines où l'on recule ne permet pas d'identifier le choix fait par l'Europe. Ce choix sera certainement nécessaire à faire. Certains disent que le fait que le règlement reprenne dans son intitulé le terme de « libre circulation » prouve que l'Europe serait prête à accepter le côté patrimonial des données[100].

Certains vont même encore plus loin et se demandent s'il ne serait pas plus simple d'instaurer un droit de propriété sur les données à caractère personnel. Cette situation qui de prime abord pourrait paraître farfelue pourra peut être se révéler être une solution aux problèmes de définitions présentés ici.

[98] BONNET (F.), « La CNIL crée un label sur la gouvernance des données personnelles », http://www.journaldunet.com, 19 janvier 2015.
[99] MOURON (P.), « Non commercialité d'un fichier de données non déclaré à la CNIL », *op. cit.*, p. 319.
[100] STORRER (P.), *op. cit.*, p. 1844.

II. La possible instauration d'un droit de propriété sur les données personnelles.

Il conviendra de démontrer qu'il est possible d'effectuer l'application des caractéristiques de la propriété aux données personnelles (A) avant de se pencher sur l'évolution des droits de la personnalité vers le droit de propriété (B).

A) L'application des caractéristiques de la propriété aux données personnelles.

A l'heure actuelle le débat, en France comme en Europe, va encore plus loin que l'idée de la patrimonialisation et se déplace vers l'idée de la possible instauration d'un droit de propriété sur les données personnelles. De prime abord, cette assimilation peut choquer ou surprendre. Cependant, lorsque l'on analyse les décisions de justice phares de ces dernières années, on se rend compte que certaines d'entre elles pourraient servir de fondement à une telle assimilation. En effet, l'évolution jurisprudentielle de ces dernières années en matière de données pourrait laisser penser que l'on se dirige vers une éventuelle instauration d'un droit de propriété sur les données à caractère personnel. Pour le moment, cette instauration n'a pas lieu. Cependant, lorsque l'on s'intéresse de façon attentive à la réalité de l'utilisation des données personnelles, on se rend compte que l'instauration du droit de propriété pourrait résoudre certains problèmes de régime ou encore de définition des données personnelles.

Le 13 mai 2014, la Cour de justice de l'Union européenne a rendu un arrêt opposant Google Inc. (le siège de Google) et Google Spain (le filiale espagnole de Google) à l'agence espagnole nationale de protection des données : l'AEPD. Cet arrêt a fait énormément parler de lui car il est présenté comme l'arrêt qui consacre le droit à l'oubli. Ce terme est d'ailleurs un peu fort car l'oubli sur internet n'existe pas pleinement. Il est extrêmement difficile de faire disparaitre complètement une information ou une donnée une fois que celle-ci a été mise sur internet. Il sera possible de faire disparaitre l'information à certains endroits et de rendre plus difficile l'accès à celle-ci mais elle ne disparaitra jamais complètement. Ainsi, la notion d'oubli sur internet est relative et il est préférable de parler de droit au déréférencement[101]. C'est un tel droit que l'arrêt de la CJUE est venu reconnaitre.

[101] FRAYSSINET (J.), *op. cit.*, p. 1.

En l'espèce, un ressortissant espagnol, en tapant son nom dans la barre de recherche du moteur de google spain s'est aperçu qu'il y avait dans la liste de résultat deux liens renvoyant sur le site d'un quotidien qui mentionnait son nom à l'occasion d'une vente aux enchères immobilières qui avait été organisée en 1998 aux fins de recouvrement d'une dette. Par conséquent, le ressortissant espagnol a saisi l'AEPD dans le but de faire supprimer ces informations ou du moins que celles-ci n'apparaissent plus dans la liste de résultats. L'autorité de protection des données espagnole a accueilli la demande concernant les sociétés Google Inc et Google Spain. Ces dernières ont alors intenté un recours devant la Haute juridiction nationale. Celle-ci a décidé de saisir la Cour de justice de l'Union Européenne de plusieurs questions préjudicielles. Parmi ces questions, l'une touchait ce que l'on appelait déjà le droit à l'oubli. Avant de se prononcer sur cette question, la CJUE a procédé par étape et c'est seulement après avoir démontré que l'activité du moteur de recherche était bien un traitement de données personnelles dont la société était responsable et que la directive s'appliquait bien aux traitements réalisés par la filiale de Google Spain pour le compte de Google Inc qu'elle s'est prononcée sur l'existence d'un droit de suppression des données personnelles d'un internaute présentes dans la liste de résultats d'un moteur de recherche[102].

La Cour va donner comme fondement à l'arrêt les articles 12 b) et 14 a) de la directive de 1995 qui prévoient respectivement un droit à l'effacement des données de la personne concernée en cas de traitement non conforme aux règles prévues par la directive et la possibilité par la personne concernée par un traitement de s'opposer à ce dernier pour des raisons légitimes tenant à sa situation particulière. C'est en ce sens que la Cour va véritablement consacrer le droit à l'oubli puisque les autres décisions qui avaient été rendues étaient fondées sur la violation de la vie privée[103].

La Cour interprète donc ces deux dispositions et précise que pour qu'elle soient respectées « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite. » et que « la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche ef-

[102] CASANOVA (A.) et VERET (D.), « La consécration d'un droit à l'oubli … principalement pour les anonymes », *Lamy Droit de l'Immatériel*, 2014, n°106, p. 90.
[103] CASANOVA (A.) et VERET (D.), *op. cit.*, p. 91.

fectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. »[104].

Ainsi, tout internaute peut désormais demander à un moteur de recherche la suppression des liens vers des pages web faisant apparaitre ses données personnelles et sans qu'il soit nécessaire que celle-ci ait subi un préjudice du fait de la présence de ces liens dans la liste de résultats. De plus, l'arrêt précise que ce droit prévaut sur l'intérêt économique de l'exploitant du moteur de recherche ainsi que sur l'intérêt du public à accéder à cette information lors d'une recherche sur le nom de cette personne. Ce droit est plus reconnu pour les anonymes que pour les personnages publics car pour ces derniers l'intérêt du public à recevoir l'information prévaudrait sur ce droit à l'oubli[105]. L'arrêt pose tout de même une limite à ce droit au déréférencement, car la Cour prévoit qu'il faudra réaliser une mise en balance des intérêts en présence et vérifier que la demande de déréférencement est légitime par rapport aux conséquences négatives qu'elle pourrait avoir sur les autres droits tels que la liberté d'expression par exemple[106].

En y regardant de plus, près cette décision pourrait être considérée comme une reconnaissance implicite d'un droit de propriété sur les données. En effet, l'article 544 du code civil définit la propriété comme le droit de jouir et de disposer des choses de façon absolue tant que l'on n'en fait pas un usage interdit par la loi ou les règlements[107]. Etre propriétaire signifie posséder un bien quelle que soit sa nature et avoir sur ce celui-ci l'usus, le fructus et l'abusus, à savoir disposer du droit d'en user, d'en jouir et d'en disposer. Pour qu'il y ait propriété, il faut donc nécessairement que l'on ait ces trois éléments, le droit d'en abuser étant particulièrement essentiel[108]. Ici ce serait les données personnelles qui seraient qualifiées de bien. Or, il semble judicieux de qualifier ces données de bien incorporel. Cette catégorie correspond, par opposition aux biens corporels, aux biens qui échappent à toute appréhension matérielle, aux biens qui sont impalpables[109]. C'est bien le cas des données personnelles lorsqu'elles se retrouvent sur internet on ne peut pas les toucher, elles sont immatérielles.

---

[104] CJUE, GC, Google Spain SL et Google Inc. c/ Agencia Espanola de proteccion de Datos (AEPD), 13 mai 2014, aff. C-131/12.
[105] CASANOVA (A.) et VERET (D.), *op. cit.*, p 92.
[106] PERRAY (R.), « La Cour de justice, les moteurs de recherche et le droit « à l'oubli numérique » : une fausse innovation, de vraies questions », *Lamy Droit de l'immatériel*, 2014, n° 109, p. 38.
[107] Code civil
[108] DROSS (W.), « Une approche structurale de la propriété », *RTD civ.*, octobre 2012, n°3, p. 419.
[109] CORNU (G.), *op. cit.*, p. 480.

Dans cet arrêt, la Cour, en consacrant le droit à l'oubli, permet à chaque internaute sous des condition assez souples de décider de faire disparaître des listes de résultats des moteurs de recherche des données personnelles le concernant. Cela signifie que sur ses propres données, une personne va pouvoir décider de les faire disparaitre ou de les maintenir à disposition du public. Bien évidemment, nous avons vu que la disparition complète sur internet n'existait pas mais avec cette consécration du droit au déréférencement, il sera possible de rendre l'accès aux données plus difficile voire quasiment impossible. Il serait donc possible d'assimiler cela à une suppression des données personnelles si plus aucune personne tiers n'y a accès. Dans le droit de propriété, l'abusus signifie le droit de détruire la chose qui nous appartient. Or, avec la consécration du droit au déréférencement, il serait alors possible que l'abusus existe sur les données personnelles. C'est une réaction circulaire qui se produit. S'il existe un droit d'abuser de la chose sur les données, c'est qu'elle est considérée comme un bien. Or, la considérer comme un bien permettrait de la vendre sans problème et d'intégrer la dimension commerciale qui est largement une réalité aujourd'hui. De plus, dans cet arrêt, même s'il peut être interprété comme une volonté de rattacher la donnée à un bien et à la possibilité de l'existence d'un droit de propriété de celle-ci, on voit que cela n'empêche pas de laisser les droits des personnes concernées intacts. En effet, tout en ouvrant vers la possibilité de laisser naître un droit de propriété sur les données à caractère personnel, la Cour rappelle l'importance de faire primer le respect de ces données et des droits des personnes concernées. C'est d'ailleurs pour cela que que l'arrêt est rendu: pour protéger la vie privée de la personne concernée.

La conciliation entre droit de propriété et protection des données personnelles semble donc possible, certains pensent même que cela serait la meilleure solution.

Nous avons vu dans un premier temps que le glissement vers la catégorie des droit patrimoniaux était envisageable mais il semble évident que la question de la propriété sur les données se pose lorsque les individus acquièrent une maîtrise renforcée sur leur données.

Tout d'abord, le fait même de numériser les éléments personnels tels que le nom, l'adresse ou encore les préférences, entraine un détachement de ces éléments par rapports à la personne. Surtout lorsque ces éléments qui sont en réalité des données sont mis sur internet, puisqu'a partir de là, tout comme des choses, elles pourront circuler indépendamment de la volonté de leur propriétaire[110]. Le droit de propriété sur les données pourrait donc se déduire de la façon dont les données sont utilisées.

[110] MOURON (P.), « Perspective sur le droit à l'identité numérique », *op. cit.*, p. 118.

En premier lieu, si on prend l'arrêt de la Cour de cassation du 25 juin 2013 précédemment cité, le fichier a été considéré par la Cour comme étant hors commerce. Or, on ne peut qualifier une chose de hors commerce que lorsque celle-ci est appropriée, c'est à dire lorsque une personne exerce sur elle un droit de propriété. En l'espèce, le fichier de clientèle, constitué de données personnelles, est par conséquent considéré comme un bien dans cette décision. A fortiori cela signifie que le bien peut être porteur d'une valeur économique et surtout la qualification de bien entraine la possibilité de l'existence d'une propriété[111]. Lorsqu'il y a un bien il y a propriété. Cette décision a été rendue pour un fichier de clientèle mais cela représente une avancée puisque celui-ci est composé de données personnelles. Cette jurisprudence ouvre la porte au juge afin que celui-ci l'applique aux autres catégories de données personnelles.

Une des premières questions à laquelle on peut être confronté est celle du propriétaire. On pourrait se demander de qui il s'agit. Théoriquement, cela sera celui qui possède sur les données l'ensemble des prérogatives à s'avoir l'usus, le fructus et l'abusus. Il semble logique de penser que le propriétaire sera le producteur de données.

Ensuite, il faut vérifier comment les caractères du droit de propriété peuvent s'adapter au données personnelles. En doctrine, il est aujourd'hui établi que l'on arrive à justifier l'existence de l'usus et du fructus. C'est l'existence du pouvoir de disposer de ces données, donc l'abusus, qui posait problème. Cependant, l'arrêt de la CJUE du 13 mai 2014 en consacrant le droit au déréférencement apporte peut être une solution à cela.

En effet, l'usus est le droit d'utiliser le bien, d'en jouir. Si on prend les données personnelles, chaque internaute en produit alors qu'il n'y est pas obligé. Il a le choix par exemple de s'inscrire sur Facebook ou de ne pas le faire. De plus, lors de la réalisation d'une telle inscription, il est demandé à l'internaute s'il accepte que la collecte de ses données soit réalisée. A ce moment-là, on lui propose de cocher une case. L'internaute en quelque sorte choisit de divulguer ses données personnelles. Il en va de même lorsque celui-ci se connecte à internet et que certains sites demandent de fournir des données personnelles: l'internaute est alors libre de choisir s'il veut quitter le site ou poursuivre en renseignant et en autorisant la divulgation de ses données personnelles. Bien évidemment, il y a un manque d'information certain de l'internaute qui fait que celui-ci, lorsqu'il s'inscrit sur un réseau social par exemple, n'a pas pleinement conscience de ce que signifie

[111] MOURON (P.), « Non commercialité d'un fichier de données non déclaré à la CNIL » *op. cit.*, p. 317.

l'autorisation de collecte des données personnelles de la même manière qu'être obligé de renseigner ses données personnelles pour accéder à un service en ligne force un peu la main de l'internaute. Cependant, dans les faits, celui-ci a le choix de la façon dont il va utiliser ses données personnelles et il est libre de choisir de les divulguer ou non. Par conséquent, on peut en déduire qu'il y a bien un droit d'usage qui existe sur les données personnelles.

En ce qui concerne le fructus, qui correspond au droit de profiter des fruits pouvant provenir du commerce du bien[112], nous savons qu'aujourd'hui les données personnelles font déjà l'objet d'une exploitation commerciale sur internet. C'est d'ailleurs pour entériner cet état de fait que le débat sur la propriété des données personnelles est apparu. Sauf qu'aujourd'hui, les bénéficiaires de l'exploitation des données sont les entreprises qui les utilisent, en instaurant un tel droit de propriété sur les données cela permettrait aux personnes concernées qui en seraient propriétaire d'en retirer les bénéfices directement. Il existe déjà dans certains pays des sortes de courtiers qui proposent aux personnes concernées de vendre leurs données afin qu'elle en retirent un bénéfice même minime. Par exemple, c'est ce que proposent des sites tels que datacoup ou yesprofile[113]. Le simple fait que les données aient une valeur économique montre qu'il est possible d'en retirer les fruits même si actuellement en Europe ce sont les entreprises qui récoltent le fruit des données des particuliers. En instaurant un droit de propriété sur les données, cela serait la personne concernée qui vendrait ses données comme n'importe quel bien. A partir du moment où il y a vente des données, l'existence d'un droit de fructus est possible[114]. En outre, si on regarde bien l'utilisation des données personnelles, on se rend compte que dans certains cas la personne concernée retire déjà les fruits de la divulgation de ses données. C'est notamment le cas quand l'accès à un service sur internet ou autre est rendu gratuit en échange de la divulgation des données personnelles. En effet, la gratuité pour l'internaute pourrait être vu comme une sorte de rémunération. C'est la plupart du temps le cas puisque ce système permet à tous les internautes d'accéder à une multitude de services divers et variés comme les applications qui pour bon nombre d'entre elles sont gratuites, les réseaux sociaux ou encore les moteurs de recherche. C'est un réel modèle économique qui s'est créée. Cela montre d'autant plus qu'un droit de fructus existe déjà sur les données personnelles. De plus, actuellement l'idée d'une possibilité de vendre ses données est de plus en plus présente et commence même à germer dans l'esprit des français. 46% des internautes français seraient ainsi prêts à révéler davantage d'informations et donc de données personnelles en échange d'avantages en nature ou bien fi-

[112]- MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *RLDI*, avril 2015, n°114, p. 61.

[113] GADDES (C.), « Parimonialisation des données personnelles », VIIIè conférence de l'AFAPDP à Bruxelles, le 25 juin 2015, p. 7.

[114] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *op. cit.*, p. 61.

nanciers. Certains accepteraient même un filage quotidien si celui-ci leur rapportait 500 euros par an[115].

Les choses sont moins évidentes à démontrer lorsqu'on aborde le droit d'abusus. En effet, pour certains auteurs, c'est l'élément manquant pour mettre en place un droit de propriété sur les données personnelles. Ce droit se définit comme le droit pour le propriétaire d'une chose d'en disposer par tout acte matériel ou juridique de transformation, de consommation, de destruction, d'aliénation ou encore d'abandon[116]. L'abusus comprend donc le droit de détruire le bien sur lequel on a la propriété. Avant la consécration du droit au déréférencement, il était difficile de concevoir ce droit de destruction sur les données personnelles, de s'imaginer dans quelle mesure il serait possible d'appliquer cette caractéristique aux données personnelles. Désormais, avec le droit au déréférencement, il est possible pour chaque internaute de demander la suppression de lien renvoyant vers ses données personnelles. A partir de là, ces données ne seront que très difficilement accessibles voire inaccessibles pour les autres utilisateurs d'internet. Cela pourrait donc s'analyser comme la reconnaissance d'un droit d'abusus sur les données personnelles. D'autant plus que ce droit est exercé par la personne concernée, par le propriétaire des données. Celui-ci peut décider de laisser ses données accessibles à tous mais il peut également demander à ce que ses données soient déréférencées, ce qui signifie quasiment qu'elles seront supprimées aux yeux de tous. Le propriétaire choisirait ainsi en quelque sorte de détruire ses propres données: il exercerait donc un droit d'abusus.

Evidemment, avant l'arrêt Google Spain de la CJUE, il était déjà possible de demander le retrait ou la cessation de traitement de ses données personnelles mais cela n'était le cas que lorsqu'elles étaient inexactes par exemple. Pour cette raison, on pouvait être un peut réticent à la reconnaissance de l'existence d'un droit d'abusus sur les données personnelles puisque les possibilité de demander le retrait étaient plutôt limitées et ne pouvaient avoir lieu que dans des cas précis. Aujourd'hui, il est possible de le faire même lorsque la personne concernée ne subit aucun préjudice, c'est à dire qu'elle ne souffre pas de l'accès que pourrait avoir des tiers à ses données. Ainsi, la possibilité d'obtenir le retrait de ses données personnelles est beaucoup plus large. Comme nous l'avons déjà dit, elle n'est pas illimitée puisqu'il est nécessaire de concilier le droit au déréférencement avec la liberté d'expression. Or, le droit de propriété classique ne s'exerce pas lui non plus de façon illimitée. En effet, la propriété est le droit de jouir d'une chose de la façon la plus absolue qui soit mais

[115] FERRAN (B.), « Les Français prêts à monnayer leurs données personnelles », lefigaro.fr, 26 octobre 2014.
[116] CORNU (G.), *op. cit.*, p. 8.

seulement à partir du moment où l'on n'en fait pas une utilisation qui serait prohibée par les lois ou les règlements[117].

Ainsi, il serait tout à fait possible d'instaurer un droit de propriété sur les données personnelles puisque l'on voit que l'utilisation réelle que l'on en fait fait apparaitre qu'il existe bien sur celles-ci un droit d'usus, de fructus et d'abusus. Alain Benssoussan prône d'ailleurs depuis une quinzaine d'années la nécessité d'instaurer un droit à l'oubli, au déréférencement qui ferait partie intégrante des droits de l'Homme numérique[118]. Bien évidemment, il précise que ce droit doit être concilié avec le droit à la liberté d'expression, le devoir de mémoire ainsi que le droit à l'histoire. Si le droit de propriété classique est limité dans le respect des lois et règlements il serait tout à fait possible d'instaurer un droit de propriété sur les données personnelles qui seraient limité par l'exercice d'autres droits fondamentaux.
De plus, l'instauration d'un droit à l'oubli ou au déréférencement va de paire avec l'instauration d'un droit de propriété sur les données. D'abord, cela permettrait comme nous venons de le dire d'avoir un droit d'abusus sur nos données et qu'ainsi les trois attributs de la propriété existent sur les données personnelles. Ensuite l'existence d'un droit à l'oubli numérique est indissociable du droit de propriété car il rendrait ce dernier encore plus efficace.

En effet, si l'idée d'instaurer un droit de propriété sur les données personnelles apparait aujourd'hui comme une solution envisageable, c'est parce que cela permettrait d'obtenir une protection des données personnelles plus efficace. Aujourd'hui, on ne peut plus se passer d'internet, on s'en sert pour de plus en plus de choses, comme effectuer des recherches, réserver un vol ou encore jouer en ligne ou utiliser les réseaux sociaux. Ce développement des usages d'internet entraine des transferts de données encore plus grands, ce qui au cours de ces dernières années a donné naissance à un véritable marché des données personnelles. Ce commerce s'exerce au détriment des internautes, c'est à dire des créateurs de données qui bien souvent ne connaissent pas l'utilisation qui est réellement faite de leurs données et ne sont pas complètement conscients du danger pour leur droit à la vie privée[119]. Par conséquent, l'instauration d'un droit de propriété au profit de la personne concernée, c'est à dire celle qui crée les données, serait une solution pour que celle-ci devienne maître de ses propres données.

[117] C. civ., art. 544.
[118] BENSOUSSAN (A.), « Le droit à l'oubli numérique : un droit naturel », www.alain-bensoussan.com, 6 février 2014.
[119] BENSOUSSAN (A.), « Faut-il réguler la marchandisation des données personnelles sur internet ? », blog.lefigaro.fr, 30 janvier 2013.

Dans un premier temps, cela aurait un côté pratique car il est plus pédagogique de parler de propriété sur les données personnelles vis à vis des profanes du droit. Le droit des données personnelles est un droit qui se révèle déjà complexe pour les praticiens étant donné qu'il s'agit d'un domaine qui connait une évolution rapide et où le droit est en train d'essayer de s'adapter. C'est donc un droit très peu lisible pour une personne lambda. Par conséquent, instaurer un droit de propriété est beaucoup plus parlant pour tout le monde. Tout à chacun sait que lorsqu'il a un droit de propriété, il est propriétaire de la chose et peut exercer un certains nombre de droits sur celles-ci. Aujourd'hui, par manque d'information et de lisibilité de la législation, les internautes ne sont pas toujours au courant des droits dont ils disposent sur leur données, ce qui fait que la protection qui est prévue par les textes se révèle être moins efficace que ce qu'elle devrait être. De plus, cela permettrait de décider de la personne qui a la propriété de ses données. Aujourd'hui, cela reste assez flou puisque les données sont considérées comme res nullius.

Dans un second temps, reconnaitre un droit de propriété sur les données personnelles permettrait de protéger ses données tout en collant à une réalité à l'heure actuelle qui est la commercialisation de ces données qui est un phénomène mondialisé et irréversible[120]. Le droit de propriété sur les données permettrait aux individus d'en avoir une réelle maîtrise et de les gérer comme ils l'entendent. L'individu pourrait décider de la publication ou non de ses données, il déciderait lesquelles devraient être considérées comme sensibles. Cela permettrait d'organiser leur protection, les modalités de détention et d'échanges de ces données de façon claire et précise[121]. En effet qui mieux que la personne concernée pourra se protéger de l'utilisation de ses données personnelles ? La personne agira dans son propre intérêt. De plus, des dispositions législatives existeront pour encadrer ce droit de propriété sur les données.

Le fait de disposer d'un droit au déréférencement va protéger les individus des utilisations qu'ils ne souhaitent pas voir être faites de leur données personnelles. Par conséquent, le droit de propriété combiné au droit à l'oubli donnerait à la personne concernée un réel pouvoir de maîtrise et de décision sur ses données personnelles. Cela éviterait également que la propriété des données tombe entre les mains de personnes mal intentionnées du fait qu'aujourd'hui on ne sait pas trop quoi englober dans la définition de données personnelles et que l'on ait du mal à choisir un régime à leur appliquer.

[120] TEXIER (B.), « Alain Bensoussan : je crois à l'émergence d'un marché des données personnelles », *Archimag*, n° 279, novembre 2014, p. 44.
[121] BENSOUSSAN (A.), « Faut-il réguler la marchandisation des données personnelles sur internet ? », *op. cit.*

Cela simplifierait les choses car on instaurerait un régime aux données personnelles par analogie à celui existant pour les biens corporels. Il serait possible d'adapter ce régime aux spécificités des données personnelles en prévoyant un régime protecteur de celles-ci mais cela éviterait de se perdre dans l'instauration d'un régime complexe, peu compris et ne prenant pas en compte la dimension commerciale. En effet, si on ne prend pas en compte cette propriété des données, le risque est que le droit qui va être mis en place notamment par l'union européenne au moment de sa sortie soit déjà obsolète.

Enfin, il ne faut pas oublier qu'en instaurant un tel droit de propriété sur les données, cela sera l'internaute qui bénéficiera au premier chef de l'exploitation de ses données. Il faudra très certainement pour pouvoir exploiter les données d'un internaute, en plus de son autorisation, lui octroyer un avantage en nature ou bien financier. Par exemple, un américain nommé Jaron Lanier conseille de mettre en place un système de micro-paiement généralisé afin de faciliter la monétisation des données personnelles. L'idée serait que les internautes reçoivent une rémunération minime en échange de la création d'une information personnelle. Pour lui, cette rémunération tomberait à un moment où la classe moyenne a de plus en plus besoin d'un soutien financier supplémentaire. Certains pensent que la rémunération serait minime mais selon lui c'est faux, car certaines données valent de l'or pour les entreprises qui seraient donc prêtes à mettre le prix pour les obtenir. En France, le fondateur de skyrock Pierre Bellanger est un fervent partisan de l'instauration d'un droit de propriété sur les données personnelles. Selon lui, il est nécessaire de rendre les individus propriétaires de leur données puisqu'il considère que les individus seraient les « auteurs » de leurs données personnelles[122].

En effet, certains ont pu évoquer la possibilité d'instaurer un droit de propriété en se fondant sur l'existence d'un droit d'auteur. Une telle proposition a été évoquée pour résoudre certains problèmes que poserait la propriété classique. L'avantage du droit d'auteur est qu'il se divise entre les droits moraux qui sont incessibles et les droits patrimoniaux qui eux sont cessibles. Il est vrai qu'il semble idéal de séparer les données personnelles en deux catégories : d'un côté les plus sensibles qui ne pourraient pas faire l'objet d'une cession et de l'autre celles qui sont moins importantes, moins sensibles et qui pourraient être cédées sans problème. Cependant, l'application du droit d'auteur ne peut intervenir que lorsque certaines conditions sont remplies. Il faut en effet que l'on puisse les qualifier d'oeuvres de l'esprit et qu'elles soient reconnues comme étant originales. Ce-

[122] MOREL (L.), « Le CNNum s'est prononcé contre l'instauration d'un droit de propriété privée sur les données personnelles », http://scinfolex.com, 19 juin 2014.

pendant, il semble difficile de reconnaitre cette qualification d'oeuvre de l'esprit à certaines données personnelles et notamment celles qui sont générées automatiquement. C'est le cas par exemple de l'adresse IP, du numéro de téléphone ou encore du numéro de sécurité sociale. Si l'on arrivait a démontrer qu'une donnée personnelle est une oeuvre de l'esprit, il faudrait encore que celle-ci soit originale. Encore moins de données pourront bénéficier de cette reconnaissance. Beaucoup d'entres elles nécessitent d'être protégées. Cependant, elles sont générées par des algorithmes déterministes qui ne laissent part à aucun apport de la personnalité de l'auteur[123]. Certains pourront dire que comme cela touche à l'essence de la personne et que les résultats sont obtenus en fonctions des caractéristiques particulières de chaque personne, on peut donc déceler la personnalité de l'auteur. Certains diront que rien ne porte mieux la marque de la personnalité de l'auteur que l'ensemble de données définissant un individu en tant qu'être unique[124]. Cependant il ne s'agira pas d'un choix personnel de l'auteur, chaque personne subit ses caractéristiques physiques comme le fait d'être une femme par exemple. Ainsi le numéro de sécurité sociale qui se composerait du numéros issus des caractéristiques physiques des personnes ne pourrait être qualifié d'original.

La question pourrait éventuellement se poser pour les données qui sont sciemment crées par l'individu comme par exemple le fait de donner un prénom très original à son enfant. Cependant, cela serait très difficile à gérer et risquerait d'avoir des conséquence néfastes. En effet, une fois que le droit d'auteur est instauré, il faut lui demander la possibilité de réutiliser son oeuvre. Dans ce cas, si l'on reprend l'exemple du prénom, il faudrait qu'à chaque fois que des parents décident de donner un nom déjà utilisé à leur enfant, on leur demande l'autorisation d'utiliser le prénom en question. Cela bloquerait les individus qui devraient sans arrêt demander l'autorisation pour telle ou telle chose et cela deviendrait très lourd à gérer pour tout le monde[125].

De plus, les données personnelles prennent souvent de la valeur lorsqu'elles sont traitées, agglomérées par une entreprise. Cela serait éventuellement là que l'originalité pourrait se trouver. Puisqu'il y a à ce moment-là un choix de croisement de données qui est fait, l'entreprise choisit quels groupes de données elle va traiter ensemble par exemple. Le problème est que dans ce cas cela ne serait pas le particulier qui bénéficierait du droit d'auteur mais plutôt l'entreprise qui s'occupe du traitement. Par conséquent, cela aurait là encore des conséquences néfastes car le risque est que l'individu serait dépossédé de ses données personnelles. Cette solution ne semble donc pas envisageable.

[123] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *op. cit.*, p. 62.
[124] CHEMLA (L.), « Nous sommes tous des ayants droits », http://blogs.mediapart.fr, 23 octobre 2013.
[125] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *op. cit.*, p. 62.

Enfin, si on y regarde de plus près, ce sont les parents qui donnent les caractéristiques à leur enfant et qui d'une certaine façon lui créent son état civil. Par conséquent, ce serait donc les parents qui pourraient être considérés comme les détenteurs des droits d'auteurs sur les données de leurs enfants puisqu'il en seraient les créateurs. Dans une telle hypothèse, les enfants devraient demander l'autorisation de leurs parents pour utiliser leurs données à caractère personnel. De plus, ce serait les parents qui bénéficieraient des avantages en nature ou financiers issus de la revente des données personnelles[126].

Ce qui semble gênant dans une assimilation au droit de propriété par le biais du droit d'auteur c'est que cela ne serait pas celui auxquels les données appartiennent qui bénéficierait des avantages. De la même façon, il faudrait sans cesse demander l'autorisation pour utiliser ses propres données. Du coup, une telle assimilation semble moins adaptée. Certains parfois ont aussi parlé de la possibilité de mettre en place un droit voisin sur les données personnelles ou même de créer un droit sui generis comme celui existant sur les bases de données. D'ailleurs quand on y pense un espace rassemblant l'ensemble des données personnelles pourrait être assimilé à une base de données. Quoi qu'il en soit, ce qu'on peut déduire de toutes ces propositions c'est qu'elles apparaissent car il y a une réelle volonté de poser un droit de propriété sur les données personnelle. Toutes ces réflexions de divers auteurs montrent que c'est une idée qui peu à peu s'impose comme la solution idéale aux yeux de nombreux auteurs et praticiens du droit. Peu importe par quel bien on impose un droit de propriété sur les données, que ce soit pas le biais du droit d'auteur, des droits voisins ou bien du droit de propriété classique, l'important est de prendre conscience que cette assimilation est importante. A l'heure actuelle, il semble que l'instauration d'un droit de propriété classique au sens de l'article 544 du code civil semble le plus adapté aux données personnelles. Pour les auteurs, instaurer un droit de propriété sur les données permettrait de mettre fin à l'exploitation abusive qui est faite des données du fait de leur qualification de chose sans maître. En effet, les entreprises et autres plateformes profitent de cet état des données personnelles pour les exploiter de façon abusive. Il est vrai qu'établir un droit de propriété en faveur des personnes concernées leur redonnerait le contrôle et la maîtrise et serait un bon moyen de réguler ce secteur[127].

Pour certains, l'instauration d'un droit de propriété sur les données doit s'accompagner de la relocalisation des serveurs contenant les données puisque la plupart sont situés hors de l'Europe. Il est

[126] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *op. cit.*, p. 63.
[127] MOREL (L.), *op. cit.*

vrai que les données, comme nous l'avons déjà précisé, est le pétrole du XXIème siècle. Or, les données des européens ne devraient pas être traitées hors de l'Europe d'une part parce que cela représente une protection moins efficace pour les européens et d'autre part parce que l'Europe devrait garder cette valeur ajoutée et créer elle même des emplois sur ce domaine plutôt que d'envoyer dans d'autres pays ces données. En effet, en les envoyant dans d'autres pays ce sont ces derniers qui profitent des avantages procurés par le traitement des données. L'Europe devrait elle-même retirer les fruits de la collecte légale des données[128].

Ce qui est certains, c'est qu'un bon nombre de décisions ont implicitement reconnu l'existence du droit à l'oubli et ce même avant la consécration de ce droit dans l'arrêt Google Spain de la CJUE. De plus, d'autres arrêts continuent de reconnaitre ce droit de manière fréquente et ainsi de favoriser le droit des personnes sur leur données au détriment des moteurs de recherche. En 2010, le juge français a imposé à Google la suppression de liens qui renvoyait vers des vidéos pornographiques mettant en scène la plaignante. Ces liens étaient obtenus suite à une recherche effectuée grâce au nom de la plaignante. Le juge a précisé que le moteur de recherche devait prévoir la possibilité de mettre en place un moyen de désindexer les pages lorsque la personne concernée le demandait[129]. Dans une autre affaire similaire de 2012, le juge avait demandé à Google de supprimer des résultats de la liste de recherche à partir du moment où la requête était effectuée grâce au nom patronymique de la requérante[130]. Ce ne sont que des exemples parmi tant d'autres.

On peut voir dans ces nombreux arrêts qui sont rendus que la jurisprudence donne une certaine importance à ce droit à l'oubli et l'applique de manière fréquente. Toutes ces affaires laissent penser que l'instauration d'un droit de propriété serait possible puisque qu'elles confèrent un réel droit d'abusus sur les données personnelles. On peut penser que de telles jurisprudences finiront peut être un jour par servir de fondement pour la reconnaissance d'un droit de propriété sur les données. Pour le moment, nous n'avons pas de consécration législative. Celle-ci pourrait venir avec la proposition de règlement européen qui entend réaliser une réelle disposition législative sur le droit à l'oubli. C'est peut être cette disposition qui un jour servira de fondement à la reconnaissance réelle d'un droit de propriété sur les données. Il semble possible voire probable qu'un jour cette consécration ait réellement lieu en droit positif. Bien que comme nous venons de le voir l'instauration d'un droit

[128] BARROUX (D.), « Gilles Babinet et Pierre Belanger : la régulation des données, défi majeur du XXIème siècle », http://www.lesechos.fr, 12 février 2014.
[129] BENSOUSSAN (A.), « Le droit à l'oubli, un droit de l'homme numérique », blog.lefigaro.fr, 21 juillet 2014.
[130] CASANOVA (A.), *op. cit.*, p. 91.

de propriété sur les données pourrait avoir des avantages, certains auteurs ou hommes politiques y sont aujourd'hui encore retissant.

Certains sont farouchement opposés à l'application d'un droit de propriété sur les données personnelles et peuvent justifier leur position. Cependant, on aura l'occasion de constater que l'idée de l'instauration d'un droit de propriété s'est déjà posée pour d'autres droits de la personnalité et qu'elle a naturellement été elle aussi accompagnée de nombreuses craintes.

B) L'évolution des droits de la personnalité vers le droit de propriété

Bien que l'idée d'instaurer un droit de propriété sur les données personnelles soit de plus en plus ancrée dans les esprits, un certains nombre de personnes s'y opposent farouchement en argumentant que cette instauration ne serait pas bénéfique pour la protection des données à caractère personnel et serait même néfaste pour celle-ci.

Le problème essentiel de l'instauration d'un droit de propriété sur les données personnelles est que lorsque l'on acquiert la propriété, cela s'accompagne de la possibilité d'effectuer un transfert de propriété. C'est au moment de ce transfert que des problèmes se poseraient en matière de données personnelles.

Tout d'abord, en ce qui concerne l'usus, le droit de jouir du bien, en cas de transfert de propriété, celui-ci serait cédé à la personne qui viendrait acquérir la propriété. Cela signifie qu'une personne pourrait en lieu et place de la personne concernée utiliser ses données personnelles à sa guise. Il y aurait une possibilité d'utiliser les données d'autrui en toute liberté une fois la propriété cédée. Cela semble difficilement imaginable étant donné qu'a ce moment-là il serait possible d'usurper l'identité d'autrui, cela pourrait même devenir légal[131]. En terme de risque au niveau de la sécurité et au niveau judiciaire c'est inimaginable. De plus, il serait possible en utilisant les données d'autrui de les discréditer et ainsi de créer une réputation numérique à une personne qui serait fausse et qui risquerait de porter atteinte à son honneur. En effet, il deviendrait aisé d'utiliser les données d'une personne, de se faire passer pour elle aux yeux des tiers et d'avoir un comportement qui créerait une mauvaise réputation à la personne à laquelle appartiennent les données.

Ensuite, concernant le fructus, en cas de transfert de propriété cela serait un tiers qui retirerait les bénéfices du fait de l'exploitation des données personnelles de la personne concernée. C'est l'aspect qui pose le moins de problème puisque c'est déjà un cas de figure que l'on connait avec les GAFA qui sont rentables grâce à l'exploitation de nos données personnelles. Ce qui apparait simplement gènant c'est que cela ne sera pas la personne concernée, c'est à dire la personne qui crée les données du fait de sa personne qui bénéficiera de l'exploitation de ses propres données mais une personne extérieure, une entreprise ou un moteur de recherche. Or, c'est ce qui dérange le plus souvent les internautes, avoir conscience que les données permettent à certains de gagner beaucoup d'argent

[131] MATTATIA (F.), « Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I), *op. cit.*, p. 61.

sans que les principaux intéressés, ceux qui permettent l'existence d'un tel commerce, ne participent aux gains de ce qu'ils créent. C'est tout de même à relativiser car dans le cadre de l'instauration d'un droit de propriété, les entreprises paieraient les internautes pour pouvoir exploiter leur données. De plus, déjà à l'heure actuelle, la contrepartie de l'exploitation des données des internautes est le fait de pouvoir utiliser gratuitement une multitude de services.

Le droit d'abusus est certainement le point qui pose le plus de problème. L'abusus comprend notamment le droit de détruire le bien. Lorsque la propriété va être transférée, ce droit de destruction de nos données sera aussi transféré. Or, il semble difficile de transférer à autrui le droit de détruire les données personnelles de quelqu'un d'autre. Ainsi, un tiers qui acquerrait la propriété sur nos données aurait la possibilité par exemple de supprimer l'identité de la personne concernée. La solution serait alors de classer les données en deux catégories: d'un côté les plus sensibles qui ne pourraient pas être cédées et d'un autre côté les données beaucoup moins sensibles dont la propriété pourrait être cédée sans risque de causer les problèmes précités[132]. Le problème est que cela enlèverait un peu de l'intérêt recherché en instaurant un droit de propriété qui est celui de simplifier les choses. Cela reviendrait à réfléchir à la question de savoir quelle donnée dépend de quelle catégorie et cela serait compliqué à lire. De plus, lorsque la propriété aura été transférée vers qui la personne concernée devra se tourner si elle souhaite voir ces données disparaitre au titre du droit à l'oubli? Pourrait-elle même invoquer ce droit ou en aura-t-elle été dépossédée au moment du transfert de propriété?

Il ne faut pas non plus oublier que la propriété classique entraine lors du décès tout un tas d'actes juridiques. Cela signifierait qu'au moment du décès de la personne les descendants auraient un droit de succession sur les données personnelles notamment. De plus, les données personnelles entreraient dans le patrimoine: elles seraient donc saisissables. On peut alors se demander si tous ces effets de l'application de la propriété aux données personnelles ne paralyseraient pas le système en alourdissant les formalités lors des échanges de données[133].
Un argument est fréquemment avancé: celui de la crainte de l'aliénation des données. En effet, beaucoup sont gênés par le fait que du moment où il y a transfert de données, il y a aliénation de celles-ci. Or, cet argument peut être réfuté car les données sont reproductibles à l'infini. Par conséquent, l'aliénation n'aura qu'une dimension limitée puisqu'il sera toujours possible pour la per-

[132] MATTATIA (F.), « Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I), *ibid.*
[133] MATTATIA (F.), « Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I), *ibid.*

sonne qui vend ses données d'en garder un exemplaire. Alors il est évident que l'aliénation existe mais sa portée est moins limitée. Du fait qu'elles sont reproductibles même lorsqu'on vend ses données on les conserve[134]. La possibilité de copie des données permet en quelque sorte au propriétaire initial des données d'en conserver un exemplaire.

De plus, certains disent même que la protection des personnes concernées ne serait pas meilleure. En effet, en 2014 le Conseil national du numérique a publié un rapport sur la neutralité des plates-formes dans lequel il évoque la nature des données personnelles et en profite pour se prononcer contre la mise en place d'un droit de propriété sur les données personnelles car pour lui, un tel régime ne serait pas protecteur des personnes concernées. Le premier problème lié à la propriété des données pointé par le Conseil est le fait qu'il incombera aux individus de gérer leur données seuls. Le problème n'étant pas qu'ils les gèrent seuls mais que cela risque de créer un clivage entre les individus. D'un côté, ceux qui auront le temps et qui auront acquis les connaissances nécessaires pour pouvoir gérer leur données de façon optimale, à savoir réussir à en tirer profit et à la fois réussir à les protéger correctement. D'un autre côté, ceux qui n'auront pas le temps et/ou les connaissances nécessaires pour s'occuper correctement de leurs données. Les données de ces derniers risquent ainsi d'être exploitées à leur insu et de façon abusive. Par conséquent il n'y aurait plus aucune protection pour cette catégorie de personnes. Bien évidemment, ils pourraient faire appel à des intermédiaires qui se chargeraient de commercialiser et gérer les données des individus mais là encore, cela n'augure rien de bon. En effet, ce seront certainement ces intermédiaires qui gagneront beaucoup d'argent grâce aux données personnelles qui leurs seront confiées mais le risque est que les personnes concernées ne reçoivent qu'une part minime de rémunération. De plus, ces intermédiaires remplaceraient certainement les entreprises actuelles et les personnes concernées se retrouveraient sous la coupe de ces nouveaux intermédiaires, ce qui pour le particulier ne changerait pas grand chose. En revanche, cela risquerait d'augmenter le phénomène de commercialisation des données puisqu'en créant un droit de propriété, la commercialisation des données personnelles serait carrément autorisée et en plus facilitée par l'existence de sortes de courtiers[135]. L'avantage, en gardant le statut de droit de la personnalité, est que les données personnelles conservent une protection légale identique pour tous tandis qu'avec la propriété des données la protection dépendrait du degré de connaissance de chaque personne et créerait des disparités entre les individus en instaurant différents niveau de protection. Vu la complexité du sujet, il est prévisible que bon nombre

[134] TEXIER (B.), « Alain Bensoussan : je crois à l'émergence d'un marché des données personnelles », *Archimag*, n° 279, novembre 2014, p. 44.
[135] MOREL (L.), *op. cit.*

d'individus se retrouvent submergés par la difficulté et laissent leurs données aux mains d'entreprise qui en profiteraient de manière abusive.

Le Conseil national du numérique craint ainsi une hausse de l'individualisme, un renforcement des inégalités et une baisse de la protection alors que le revenu perçu par chaque personne concernée serait minime. Enfin, certains craignent l'apparitionn d'un « troisième mouvement d'enclosure » faisant suite aux deux premiers, à savoir la naissance du droit de propriété sur les terres au 12ème siècle qui a conduit à la création d'une nouvelle classe de riches propriétaires au détriment des premiers occupants ainsi que l'instauration du droit d'auteur ayant abouti à l'émergence d'intermédiaires puissants au détriment des droits du public sur les connaissances. L'instauration d'un droit de propriété sur les données personnelles aurait pour conséquence selon certaines personnes réellement opposées à la propriété des données de précipiter un troisième mouvement d'enclosure qui entrainerait l'émergence d'intermédiaires puissants (les courtiers en données ou les entreprises dont le modèle économique est basé sur la commercialisation des données) au détriment de la protection des données personnelles et des personnes concernées. Selon les non partisans de la propriété des données, ce mouvement serait pire que les autres car il touche à l'essence même de l'être humain[136].

Si cette dernière vision des choses semble un peu radicale, d'autres auteurs pointent des risques et des problèmes plus réalistes issus de la propriété des données. La principale difficulté que l'appât d'un gain éventuel issu de l'exploitation de nos données peut faire oublier est celle du décalage d'information qu'il peut y avoir entre le vendeur et l'acheteur et la difficulté d'évaluer la valeur des données personnelles.

L'évaluation de la valeur des données personnelles se révèle être plutôt complexe. Tout d'abord, il n'existe pas encore vraiment de méthode d'évaluation de la valeur des données et le peu qui existe reste flou. L'idéal serait d'avoir des techniques d'évaluation nationales ou au moins un guide afin d'être certains que la méthode soit fiable et respectueuse du vendeur. C'est d'autant plus un problème que les intérêts des vendeurs et des acheteurs sont antagonistes. Les personnes concernées qui seront les vendeurs de données personnelles seraient intéressées par des avantages en nature tandis que les acheteurs, à savoir les entreprises, recherchent une valeur en argent[137]. Le risque est

[136] MOREL (L.), *op. cit*.
[137] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », *RLDI*, mai 2015, n°115, p. 64.

que les vendeurs cèdent trop facilement leur données aux acheteurs qui en retireraient un bénéfice énorme. Le risque est celui de la vente pour un prix dérisoire.

Cela nous amène faec à un autre problème: bien souvent, l'acheteur connait le revenu qu'il obtiendra grâce à l'obtention d'une donnée tandis que le vendeur n'en a aucune idée ce qui fait qu'il n'a aucune idée du prix qu'il doit fixer pour la vente. Cette difficulté est accentuée par le fait que la valeur des données va dépendre de nombreux facteurs et va différer en fonction de l'entreprise qui l'achète, de l'usage qu'elle en fait ou encore de l'association qui en sera faite avec d'autres données. Le risque est que l'acheteur soit systématiquement défavorisé par rapport au vendeur. Cela peut avoir des conséquences graves dans la mesure où la cession peut être définitive et entrainera la perte de la maîtrise sur ses données pour la personne concernée. Cela signifie que le vendeur cèderait ses données personnelles de manière définitive en prenant le risque que la rémunération qui lui aura été offerte ne corresponde pas réellement à la valeur des données cédées. Par la suite, le vendeur n'aurait aucun moyen de récupérer ses données, n'aurait pas obtenu une rémunération suffisante et n'aurait plus aucun moyen de les récupérer[138].

De plus, au niveau juridique, cela risquerait d'imposer la mise en place d'un formalise très lourd pour organiser la cession des données personnelles. En effet, lorsque l'on vend quelque chose il y a nécessairement un contrat dans lequel le consentement est manifesté. C'est essentiel. Bien évidemment pour la plupart des choses que les individus achètent il n'est pas nécessaire de conclure un contrat écrit comme par exemple lorsqu'il s'agit d'acheter des fruits chez le primeur. Dans cet exemple, le consentement est tacite. Si on voulait réellement faciliter les transactions, il ne faudrait pas imposer la conclusion d'un contrat écrit, ce qui est parfaitement autorisé. Cependant, cela serait peu protecteur du vendeur. Les données personnelles touchent quand même à l'essence de la personne et pour obtenir une protection efficace de la personne concernée, il faudrait exiger un consentement exprès de celle-ci à chaque transaction. Dans ce cas, cela deviendrait très lourd voire trop lourd au niveau administratif. Il faudrait à chaque transaction vérifier l'identité du vendeur, sa capacité et trouver une solution pour avoir une signature représentant le consentement non équivoque du vendeur[139]. Cela semble peu adapté à la fluidité existant sur internet et contraire à l'objectif européen de faciliter la circulation des données tout en protégeant les personnes concernées. De plus, il faudra mettre en place des mécanismes de sanction ou de dédommagement en cas de dol ou d'escroquerie. Il faudra décider de la possibilité ou non de sanctionner les personnes vendant de

[138] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », *op. cit.*, p. 65.

[139] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », *RLDI*, mai 2015, n°115, p. 64.

fausses données. Ce sont des cas à prévoir. Il faudra aussi décider du sort à réserver aux données sensibles. Seront-elles vendues comme les autres, bénéficieront-elles d'un régime adapté ? Ce sont à toutes ces questions qu'il faudra répondre[140].

Evidemment, il faudrait aménager ce régime de propriété, ce qui d'ailleurs a déjà été fait pour des domaines particuliers mais cela ne semble pas infaisable. On pourrait d'ailleurs demander à tous les détracteurs s'il n'est pas naturel que toute évolution s'accompagne de craintes, d'appréhensions et d'une nécessité de réfléchir aux adaptations qu'il faudrait apporter au régime. Ce sont d'ailleurs des craintes similaires qui ont été avancées lorsque l'idée de la mise en place d'un droit de propriété a été avancée pour d'autres droits de la personnalité, ce qui n'a pas empêché qu'aujourd'hui pour certains d'entre eux un tel droit est quasiment présent.

Cette question de la patrimonialisation des droits extrapatrimoniaux n'est pas nouvelle et derrière elle se cache l'idée de la possible existence d'un droit de propriété sur ces droits. On parle même parfois de crise d'identité des droits de la personnalité[141]. Traditionnellement, le droit à l'image ou encore le droit à la voix sont considérés comme des droits de la personnalité et donc comme appartenant à la famille des droits extrapatrimoniaux. Pourtant en pratique, au fil des années, n'a cessé de se développer des contrats par lesquels une personne autorise l'exploitation commerciale de son image ou de sa voix. Le droit à l'image est le plus caractéristique de ce phénomène de patrimonialisation[142]. En effet, il est fréquent qu'une personne célèbre monnaye son image ou sa voix. Cela arrive très fréquemment avec la presse notamment. Les célébrités peuvent par exemple donner l'exclusivité des photographies de leur enfant venant de naitre. Ces photos seront vendues à prix d'or. Les célébrités font vraiment une exploitation commerciale de leur image et cela n'est pas interdit. On trouve des exemples dans la vie de tous les jours, les sportifs vendent leurs images, mais il y aussi des personnes qui ne sont pas connues qui exploitent leur image. C'est le cas par exemple des personnes posant pour les cartes postales ou jouant dans des publicités[143]. Certains auteurs prônent même la reconnaissance d'une catégorie qui se nommerait les droits patrimoniaux de la personnalité. Cela consisterait à séparer en deux les droits de la personnalité, avec d'un côté les droits classiques de la personnalité par le biais desquels les individus peuvent protéger leurs droits moraux, et d'un autre côté les droits de la personnalité qui ont dérivé et dont l'exploitation commer-

[140] MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », *op.cit.*, p.63.
[141] HASSLER (T.), « La patrimonialisation des droits extrapatrimoniaux », *Petites affiches*, décembre 2004, n°244, p.3.
[142] LEPAGE (A.), « Débat relatif au droit patrimonial à l'image », *Répertoire de droit civil*, 2009, paragraphe n°141
[143] HASSLER (T.), « Contribution à la nature juridique du droit « patrimonial » à l'image », *RLDI*, 2010, n° 59, p. 70.

ciale est possible, qui permettraient aux individus de protéger leur intérêts patrimoniaux. En regardant la jurisprudence, on s'aperçoit que cette double conception existe déjà. En effet, lorsqu'une personne demande réparation devant les tribunaux d'une atteinte au droit à son image, les dommages et intérêts obtenus en cas de succès serviront à réparer deux atteintes en réalité. Dans un premier temps les dommages et intérêts alloués au plaignant serviront à réparer le fait que toute personne a droit à ce que ne soit pas publiée ni réalisée une image de sa personne dans sa vie privée sans son autorisation. Les dommages et intérêts vont donc servir à réparer le préjudice moral issu de la diffusion d'une image de la personne la représentant dans sa vie privée sans son autorisation. Mais dans un second temps l'action en justice va permettre de protéger un intérêt plus matériel. L'allocation de dommages et intérêts va permettre au plaignant de recevoir une réparation du préjudice subi qui correspondra au dédommagement du manque à gagner provenant de la diffusion de son image sans que celle-ci ait donné lieu à rémunération du plaignant. Cela confère un vrai monopole d'exploitation en faveur de la personne sur son image[144].

Dans une affaire en 2002 devant la Cour d'appel de Versailles, la demanderesse était actrice et mannequin et demandait la réparation de son préjudice commercial du fait de la diffusion de photos de sa personne sans son autorisation. La Cour a accueilli cette demande en précisant que la société qui avait exploité l'image de la demanderesse sans son autorisation avait ainsi bénéficié de retombées économiques importantes au détriment des droits patrimoniaux de la demanderesse[145].

On voit à travers cet arrêt que la jurisprudence reconnait clairement la dimension patrimoniale du droit à l'image. Il faut tout de même préciser que la Cour de Cassation est frileuse vis à vis d'une telle reconnaissance mais elle accepte très bien les cessions d'images à titre onéreux. Bien entendu on ne peut pas faire n'importe quoi avec les images, cela reste un domaine bien protégé puisqu'il l'est par le biais du droit de à la vie privée. En revanche pour ce qui est de l'image on y ajoute la dimension commerciale, on prend en compte le côté patrimonial. En réalité en ce qui concerne le droit à l'image on a trouvé une sorte de compromis entre protection efficace et possibilité pour l'intéressé de tirer profit de son image. En y regardant bien, cela serait peut être une solution pour les données personnelles. Créer un régime hybride permettant d'un côté de conserver une protection équivalente à la protection actuelle et d'un autre côté permettre aux individus de tirer profit des données qu'ils produisent ou du moins que leur exploitation leur profite directement. Cela passerait alors peut être par la reconnaissance d'un catégorie de droits hybrides que l'on qualifierait effecti-

[144] LEPAGE (A.), « Débat relatif au droit patrimonial à l'image », *Répertoire de droit civil*, 2009, paragraphe n°143
[145] LEPAGE (A.), « Débat relatif au droit patrimonial à l'image », *Répertoire de droit civil*, 2009, paragraphe n°146

vement de droits patrimoniaux de la personnalité. Cela permettrait de garder le côté droits personnels avec une protection élevée et d'ajouter la dimension commerciale.

L'instauration d'un droit de propriété sur l'image n'existe pas encore, mais tout comme pour les données personnelles c'est un débat qui existe aujourd'hui. En effet certains auteurs et praticiens sont partisans d'une telle instauration. Il est vrai que lorsqu'on regarde la façon dont fonctionne le droit à l'image on comprend que certains pensent à changer de régime. C'est comme pour les données personnelles, on sait qu'il faut agir au niveau juridique pour coller à une réalité qui s'installe : la commercialisation de certains droits de la personnalité. Celle-ci est inévitable à l'heure actuelle. Notre société à trop évolué et interdire un tel commerce serait source de régression. On imagine mal une société ou de nombreux services que l'on utilisait gratuitement deviennent payant du fait de l'interdiction de la commercialisation ou utilisation des données personnelles, de la même manière qu'il paraitrait inconcevable d'exploiter l'image de la vie privée des célébrités sans que celles-ci reçoivent de contrepartie.

Les questions qui se posent en matière de droit à l'image sont similaires à celles qui se posent en matière de données à caractère personnel. En effet, des auteurs avancent que l'instauration d'un droit de propriété pourrait être bénéfique.

Ainsi les arguments pour l'instauration d'un droit de propriété sur l'image seraient les suivants. L'instauration d'un tel droit permettrait à l'intéressé de défendre plus facilement ses droits. De plus, cela rapprocherait ce droit du droit américain ce qui permettrait une certaine harmonisation. Enfin, comme pour la propriété des données personnelles l'argument principal serait l'application d'un régime juridique que l'on connait bien dans les moindres détails. Cela serait l'application d'un droit prévisible en quelque sorte. On connait bien le droit de propriété on sait l'appliquer, certains pensent que l'application d'un tel droit à l'image ou aux données personnelles rendait les choses moins complexes et par conséquent offrirait une certaine sécurité juridique. Il est également intéressant de voir que comme pour l'idée d'une propriété des données on pense à une application du droit d'auteur pour le droit à limage. En effet, certains auteurs pensent qu'il serait possible d'adapter le droit d'auteur classique pour venir l'appliquer au droit à l'image[146].

Certes ces visions semblent aujourd'hui curieuses ou extrapolées cependant elles naissent pour de plus en plus de droits de la personnalité et les données personnelles ne font pas exception. Avec tout

[146] HASSLER (T.), « Contribution à la nature juridique du droit « patrimonial » à l'image », *op.cit.*, p. 73.

ce que l'on vient de voir on constate que des réticences existent en ce qui concerne l'instauration d'un droit de propriété sur les données personnelles. Cependant, ce n'est pas le seul droit où cette question de la propriété est soulevée et dans les autres domaines où la question se pose on se rend compte qu'il y a aussi des craintes. C'est une réaction normale face à tout phénomène de changement. La question de la propriété des données s'inscrit dans un mouvement général de crise des droits de la personnalité. La société a évolué de telle manière à ce que certains droits de la personnalités ont toujours besoin d'être protégés mais ont aussi besoin de bénéficier de plus de liberté. D'autant plus qu'en analysant la pratique on réalise qu'il existe une patrimonialisation. De cette patrimonialisation certains espèrent instaurer un droit de propriété sur les données personnelles, cela ne se fera peut être jamais mais l'idée comme nous l'avons vu n'est pas totalement mauvaise. A l'heure actuelle on peut dire que si la propriété sur les droits de la personnalité et a fortiori sur les données personnelles n'est pas d'actualité, il faudrait nécessairement arriver au moins à reconnaitre un vrai droit patrimonial sur les données.

Conclusion

Ainsi, nous retiendrons que le droit des données à caractère personnel est complexe et en évolution. Nous nous trouvons à une période cruciale pour l'avenir de nos données personnelle. La complexité étant qu'il faut arriver à faire évoluer le droit en maintenant un niveau de protection élevé tout en prenant en compte l'utilisation réelle des données.

Le projet de règlement européen nous donne tout de même bon espoir quant à la future régulation de nos données. Un des points forts de ce projet étant, comme nous l'avons vu, qu'il met tout en oeuvre pour maintenir une protection élevée pour les personnes concernées, notamment en reconnaissant le droit à l'oubli numérique tout en prenant en compte la dimension patrimoniale des données.

Aujourd'hui on ne peut en effet plus considérer les données personnelles comme faisant partie des droits de la personnalité. Du moins pas dans leur définition classique. Il est clair qu'à l'heure actuelle, des entreprises de renommée mondiale ont fondé leur économie sur l'utilisation ou la commercialisation des données personnelles. Il semble donc primordial de prendre en compte la dimension patrimoniale des données personnelles.

Nous pouvons nous féliciter que l'Europe semble vouloir prendre en compte cette dimension patrimoniale. En revanche, il faut espérer que l'on réussisse à trouver un accord sur le texte définitif qui fait encore débat à l'heure actuelle au sein de l'Union européenne. Il existe un fort lobbying sur ce

texte depuis le début des réflexions qui ont conduit au projet. Les données personnelles sont en effet un sujet d'actualité brulant ces dernières années du fait que l'on peut les considérer comme le nouveau pétrole du 21ème siècle et que les personnes concernées se préoccupent de plus en plus du sort de ces données.

Nous avons beaucoup à attendre de ce texte qui pour le moment éprouve des difficultés concernant la définition des données personnelles. Selon les catégories de données qu'elle fera rentrer dans cette définition on s'orientera vers une dimension plus ou moins patrimoniale. Il ne reste plus qu'à espérer que l'Union européenne penche pour la dimension patrimoniale afin de ne pas risquer que le droit ait un temps de retard par rapport à la réalité.

Si jamais cette option n'était pas satisfaisante, il reste toujours l'idée de l'instauration d'un droit de propriété sur les données personnelles qui résoudrait certains problèmes rencontrés par les rédacteurs du projet de règlement mais qui s'accompagnerait de certains inconvénients. Pour le moment il ne s'agit que d'une possibilité mais il semblerait que les mentalités ne soient pas encore prêtes à accepter une telle solution.

Mais qui sait peut-être que dans quelques années nos enfants trouverons naturel d'avoir un droit de propriété sur leurs données et que notre système actuel leur semblera archaïque. Ce qui est certain c'est que c'est un domaine qui n'a pas terminé son évolution et qui est pas prêt de la finir.

Bibliographie

I - OUVRAGES GENERAUX ET SPECIALISES

- ANONYME, *Informatique et liberté mode d'emploi*, Groupe Revue Fiduciaire, Paris, 2007, 233 p.

- CORNU (G.), *Vocabulaire juridique*, Puf, 8e éd., Paris, 2009, 986 p.

- Code civil.

- DESGENS-PASANAU (G.), *La protection des données à caractère personnel - La loi « informatique et libertés »*, LexisNexis, Paris, 2012, 281 p.

- EYNARD (J.), *Les données personnelles : quelle définition pour un régime de protection efficace ?*, Michalon, Paris, 2013, 435 p.

- HAAS (G.) et COHEN-HADRIA (Y.), *Guide juridique informatique et libertés : collecte, traitement et sécurité des données dans l'univers numérique : ce que vous devez savoir*, ENI, St Herblain, 2012, 183 p.

- *Manuel de droit européen en matière de protection des données*, office des publications de l'Union européenne, Luxembourg, 2014, 215 p.

- MATTATIA (F.), *Traitement des données personnelles : le guide juridique : la loi informatique et liberté et la CNIL, jurisprudence*, Eyrolles, Paris, 2013, 187 p.

II - ARTICLES, CONTRIBUTIONS, INTERVENTIONS

- ANONYME, « 1977 - 1978 : le Sénat invente les autorités administratives indépendantes », http://www.senat.fr, 20 juin 2008.

- ANONYME, « La protection des données personnelles », http://www.senat.fr, 12 février 2014.

- ANONYME, « 90% des citoyens espionnés par la NSA sont des « gens ordinaires » », lexpress.fr, 07 juillet 2014.

- ANONYME, « Bilan 2014 : les données personnelles au coeur du débat public et des préoccupations des français », http://www.cnil.fr, 16 avril 2015.

- ANONYME, « Enjeux 2015 (3) : quels nouveaux droits pour mieux maîtriser ses données ? », http://www.cnil.fr, 15 avril 2015.

- ANONYME, « Enjeux 2015 (2) : la protection des données, clé de voûte de l'innovation », http://www.cnil.fr, 16 avril 2015.

- ANONYME, « la nécessité d'une refonte en profondeur », *Lamy droit des médias et de la communication*, tome 1, Lamy, étude 479-30, mai 2015.

- ANONYME, « Les chiffres du vol des données en 2014, cil.cnrs.fr, 20 février 2015.

- ANONYME, « Origine de la loi Informatique et Liberté », cil.cnrs.fr, 15 novembre 2012.

- ANONYME, « Quand « Big Data » menace de devenir « Big Brother » », laquadrature.net, 06 janvier 2014.

- RONFAUT (L.), « Qu'est-ce que la loi renseignement ?, lefigaro.fr, 25 juin 2015

- AUFFRAY (C.), « Données personnelles : nous aurons le règlement européen en 2015 », http://www.zdnet.fr, 28 janvier 2015.

- BARROUX (D.), « Gilles Babinet et Pierre Belanger : la régulation des données, défi majeur du XXIème siècle », http://www.lesechos.fr, 12 février 2014.

- BENSOUSSAN (A.), « Faut-il réguler la marchandisation des données personnelles sur internet ? », blog.lefigaro.fr, 30 janvier 2013.

- BENSOUSSAN (A.), « Le droit à l'oubli numérique : un droit naturel », www.alain-bensoussan.com, 6 février 2014.

- BENSOUSSAN (A.), « Le droit à l'oubli, un droit de l'homme numérique », blog.lefigaro.fr, 21 juillet 2014.

- BERREBI (C.), COHEN-HARDI (Y.), « protection des données personnelles et avocats CIL », *Gazette du Palais*, 22 novembre 2014, n°326, pp. 9-12.

- BONNET (F.), « La CNIL crée un label sur la gouvernance des données personnelles », http://www.journaldunet.com, 19 janvier 2015.

- BOUCHER (P.), « A l'origine de la CNIL : « Safari » ou la chasse aux Français », http://ldh-toulon.net, 1er octobre 2008.

- CASANOVA (A.) et VERET (D.), « La consécration d'un droit à l'oubli … principalement pour les anonymes », *Lamy Droit de l'Immatériel*, 2014, n°106, pp. 87-92.

- CASTEX (F.), « Mes données personnelles ne sont pas à vendre ! », liberation.fr, le 18 mars 2013.

- CHEMINAT (J.), « Un pas de plus vers le règlement européen sur la protection des données privées », http://www.lemondeinformatique.fr, 12 mars 2014.

- CHEMLA (L.), « Nous sommes tous des ayants droits », http://blogs.mediapart.fr, 23 octobre 2013.

- DROSS (W.), « Une approche structurale de la propriété », *RTD civ.*, octobre 2012, n°3, pp. 419-439.

- FERRAN (B.), « Les Français prêts à monnayer leurs données personnelles », lefigaro.fr, 26 octobre 2014.

- HASSLER (T.), « La patrimonialisation des droits extrapatrimoniaux », *Petites affiches*, décembre 2004, n°244, p.3.

- HASSLER (T.), « Contriburion à la nature juridique du droit « patrimonial » à l'image », *RLDI*, 2010, n° 59, pp. 70-75.

- HOTTOT (K.), « Facebook en 2014 : 1,39 milliard d'utilisateurs et 2,93 milliards de bénéfices », nextinpact.com, 29 janvier 2015.

- LEPAGE (A.), « Débat relatif au droit patrimonial à l'image », *Répertoire de droit civil*, 2009, paragraphe n°141 à 147.

- MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I) », *RLDI*, avril 2015, n°114, pp. 60-63.

- MATTATIA (F.), « Être propriétaire de ses données personnelles : peut-on envisager un régime spécifique ? (partie II) », *RLDI*, mai 2015, n°115, pp. 63-65.

- MARTIAL-BRAZ (N.), ROCHFELD (J.) et GATTONE (E.), « Quel avenir pour la protection des données à caractère personnel en Europe ? » , *Recueil Dalloz*, 2013, p. 2788-2795.

- MEHN (A.), « Peut-on vraiment contrôler ses données personnelles ? », france5.fr, 15 janvier 2015.

- MOHAMED (R.), « Données personnelles : les impacts du futur règlement européen : une conférence au sommet pour l'AFDIT », http://www.linkipit.com, 16 avril 2014.

- MOREL (L.), « Le CNNum s'est prononcé contre l'instauration d'un droit de propriété privée sur les données personnelles », http://scinfolex.com, 19 juin 2014.

- MOURON (P.), « Perspective sur le droit à l'identité numérique », L'ordre public numérique - Libertés, propriété, identité, Presses universitaires d'Aix-Marseille, 2015, pp. 115-127.

- MOURON (P.), « Non commercialité d'un fichier de données non déclaré à la CNIL », paru dans l'ouvrage *Droit commercial - Sociétés commerciales 2014 - Un an de jurisprudence commentée*, pp. 317-319

- PERRAY (R.), « La Cour de justice, les moteurs de recherche et le droit « à l'oubli numérique » : une fausse innovation, de vraies questions », *Lamy Droit de l'immatériel*, 2014, n° 109, pp. 35-44.

- POIDEVIN (B.), « Les apports du projet de règlement européen du 25 janvier 2012 relatif aux données personnelles », http://www.village-justice.com, 1er avril 2015.

- REES (M.), « Droit à l'oubli, etc. Les eurodéputés votent le Règlement Données personnelles », http://www.nextinpact.com, 13 mars 2014.

- SERIAUX (A.), « la notion juridique de patrimoine », *RTD Civ.*, décembre 1994, n°4, pp. 801-815.

- STORRER (P.), « Pour un droit commercial des données à caractère personnel », *RTD Civ.*, juillet 2013, n°27, pp. 1844-1846.

- TEXIER (B.), « Alain Bensoussan : je crois à l'émergence d'un marché des données personnelles », *Archimag*, n° 279, novembre 2014, pp. 44-45.

- VANDYSTADZT (N.), « Les collectivités européennes opposées au renforcement de la protection des données personnelles », http://www.lagazettedescommunes.com, 18 novembre 2014.

- VINCENT (C.), « La ruée vers l'or des données personnelles », lesechos.fr, le 7 mars 2013.

III - RAPPORTS, CONFERENCES ET CONTRIBUTIONS

- « Conférence de presse 16 avril 2015, présentation du 35ème rapport d'activité 2014 », Rapport de la CNIL, 16 avril 2015, disponible sur cnil.fr, 25 p.

- GADDES (C.), « Parimonialisation des données personnelles », VIIIè conférence de l'AFAPDP à Bruxelles, le 25 juin 2015, 13 p.

- FRAYSSINET (J.), Droit des TIC approfondi, cours du Master 2 droit des médias et des télé-communications, IREDIC, 2014-2015, 16 p.

- « Neutralité des plateformes : Réunir les conditions d'un environnement numérique ouvert et soutenable », Rapport du Conseil National du numérique, mai 2014, disponible sur www.cnnumerique.fr, 117 p.

IV - TRAVAUX PARLEMENTAIRES

- « Proposition de règlement du Parlement européen et du Conseil 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 », Commission européenne, le 25 janvier 2012, disponible sur ec.europa.eu, 134 p.

V - Textes législatifs

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

VI - JURISPRUDENCE

- C. Cass., Ch. Comm., 25 juin 2013, n°12-17.037, FS-P+B+I

- CJUE, GC, Google Spain SL et Google Inc. c/ Agencia Espanola de proteccion de Datos (AEPD), 13 mai 2014, aff. C-131/12.

Table des matières