

Protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique

Auteur : Lifrange, Marie

Promoteur(s) : Thirion, Nicolas

Faculté : Faculté de Droit, de Science Politique et de Criminologie

Diplôme : Master en droit, à finalité spécialisée en mobilité interuniversitaire

Année académique : 2017-2018

URI/URL : <http://hdl.handle.net/2268.2/4888>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

Protection des données à caractère personnel : le consentement à l'épreuve de l'ère numérique

Marie LIFRANGE

Travail de fin d'études

Master en droit à finalité spécialisée en droit des affaires

Année académique 2017-2018

Recherche menée sous la direction de :

Monsieur Nicolas THIRION

Professeur ordinaire

RESUME

Ces dernières années, le respect de la vie privée s'est vu de plus en plus menacé par le développement exponentiel des nouveaux systèmes d'information et de collecte des données personnelles. L'Union européenne est alors intervenue, plus de vingt ans après sa première législation en matière de protection des données à caractère personnel, en adoptant le 27 avril 2016 un nouveau règlement. L'un des principaux changements apportés réside dans la notion de consentement, mode de légitimation du traitement des données personnelles.

La présente contribution vise à déterminer si le consentement, mécanisme juridique datant de l'antiquité, constitue toutefois un outil approprié à la protection des données personnelles face à l'environnement numérique d'aujourd'hui. Notre travail se scindera en deux grandes parties. En premier lieu, plusieurs aspects de la protection des données personnelles seront abordés : la genèse législative, les enjeux économiques et politiques, les principales définitions. Dans la seconde partie, nous présenterons les différentes modifications apportées au consentement. Nous envisagerons ensuite les critiques émises à son égard, tant empiriques que juridiques tout en relativisant celles-ci. Nous terminerons notre travail sur quelques pistes de réflexion autour du consentement.

REMERCIEMENTS

Je tiens à remercier tout d'abord le professeur Nicolas Thiron pour sa disponibilité et son attention dans la supervision et l'encadrement de ce travail. Ces remarques pertinentes et ses conseils avisés furent essentielles pour l'acheminement de ce travail.

Je remercie tout particulièrement mon père pour avoir suscité mon intérêt dans ce domaine et pour ses précieuses relectures.

Je remercie ma mère pour son soutien inconditionnel durant ces cinq années d'études.

TABLE DES MATIERES

INTRODUCTION	8
I. LA PROTECTION DES DONNÉES PERSONNELLES EN EUROPE	8
A) CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES PERSONNELLES	10
1) ORIGINE	10
2) LE CONSEIL DE L'EUROPE	10
2.1. La Convention européenne des droits de l'Homme	10
2.2. Convention n°108	11
3) L'UNION EUROPEENNE	12
3.1. Les directives relatives à la protection des données à caractère personnel	13
3.1.1. Directive 95/46/CE	13
3.1.2. Directive 2002/58/CE	13
3.2. La Charte des droits fondamentaux de l'Union européenne	14
3.3. Le nouveau règlement relatif à la protection des données à caractère personnel	15
B) DÉFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES ..	16
1) GENERALITES	16
1.1. Définition d'une donnée personnelle	16
1.2. Définition d'un traitement	17
2) ENJEUX DE LA PROTECTION DES DONNEES PERSONNELLES	17
2.1. Enjeux économiques	17
2.2. Enjeux politiques et sociétaux	18
II. LE CONSENTEMENT COMME OUTIL DE PROTECTION DES DONNÉES PERSONNELLES ?	19
A) LA NOTION DE CONSENTEMENT DANS LA PROTECTION DES DONNÉES PERSONNELLES	19
1) GENERALITES	19
2) ANCIEN REGIME DE LA DIRECTIVE 95/46/CE	20
2.1. Définition et caractéristiques du consentement	20
2.2. Particularité des données sensibles	20
2.3. Faiblesse de la notion de consentement	21
3) INTERVENTION DU GROUPE DE TRAVAIL 29	21
3.1. Modalités du consentement	22
3.1.1. Utilisation adéquate du consentement	22
3.1.2. Moment où le consentement est donné	22
3.1.3. Forme du consentement	22
3.1.4. Le consentement dans la directive 2002/58/CE	23
3.2. Caractéristiques du consentement	23
3.2.1. Un consentement libre	23
3.2.2. Un consentement spécifique	24
3.2.3. Un consentement informé	24
3.2.4. Un consentement indubitable	25

4) CHANGEMENTS APPORTES AU CONSENTEMENT SOUS LE NOUVEAU REGLEMENT 2016/679	26
4.1. Définition du consentement	26
4.2. Charge de la preuve	26
4.3. Déséquilibre significatif	27
4.4. Consentement informé	27
4.5. Protection renforcée des personnes vulnérables	27
4.6. Droit de retirer son consentement	28
 B) REMISE EN QUESTION DE LA NOTION DE CONSENTEMENT COMME OUTIL DE PROTECTION À L'ÉGARD DES DONNÉES PERSONNELLES	29
 1) REMISE EN CAUSE DU CONSENTEMENT	29
1.1. Les limites du consentement à l'ère numérique	29
1.1.1. Absence de maîtrise intellectuelle	29
1.1.2. Surcharge de demande et d'information	30
1.1.3. Absence de choix significatif	31
1.1.4. Privacy Paradox	32
2) RELATIVISATION DU CARACTERE ILLUSOIRE DU CONSENTEMENT	32
2.1. Obligations contraignantes à charge des acteurs du traitement	33
2.1.1. Principes de licéité, loyauté et transparence	33
2.1.2. Principe de limitation des finalités	34
2.1.3. Principe de minimisation	34
2.1.4. Principe d'exactitude	35
2.1.5. Principe de conservation	35
2.1.6. Principes d'intégrité et de confidentialité	35
2.2. Autres droits conférés aux personnes concernées	36
3) REFLEXION AUTOUR DU CONSENTEMENT	36
3.1. Innovations technologiques infinies et solutions juridiques limitées	36
3.2. L'intelligence artificielle comme complément à l'arsenal juridique ?	38
 CONCLUSION	40
BIBLIOGRAPHIE	43

INTRODUCTION

« On n'a pas tout dit du consentement quand on a dit qu'il est sympathie et sourire d'un être humain à un autre. Le sourire ne dure pas toujours et les difficultés restent au juriste »

J. Carbonnier, *Droit civil*.

Le marché européen est confronté à de nouveaux enjeux commerciaux à l'ère numérique. Le développement exponentiel des technologies de l'information et de la communication interpelle en ce qu'il permet une intrusion massive dans la vie privée des citoyens, des consommateurs. Ces innovations favorisent l'extraction de ce que l'on nomme aujourd'hui le nouvel or noir du 21^{ème} siècle : les données personnelles, nouvel eldorado des grandes entreprises. Les discussions à ce sujet ne se sont pas fait attendre, pointant dès lors la complexité sous-jacente au traitement des données. La législation européenne doit faire face à deux intérêts distincts : l'un économique et l'autre personnel. Dans cet environnement, le consentement du sujet constitue-t-il toujours un moyen approprié à la protection de ses données ?

La notion de consentement est depuis toujours une notion cruciale dans la pensée juridique occidentale. Il n'est donc pas surprenant de constater que la nouvelle législation en matière de protection des données personnelles se soit essentiellement axée sur une clarification de la portée du consentement afin de renforcer la maîtrise des citoyens sur leurs données personnelles. L'Europe adopte ainsi un modèle juridique humaniste en plaçant le sujet de droit, l'individu, au centre de sa législation¹.

Nous examinerons la problématique posée en scindant notre travail en deux parties distinctes. La première partie consiste à tracer la genèse législative de la protection des données personnelles au sein de l'Europe. Comment d'un droit à la vie privée, sommes-nous arrivés à protéger un droit à la protection des données personnelles ? Malgré une initiative entreprise au départ par le Conseil de l'Europe, la protection des données personnelles est à présent intégralement consacrée par la réglementation de l'Union européenne. Ce fut tout d'abord une directive, adoptée au début des années 1990, qui régla le sujet. Au vu des progrès technologiques et des disparités résultant du manque d'harmonisation de la directive, il a fallu entreprendre une importante réforme en la matière, qui donna lieu en 2016 à l'adoption d'un nouveau règlement. Ensuite, afin d'établir le contexte économique et politique, la première partie tente d'expliquer les principales notions et enjeux de la protection des données personnelles. Qu'est-ce qu'une donnée personnelle ? Quels sont les buts sous-jacents au traitement des données personnelles ?

¹ E. GEFFRAY, « Comment assurer l'effectivité de la protection des droits à l'ère post-Snowden ? » in A. GROSJEAN, *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 19.

Dans la seconde partie de notre contribution, nous nous consacrons exclusivement à la place du consentement dans la réglementation européenne. Nous analysons cette notion qui, au fil du temps, a fait l'objet de nombreuses clarifications et modifications importantes. Il nous faut ensuite nous pencher sur les différentes critiques émises à l'égard du consentement, spécialement soulevées par les nouveaux défis du numérique. Nous tâchons toutefois de relativiser les critiques émises à son propos par les autres principes et droits offerts par la réglementation. Pour finir, notre travail émet quelques pistes de réflexion relatives à la corrélation possible entre les solutions apportées en matière de protection des données personnelles et la logique sous-entendant le droit privé de manière générale. A l'ère numérique, la réponse aux critiques avancées ne devrait-elle pas plutôt se diriger vers l'intelligence artificielle ?

I. LA PROTECTION DES DONNÉES PERSONNELLES EN EUROPE

A) CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES PERSONNELLES

1) ORIGINE

Samuel Warren et Louis Brandeis sont considérés comme les premiers auteurs à avoir traité d'un point de vue juridique de la notion de « vie privée » dans leur célèbre article « The right to privacy »² publié en 1890³. Ils y définissent le droit à la vie privée comme le droit d'être laissé seul (« the right to be alone »)⁴. De nombreux juristes ont tenté depuis lors de définir la notion de vie privée sans qu'un réel consensus juridique ne soit toutefois admis. La difficulté de l'exercice résulte notamment du fait que le champ d'application de la vie privée tend à s'élargir constamment : la vie familiale, la santé, les opinions politiques, philosophiques, la vie sexuelle sont d'autant d'aspects repris sous sa définition⁵.

2) LE CONSEIL DE L'EUROPE

2.1. La Convention européenne des droits de l'Homme

En Europe, la consécration du droit au respect de la vie privée en tant que concept juridique intervient seulement à la suite de la Seconde Guerre mondiale et du développement conséquent des droits de l'Homme⁶. Le droit au respect de la vie privée est inscrit comme droit fondamental à l'article 8 de la Convention européenne des droits de l'Homme⁷ (ci-après, « CEDH »), qui est indéniablement inspiré de l'article 12 de la Déclaration universelle des droits de l'Homme des Nations Unies⁸ de 1948⁹.

Ce droit au respect de la vie privée comporte une double dimension : d'une part, le droit à l'intimité, c'est-à-dire le droit de ne pas laisser exposer publiquement des informations personnelles, et, d'autre part, un droit à l'autonomie personnelle selon lequel chacun peut mener sa vie comme il l'entend¹⁰. Ainsi, le droit à la protection des données à caractère

² L'article est publié en 1890 dans la Harvard Law Review. Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

³ F. RIGAUX, « La liberté de la vie privée », *R.D.I.D.C.*, 1991, Vol. 43, pp. 539.

⁴ B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, p. 27.

⁵ Y. LELEU, *Droit des personnes et des familles*, Bruxelles, Larcier, 2016, p. 188.

⁶ R. ERGEC, *Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2014, p. 26.

⁷ Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH) signée le 4 novembre 1950 à Rome par les Etats membres du Conseil de l'Europe et entrée en vigueur le 3 septembre 1953.

⁸ Déclaration universelle des droits de l'homme adoptée le 10 décembre 1948 à Paris par l'Assemblée générale des Nations Unies. Cette déclaration n'a pas de portée juridique en tant que telle, elle n'a qu'une valeur de proclamation de droit.

⁹ R. ERGEC, *op.cit.*, p. 682.

¹⁰ L. BURGORGUE-LARSEN, *La Convention européenne des droits de l'homme*, Paris, Lextenso Éditions, 2012, p. 97.

personnel est recouvert par l'article 8 de la CEDH. Notons par ailleurs que le droit au respect de la vie privée n'est pas un droit absolu. L'article 8, paragraphe 2 de la CEDH admet des ingérences lorsqu'elles sont nécessaires à la sécurité nationale ou à la défense de l'ordre et à la prévention des infractions pénales dans une société démocratique.

La jurisprudence de la Cour de Strasbourg regorge d'affaires soulevant la problématique de la protection des données personnelles sur la base de l'article 8 de la Convention, notamment en ce qui concerne la collecte de données personnelles telle que l'ADN ou les empreintes digitales¹¹, les procédés de surveillance secrète¹² et l'interception des communications privées¹³. En outre, la Cour rappelle que les Etats doivent s'abstenir de toute ingérence susceptible de violer le respect au droit à la vie privée mais met également à leur charge une obligation positive, dans certaines circonstances, de garantir l'effectivité du droit au respect de la vie privée. On peut alors y voir une responsabilisation de l'Etat envers la protection des données de ses citoyens, l'Etat devant intervenir comme garant lorsque la protection n'est plus effective.

La jurisprudence de la Cour européenne des droits de l'Homme accorde également une attention particulière à l'égard de la confidentialité des données médicales et au rôle que joue le consentement du patient dans la divulgation de ses données. En effet, ces données constituent par leur nature des informations profondément intimes à propos de la vie privée du patient. En conséquence, il n'est permis de déroger au secret médical et à l'exigence du consentement du patient que dans des cas exceptionnels et après pondération des intérêts en présence¹⁴.

2.2. La Convention n°108

Notre société se voit profondément bouleversée par l'émergence de nouvelles techniques de l'information et de la communication dès les années 1960¹⁵. Ces découvertes ont directement un impact sur le droit à la vie privée des citoyens et sur ses diverses facettes : droit du travail, droit des entreprises, droit administratif. Malgré une interprétation évolutive et dynamique de l'article 8 de la CEDH, le droit a besoin de s'adapter à la mutation sociétale et aux développements technologiques, pour faire en sorte de protéger de manière appropriée les individus¹⁶. Par conséquent, le Conseil de l'Europe adopte le 28 janvier 1981, une législation

¹¹ Cour eur. D.H., *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n° 30562/04 et 30566/04.

¹² Cour eur. D.H., *Klass et autres c. Allemagne*, 6 septembre 1978, req. n°5029/71.

¹³ Cour eur. D.H., *Malone c. Royaume-Uni*, 2 août 1984, req. n°8691/79.

¹⁴ R. ERGEC, *op.cit.*, p. 700. L'auteur poursuit avec une illustration de l'arrêt *Z. c. Finlande*, où la Cour a jugé que la révélation par des médecins d'un état de séropositivité d'une personne sans son consentement, alors que cette personne est contrainte par la justice à témoigner, ne peut se justifier que dans l'intérêt des poursuites pour homicide volontaire dirigées contre son mari suspecté de l'avoir contaminée. Cour eur. D.H., *Z c. Finlande*, 25 février 1997, req. n°22009/93.

¹⁵ F. DEHOUSSE, T. VERBIEST, T. ZGAJEWSKI, *Introduction au droit de la société de l'information*, Bruxelles, Larcier, 2007, p. 7.

¹⁶ J. RIDEAU, *Les droits fondamentaux dans l'Union européenne*, Bruxelles, Bruylant, 2009, p. 61.

particulière à la protection des données personnelles, la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel¹⁷. Cette Convention est ouverte à la signature des Etats Membres du Conseil de l'Europe mais également à l'adhésion d'Etat tiers¹⁸. De plus, en 1999, elle est modifiée afin de pouvoir permettre à l'Union Européenne d'y adhérer.

La Convention n°108 est le premier, et reste à ce jour, le seul instrument international contraignant ayant pour objet la protection des personnes contre l'usage abusif du traitement automatisé des données à caractère personnel¹⁹. De par sa vocation universelle, elle dispose de la faculté de remédier à l'absence de convention mondiale dans ce domaine²⁰. La convention a également influencé de nombreuses politiques et législations en matière de protection des données, en premier lieu celles de la Commission européenne lorsqu'elle décida d'élaborer sa propre législation en la matière. Ainsi, la première directive de l'Union européenne sur ce sujet, la directive 95/46/CE, reprend expressément dans son préambule qu'elle précise et amplifie les principes établis par la Convention n°108²¹.

La Convention énonce les droits dont dispose l'individu sur ses données personnelles tels que le droit à l'information, le droit d'accès aux données, le droit à l'effacement ainsi que les principes directeurs que les acteurs, tant privés que publics, doivent respecter lors du traitement des données, comme par exemple le principe de minimisation, de loyauté ou encore de proportionnalité. Une partie est également consacrée au transfert des données hors Europe et aux données sensibles qui requièrent une protection particulière.

En ce qui concerne plus spécifiquement le rôle du consentement, la Convention est muette par rapport à ce dernier. Elle évoque les notions de traitement licite et de finalité légitime mais ne dresse pas de critères pour obtenir un traitement légitime. Ce n'est que dans certaines recommandations du Comité des ministres, que l'obligation de consentement a été mentionnée par la suite²².

3) L'UNION EUROPEENNE

3.1. Les directives relatives à la protection des données à caractère personnel

¹⁷ Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel adoptée le 28 janvier 1981 à Strasbourg par le Conseil de l'Europe. La convention compte actuellement 51 États Parties, à savoir les 47 États membres du Conseil de l'Europe et l'Uruguay, l'île Maurice, le Sénégal et la Tunisie. L'Argentine, le Burkina Faso, le Cap Vert et le Maroc ont également été invités à y adhérer et le Mexique vient d'en faire la demande.

¹⁸ Ainsi, l'Uruguay fut le premier pays non-européen à adhérer à la Convention en 2013.

¹⁹ F. DEHOUSSE, T. VERBIEST, T. ZGAJEWSKI, *op.cit.*, p. 279.

²⁰ J. WALTER, « Modernisation de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) », disponible à l'adresse http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/auditionlibe_/auditionlibe_en.pdf

²¹ Considérant 11 de la directive 95/46/CE.

²² Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 5.

3.1.1. Directive 95/46/CE

Suite à l'adoption de la Convention n°108, la Commission européenne constate que différents Etats membres ont adopté leur propre législation nationale sur la protection des données personnelles²³. Néanmoins, ces législations, par leur manque de concordance, étaient susceptibles d'entraîner des distorsions dans le marché intérieur²⁴. Le 24 octobre 1995, la Commission adopte la directive 95/46/CE relative à la protection des données²⁵, avec un double objectif : assurer la libre circulation des données entre Etats membres tout en garantissant un niveau équivalent de protection des données dans toute l'Union. La directive énonce les différents principes de licéité à respecter lors du traitement de données personnelles. Elle apporte également des droits spécifiques aux personnes concernées, comme le droit à l'information, à la consultation et, le cas échéant, à l'opposition au traitement ou à la rectification des données personnelles. Elle impose également l'obligation pour chaque Etat Membre d'instituer une autorité de contrôle afin de surveiller la bonne exécution de la directive.

A l'inverse de la convention n°108, il est convenu dès le départ de l'élaboration de la directive que le consentement constituerait un fondement juridique de légitimité du traitement des données²⁶. Ce sont les articles 2 et 6 de la directive qui fixent la définition et les conditions d'un consentement valable : libre, spécifique et informé. Nous reviendrons ultérieurement, plus en détails sur la conception du consentement dans la directive de 1995.

3.1.2. Directive 2002/58/CE

Au vu de l'essor des données qui transitent par voie électronique, la Commission européenne adopte en 2002 la directive 2002/58/CE relative au secteur des communications électroniques afin d'émettre des règles plus détaillées et particulières à ce domaine^{27 28}. La directive de 2002 règle notamment les questions relatives aux cookies²⁹ et au spamming³⁰. Ainsi, la

²³ Le Danemark, la France, le Royaume-Uni, l'Allemagne, l'Irlande, le Luxembourg, et les Pays-Bas. Notons que ce nombre est très significatif étant donné qu'il n'y avait que 12 Etats membres à l'époque.

²⁴ E. KOSTA, *Consent in European data protection law*, Leiden, Martinus Nijhoff, 2013, p. 84.

²⁵ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

²⁶ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 5.

²⁷ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Notons que cette directive sera ensuite modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques.

²⁸ M. BOURGEOIS, *Droit de la donnée : principes théoriques et approche pratique*, Paris, LexisNexis, 2017, p. 13.

²⁹ Les cookies informatiques ou « traceurs de connexion » sont « des fichiers textes stockés sur un terminal (ordinateur, smartphone) par exemple lors de la consultation d'un site internet, de la lecture d'un mail, de

directive affecte directement sur les techniques de marketing des entreprises qui basent essentiellement leur politique commerciale sur une philosophie de personnalisation du client³¹.

L'article 2, point f) et le considérant 17 de la directive 2002/58/CE, définissent la notion de consentement par référence à celle énoncée dans la directive 95/46/CE. Avec l'entrée en vigueur du nouveau règlement, il est convenu que la notion de consentement dans la directive de 2002 se fera en référence à la nouvelle définition du consentement³².

3.2. La Charte des droits fondamentaux de l'Union européenne

A l'origine, les traités fondateurs de l'Union européenne ne contiennent aucune référence relative aux droits de l'homme. Cela peut s'expliquer par le fait que, d'une part, l'objectif poursuivi était l'établissement d'un marché intérieur et que, d'autre part, la matière des droits de l'homme relevait essentiellement du Conseil de l'Europe. La Cour de justice a néanmoins progressivement appréhendé la dimension humaine au fil de sa jurisprudence, pour ensuite en déléguer la tâche au législateur européen³³.

Les Etats membres ont finalement adopté, le 7 décembre 2000, la charte des droits fondamentaux de l'Union européenne, instrument purement politique mais sans valeur juridique³⁴. Il faut attendre l'entrée en vigueur du traité de Lisbonne en 2009 pour que la Charte acquiert enfin une valeur juridique contraignante et équivalente aux traités instituant l'Union^{35 36}.

Tandis que l'article 7 énonce le droit au respect de la vie privée, l'article 8 de la Charte dispose quant à lui que : « Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ». La Charte des droits fondamentaux érige alors au rang de droit fondamental le droit à la protection des données personnelles, droit propre et distinct du droit au respect de la vie privée³⁷. Par le biais de cette disposition, la Charte des

l'installation d'un logiciel, etc ». Voy. V. FAUCHOUX, P. DEPREZ, F. DUMONT, J-M. BRUGUIERE, *Le droit de l'internet*, Paris, Lexis Nexis, 2017, p. 282.

³⁰ Le spamming correspond à l'envoi massif de courriers électroniques non sollicités, le plus souvent à des fins publicitaires.

³¹ A. BELLEIL, *E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'internet*, Paris, Dunod, 2001, p. 10.

³² E. KOSTA, *op.cit.*, p. 227.

³³ C. GAUTHIER, S. PLATON, D. SZYMCAK, *Droit européen des droits de l'Homme*, Paris, Dalloz, 2017, p. 32.

³⁴ Charte des droits fondamentaux de l'Union européenne adoptée le 7 décembre 2000 à Nice par l'Union européenne.

³⁵ Voy. article 6 §1 du Traité sur l'Union européenne.

³⁶ F. PICOD, S. VAN DROOGHENBROECK, *Charte des droits fondamentaux de l'Union européenne*, Bruxelles, Bruylant, 2018, p.13.

³⁷ F. PICOD, S. VAN DROOGHENBROECK, *op.cit.*, p.190.

droits fondamentaux se démarque de la CEDH, elle modernise les droits fondamentaux suite à une prise de conscience des bouleversements technologiques³⁸.

Quant à sa relation avec la directive 95/46/CE, la Cour de Justice précise que « les dispositions de la directive 95/46/CE, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux »³⁹.

En ce qui concerne le rôle du consentement, ce dernier est expressément reconnu dans la Charte⁴⁰. En effet, L'article 8, paragraphe 2, de cet instrument postule que les données à caractère personnel peuvent faire l'objet d'un traitement « sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ».

3.3. Le nouveau règlement européen sur la protection des données à caractère personnel

La Commission européenne constate que la directive de 1995 est déjà dépassée et qu'elle ne peut plus faire face aux nouveaux défis posés par les nouvelles technologies qui permettent une collecte et un stockage toujours plus important des données personnelles⁴¹. En effet, elle a été pensée à une époque où les réseaux sociaux, les objets connectés, la révolution des Big Data n'existaient pas encore⁴². Le Big data ou méga données désignent l'ensemble des données numériques créés par l'utilisation des nouvelles technologies dont le très grand volume requiert des outils d'analyse adaptés⁴³. De plus, les disparités résultant de la mise en œuvre de la directive, créent des insécurités juridiques, auxquelles il faut remédier grâce notamment à l'adoption d'un règlement qui permet une harmonisation totale de la matière⁴⁴. Les institutions européennes se lancent alors dans un long processus législatif faisant l'objet de plus de 4500 amendements et d'un intense lobbying. Le règlement général sur la protection des données est finalement adopté le 27 avril 2016⁴⁵. Son entrée en vigueur est fixée au 25 mai 2018 et les dispositions sont directement applicables dans l'ensemble des Etats membres le 25 mai 2018.

³⁸ *Ibidem*, p. 186.

³⁹ C.J.U.E., arrêt *Rechnungshof*, 20 mai 2003, aff. jointes C-165/01, C-138/01 et C-139/01.

⁴⁰ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 6.

⁴¹ G. SKOUMA, L. LEONARD, « Chapitre 1 - Les grands changements liés à la réglementation sur la protection des données personnelles et ses implications pratiques pour les entreprises et les professionnels » in A. GROSJEAN *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Éditions Larcier, 2015, p. 404.

⁴² B. DOCQUIR, *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, p. 10.

⁴³ D. BOURCIER, P. DE FILIPPI, *Open data & Big Data : nouveaux défis pour la vie privée*, Paris, Mare&Martin, 2016, p. 99.

⁴⁴ G. SKOUMA, L. LEONARD, *op.cit.*, p. 403.

⁴⁵ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) adopté le 27 avril 2016 et entra en vigueur le 25 mai 2018.

Dans la perspective de modernisation de la directive 95/46/CE, le nouveau règlement poursuit comme objectif le renforcement du contrôle de l'individu sur l'utilisation qui est faite de ses données, notamment en accentuant le rôle du consentement et le droit à l'information⁴⁶. Par le biais de ces changements, l'Union Européenne cherche à établir un climat de confiance dans le développement de l'économie numérique du marché intérieur⁴⁷. Elle tend également à responsabiliser les autorités, les entreprises, et toutes autres entités traitant de données personnelles.

Dans cette optique, le règlement établit, pour la première fois en matière de protection des données, un arsenal de sanctions en cas d'entorse, allant jusqu'à des amendes pouvant atteindre les 20 millions d'euros ou 4% du chiffre d'affaires⁴⁸. Un vent de panique souffle sur les entreprises, inquiètes de ne pas être conformes au nouveau règlement. On peut raisonnablement penser que ce nouvel élément va sensibiliser au respect de la nouvelle législation.

La définition du consentement est redéfinie et remodelée afin de poursuivre le principal objectif du nouveau règlement, à savoir le renforcement des droits des citoyens sur leurs données. Nous aborderons les changements relatifs à la notion du consentement dans la seconde partie de notre travail.

B) DÉFINITIONS ET ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES

1) GENERALITES

1.1. Définition d'une donnée personnelle

Le Règlement européen définit les données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Il précise ensuite que pour être considéré comme une personne identifiable, il suffit de « pouvoir être identifié, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »⁴⁹.

La philosophie du règlement étant la protection des données personnelles des citoyens de l'Union européenne, le règlement s'applique uniquement aux personnes physiques. Ainsi sont

⁴⁶ COMMISSION EUROPEENNE, Communiqué de presse du 4 novembre 2010 : « Une approche globale de la protection des données à caractère personnel dans l'Union européenne ».

⁴⁷ J. VETOIS, « L'Europe redéfinit la protection des données personnelles », *Terminal*, 2013, p. 1.

⁴⁸ G. SKOUMA, L. LÉONARD, *op.cit.*, p. 417.

⁴⁹ Article 4, al. 1^{er} du Règlement 2016/679.

exclues les données à caractère personnel relatives aux personnes morales et, en particulier, aux entreprises dotées de la personnalité juridique⁵⁰ et celles relatives aux personnes décédées⁵¹.

Il existe certaines données potentiellement plus sensibles pour le respect de la vie privée, par le simple fait qu'elles apportent des informations particulièrement intimes sur l'individu. Ainsi, les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle ou l'orientation sexuelle d'une personne sont considérées comme des données sensibles. Sont également visées par cette notion, les données génétiques, biométriques et médicales. Une protection plus élevée doit leur être accordée. La législation interdit en principe leur traitement, sous réserve d'exceptions telles que le consentement de la personne concernée, des motifs d'intérêt public ou encore l'exécution d'obligations contractuelles⁵².

1.2. Définition d'un traitement

La législation vise les traitements de données à caractère personnel, automatisés en tout ou en partie, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier⁵³. Un grand nombre de personnes peuvent se méprendre sur le champ d'application du règlement, en partie du fait qu'il est la conséquence de l'émergence croissante du traitement informatisé des données. Or, le traitement manuel tombe également sous la protection du règlement si les données à caractère personnel sont contenues ou destinées à être contenues dans un fichier structuré⁵⁴.

La législation couvre un éventail très large de situations. Les opérations ainsi visées sont notamment la collecte, le stockage, la modification, l'extraction, la consultation, le transfert de données à caractère personnel.

2) ENJEUX DES DONNEES PERSONNELLES

2.1. Enjeux économiques

Avant de nous plonger au cœur de notre sujet, il est important de souligner l'importance que les données personnelles représentent aujourd'hui, spécialement dans le secteur commercial. « Si c'est gratuit, c'est vous le produit » est une célèbre maxime dans l'environnement en ligne. De par le fait que les données sont à présent monétisables, il existe un véritable marché des données personnelles, certains allant jusqu'à parler du nouvel or noir du 21ème siècle. Le

⁵⁰ *Ibidem*, consid. 14.

⁵¹ *Ibidem*, consid. 27. Sur ce dernier point étonnant, notamment pour des données médicales qui pourraient concerner des apparentées vivantes, notons que le règlement permet aux Etats Membres de prendre les dispositions qu'ils estimeront utiles.

⁵² *Ibidem*, article 9.

⁵³ *Ibidem*, article 3.

⁵⁴ C. PIERRE-BEAUSSE, *La protection des données personnelles*, Luxembourg, Editions pomoculture, 2005, p. 29.

phénomène « Big data »⁵⁵ amplifie la possibilité d'espaces de stockage et d'échanges de données pour les entreprises. Une certaine logique s'est alors installée dans le paysage économique : l'entreprise ayant collecté le plus d'informations sur les consommateurs serait la plus à même de contrôler ceux-ci⁵⁶. Ce postulat soulève inévitablement, outre des questions sur le droit de la vie privée, des questions relatives au droit de la concurrence en ce qu'elle permet à l'entreprise de détenir un pouvoir de marché⁵⁷.

Dans l'environnement du commerce en ligne, le marketing ciblé cherche à personnaliser les offres aux clients dans une perspective plus durable de fidélisation. La pratique des cookies en est l'exemple le plus démonstratif. Cette révolution de l'information met en concurrence deux grands paradigmes, d'une part, la liberté de l'échange et du commerce et, d'autre part, le respect de la vie privée. Des enquêtes menées en Europe ainsi qu'aux Etats-Unis ont souligné l'inquiétude et la méfiance des consommateurs à l'encontre des pratiques du commerce en ligne⁵⁸. Les récentes affaires divulguant des scandales propres aux sites tels que Facebook ou Google, alimentent les appréhensions des internautes.

L'exploitation de données personnelles collectées sur internet avec des objectifs économiques sous-jacents pose problème. Il est nécessaire que le droit intervienne pour encadrer ces pratiques et empêcher les abus. Il est également de l'intérêt des entreprises de prendre en considération ces notions de droit au respect de la vie privée notamment dans la perspective d'établir un climat de confiance pérenne avec leur clientèle.

2.2. Enjeux politiques et sociétaux :

A côté des enjeux économiques évidents de l'exploitation des données personnelles, il existe également des enjeux d'ordre politiques et sociétaux. Il est habituel d'associer les techniques de surveillance comme moyen politique d'asservissement du peuple⁵⁹. De nombreux ouvrages littéraires en font la référence. On pense tout d'abord, en matière de contrôle de la vie privée, au célèbre roman d'anticipation de Georges Orwell, « 1984 »⁶⁰, et sa société contrôlée par Big Brother. Le roman est d'ailleurs souvent cité, parfois de façon excessive, pour nous mettre en garde sur les dérives potentielles du traitement de nos données dans nos sociétés contemporaines. Par exemple, les données extraites à partir de notre géolocalisation, ou encore les procédés de reconnaissance faciale, pourraient être utilisées à mauvais escient en vue d'exercer un contrôle permanent sur les citoyens.

⁵⁶ A. BELLEIL, *E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'internet*, Paris, Dunod, 2001, p. 31.

⁵⁷ M. BOURGEOIS, *op.cit.*, p. 279.

⁵⁸ J. FRAYSSINET, « La protection des données personnelles est-elle assurée sur l'Internet ? » in G. CHATILLON, *Le droit international de l'internet*, Bruxelles, Bruylant, 2003, p. 435.

⁵⁹ Voy. C. RAGOUCY, « Le panoptique et 1984 : confrontation de deux figures politiques d'asservissement », *Psychanalyse*, vol. 18, 2010, pp. 45-58.

⁶⁰ 1984 est un roman d'anticipation publié en 1949 par l'écrivain anglais George Orwell.

Dans le même ordre d'idées, Michel Foucault, dans « Surveiller et punir », analyse le panoptique imaginé par Bentham au 19^{ème} siècle comme une technique permettant la surveillance la plus efficace et la plus complète possible des prisonniers⁶¹. Le procédé a l'avantage d'être totalement anonyme, de sorte que les prisonniers ne peuvent jamais savoir s'ils sont surveillés ou non. L'architecture virtuelle engendrée par le World Wide Web (W.W.W.) constitue en quelque sorte la concrétisation du panoptique de Bentham à une échelle mondiale. Les nouvelles technologies de traitement massif de données (Big Data) permettent non seulement la surveillance des citoyens mais également la connaissance de ceux-ci jusque dans leurs pensées les plus intimes, le plus souvent à leur insu.

D'un autre côté, ces extractions de données sont également très utiles en matière de prévention de toutes sortes de crimes et délits. En Europe, la promotion d'une coopération policière et judiciaire encourage l'échange d'informations, telles que les empreintes digitales ou les immatriculations de véhicules⁶². La protection des données personnelles est alors amoindrie dans ce contexte où l'intérêt collectif prime sur l'intérêt individuel⁶³. En cela, les traitements de données à caractère personnel à finalité de sécurité publique échappent à une série de dispositions de la réglementation européenne. Par ailleurs, les banques sont fortement touchées par la législation sur la protection des données en ce qu'elles doivent jouer un rôle actif dans la lutte contre le blanchiment d'argent et le financement du terrorisme.

II. LE CONSENTEMENT COMME OUTIL DE PROTECTION DES DONNÉES PERSONNELLES ?

A) LA NOTION DE CONSENTEMENT DANS LA PROTECTION DES DONNÉES PERSONNELLES

1) GENERALITES

Le consentement peut être défini comme l'expression d'une manifestation de volonté. En droit, il revêt une fonction particulière, en ce qu'une personne, par son consentement, pourrait accepter une situation juridique susceptible de lui causer un préjudice.

Notion fondamentale dans la pensée juridique, le consentement est omniprésent, que ce soit par exemple en droit pénal, lorsqu'il conditionne l'interprétation d'une situation litigieuse comme licite ou illicite, ou en droit des contrats, dans lequel il constitue une des conditions

⁶¹ N. THIRION, *Théorie du droit : droit, pouvoir, savoir*, Bruxelles, Larcier, 2011, p. 69.

⁶² Voy. la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

⁶³ C. CASTETS-RENARD, *Quelle protection des données personnelles en Europe ?*, Larcier, Bruxelles, 2015, p.30.

essentielles de validité de l'acte établi entre les parties⁶⁴. La matière de protection des données n'échappe pas à ce postulat. En effet, dans le nouveau règlement, on retrouve le consentement en tant que condition de légitimation du traitement des données. Le consentement est cité en premier parmi les autres conditions de licéité, ce qui, pour certains, démontre son importance fondamentale dans le domaine.

2) ANCIEN REGIME DE LA DIRECTIVE 95/46/CE

2.1. Définition du consentement

L'ancienne directive 95/46/CE, dans son article 2 (h), définit le consentement comme « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement »⁶⁵.

En outre, dans son article 7, la directive énonce le consentement comme procédé de légitimation du traitement de données personnelles et précise que la personne concernée doit avoir donné son consentement de manière *indubitable*⁶⁶.

2.2. Particularité des données sensibles

Une protection particulière est mise en place pour le traitement de données sensibles, en raison de l'ingérence grave que le traitement de ces données peut engendrer au niveau de la vie privée⁶⁷. En conséquence, le traitement de ces données sensibles est interdit sauf dérogations prévues par la législation, dont le consentement de la personne concernée.

La condition d'obtention du consentement est plus stricte en ce que le consentement doit être *explicite* et non plus *indubitable*. En droit, l'expression « consentement explicite » a la même signification qu'un consentement exprès⁶⁸. Il est alors donné généralement par une signature, qu'elle soit manuscrite ou électronique. Il est admis également qu'un consentement explicite soit donné oralement, toutefois il est plus difficile à prouver, ce qui peut être problématique⁶⁹.

En ce qui concerne spécialement les moyens de donner son consentement à l'exploitation de données sensibles dans l'environnement en ligne, la signature électronique ou numérique, en plus d'être un consentement explicite valable, a l'avantage d'avoir une importante force probante⁷⁰. Le consentement explicite peut être également valablement donné lorsqu'il est demandé à la personne concernée, en plus de consentir, de compléter un formulaire

⁶⁴ Article 1108 du Code civil belge.

⁶⁵ Art. 2, h), de la Directive 95/46/CE.

⁶⁶ Art. 7, de la Directive 95/46/CE.

⁶⁷ Art. 8, de la Directive 95/46/CE.

⁶⁸ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 28.

⁶⁹ *Ibidem*.

⁷⁰ *Ibidem*.

d'inscription en ligne où les utilisateurs doivent remplir leurs coordonnées afin de s'identifier⁷¹.

2.3. Faiblesses du consentement

En matière de consentement, un des reproches adressés à la directive est de ne pas expliquer davantage ce que l'on entendait par un consentement *libre, spécifique et informé*. En outre, la notion de consentement *indubitable* porte également à confusion lorsqu'on la compare avec la notion de consentement *explicite*⁷². Il n'est pas toujours aisé d'apprécier ce que constitue un consentement authentique, non-univoque, ce qui amène certains responsables de traitement des données à abuser de la faiblesse de la définition, spécialement dans l'environnement en ligne.

Dans la mesure où la nature juridique de la directive entraîne une possibilité pour les Etats membres de transposer la notion de consentement selon leurs interprétations, il en résulte des approches différentes⁷³. Ces disparités ont entraîné des incohérences qui créent de la complexité, de l'insécurité juridique et des coûts administratifs⁷⁴. De l'insécurité juridique, notamment en affaiblissant la position des personnes concernées sur la maîtrise de l'utilisation de leurs données. Une illustration de ces divergences peut être que certains admettent un consentement implicite alors que d'autres requièrent l'obligation générale d'obtenir un consentement écrit⁷⁵.

3) INTERVENTION DU GROUPE DE TRAVAIL 29

En 2010, la Commission européenne a demandé un travail général de contribution sur la révision de la directive 95/46/CE. Le Groupe de travail article 29 sur la protection des données (ci-après « G29 ») est un organe consultatif européen indépendant sur la protection des données personnelles et de la vie privée^{76 77}. Dans son avis 15/2011, le travail du G29 se concentre exclusivement sur le rôle du consentement en matière de protection des données personnelles⁷⁸. L'objectif poursuivi est double : d'une part, le groupe clarifie la plupart des dispositions ambiguës de la directive et d'autre part, en vue de la révision de la directive, le groupe propose les changements à apporter à la définition du consentement⁷⁹.

⁷¹ *Ibidem*, p. 30.

⁷² E. KOSTA, *op.cit.*, p. 149.

⁷³ *Ibidem*, p. 148.

⁷⁴ COMMISSION EUROPEENNE, Communiqué de presse du 21 décembre 2015 : « Questions réponses : la réforme de la protection des données ».

⁷⁵ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 3.

⁷⁶ A. BENSOUSSAN, *La protection des données personnelles de A à Z*, Bruxelles, Bruylant, 2017, p.50.

⁷⁷ Voy. articles 29 et 30 de la directive 95/46/CE pour l'organisation et les missions du groupe 29.

⁷⁸ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition, adopté le 13 juillet 2011, p. 30.

⁷⁹ *Ibidem*, p. 1.

Toutefois, précisons que ces lignes directrices ne sont pas juridiquement contraignantes, elles n'ont donc pas de réelle portée juridique. Les clarifications apportées à cette époque présentent néanmoins un intérêt, spécialement dans l'environnement en ligne, où il était difficile d'établir une pratique conforme à la directive.

3.1. Modalité du consentement

3.1.1. Utilisation adéquate du consentement

Il est capital de choisir correctement le fondement juridique sur lequel repose le traitement de données personnelles, afin de ne pas amoindrir l'efficacité du consentement dans une situation où il serait inapproprié⁸⁰. Le groupe de travail 29 insiste pour rappeler qu'il existe cinq autres moyens de légitimer un traitement de données personnelles⁸¹. En plus du consentement, l'article 7 de la directive énonce notamment l'exécution d'un contrat auquel la personne concernée est partie, les missions d'intérêt public ou encore l'intérêt légitime du traitement.

Les autres fondements pour légitimer le traitement des données personnelles induisent un critère de nécessité qui restreint significativement le contexte dans lequel chacun peut s'appliquer. Il ne faut pas pour autant en déduire que l'obligation de consentement dispose d'une plus grande marge de manœuvre par rapport aux autres fondements juridiques⁸².

3.1.2. Moment où le consentement est donné

Malgré le silence de la directive sur le moment où le consentement doit être donné, il est convenu de manière unanime que le consentement doit être obtenu avant le début de traitement des données⁸³. Dans l'hypothèse d'un changement de finalité durant le traitement des données, un nouveau consentement est requis.

3.1.3. Forme du consentement

En ce qui concerne la forme que doit revêtir le consentement, la directive ne précise rien, elle énonce simplement que le consentement est « toute manifestation », ce qui englobe aussi bien le consentement écrit qu'oral. Les termes « manifestation de volonté » et « accepte » induisent inévitablement une action de la personne concernée. En ce qui concerne le consentement déduit d'une absence de comportement de la personne concernée, cela peut être considéré comme consentement valable uniquement si aucun doute sur les intentions de la personne concernée ne peut être soulevé⁸⁴.

⁸⁰ *Ibidem*, p. 11.

⁸¹ *Ibidem*, p. 7.

⁸² *Ibidem*, p. 8.

⁸³ *Ibidem*, p. 10.

⁸⁴ *Ibidem*, p. 23.

L'article 7 de la directive conforte cette interprétation en ce qu'il requiert un consentement indubitable de la personne concernée, c'est-à-dire qui ne laisse aucun doute. Le G29 illustre ses propos avec un exemple assez éloquent : une entreprise envoie et informe cent clients par courrier électronique que leurs données vont faire l'objet d'un transfert sauf s'ils s'y opposent dans les deux semaines. Seulement dix clients s'y opposent. Concernant les 90 autres clients, on ne peut avancer de façon certaine qu'ils ont donné leur accord de façon non-ambiguë⁸⁵. Les conditions émises par la directive ne sont dès lors pas rencontrées.

3.1.4. Le consentement dans la directive 2002/58/CE

La directive 95/46/CE et la directive 2002/58/CE ne s'excluent pas⁸⁶. Par conséquent, les conditions générales d'un consentement valable aux yeux de la directive 95/46/CE s'appliquent également à la directive 2002/58/CE. La directive 2002/58/CE (vie privée et communications électroniques) détaille seulement ces conditions dans le cadre plus spécifique des services en ligne.

3.2. Caractéristiques du consentement

3.2.1. Un consentement libre

Le G29 aborde tout d'abord le souci d'obtenir un consentement *libre*⁸⁷. C'est-à-dire un consentement obtenu sans aucune contrainte, intimidation mais aussi sans aucune tromperie. Le groupe vise notamment les situations où on est en présence d'une relation comportant un lien de subordination avec le responsable du traitement des données, tel que dans les rapports professionnels ou dans le cadre des services publics de la santé.

Un appel d'offre d'emploi est le premier exemple évocateur de cette relation de subordination. Il est demandé au candidat de communiquer des données personnelles, parfois intimes, sur sa personne. L'autonomie de la personne concernée se voit particulièrement amoindrie dans ces situations. Il est alors légitime de penser que, la plupart du temps, le consentement du candidat dans le besoin d'un emploi relève de l'artificiel⁸⁸. Le consentement n'est dès lors pas le fondement juridique le plus approprié. C'est pourquoi, dans ces hypothèses, un examen approfondi pour savoir si la personne a réellement donné son consentement de manière libre est requis.

Par ailleurs, le groupe 29 admet des hypothèses où le consentement de la personne concernée est valable dans le cadre professionnel. Par exemple, une entreprise demande à ses employés s'ils acceptent ou non qu'une photographie de leur personne soit mise à côté de leur nom sur

⁸⁵ *Ibidem*, p. 13.

⁸⁶ *Ibidem*, p. 12.

⁸⁷ *Ibidem*, p. 12.

⁸⁸ F. RIGAUX, *op.cit.*, p. 585.

l'intranet. Si l'employé envoie une photo, cet envoi sera considéré comme un consentement valide⁸⁹.

3.2.2. Un consentement spécifique

Pour être valable, le consentement doit être *spécifique*, c'est-à-dire qu'il ne doit pas être de portée générale mais bien porter sur un traitement précis⁹⁰. Cette condition est étroitement liée à la condition d'information du consentement, dans la mesure où le consentement est spécifique dès qu'il porte sur les informations fournies à la personne concernée⁹¹. Pour obtenir un consentement spécifique, le consentement ne doit pas être donné de manière générale, mais il doit porter sur une finalité exacte du traitement de données⁹².

Prenons comme exemple les réseaux sociaux qui permettent l'utilisation d'applications externes. De manière générale, lorsque les utilisateurs désirent utiliser une application externe, on demande le consentement de ces derniers pour la transmission de leurs données au concepteur de l'application, notamment dans une perspective de publicité comportementale et de revente à des tiers. Toutefois, l'application peut marcher sans le transfert de ces données. Pour se conformer à l'exigence de spécificité, il est recommandé de demander un consentement distinct, l'un pour la revente à des tiers et l'autre pour la publicité comportementale⁹³.

3.2.3. Un consentement informé

L'obligation d'information aspire à rendre le processus de traitement de données plus transparent aux yeux de la personne concernée⁹⁴. L'article 10 de la directive énonce les différentes informations essentielles à transmettre à la personne concernée à propos du traitement de ses données : identité du responsable de traitement des données, les finalités du traitement, etc.

Le G29 précise deux exigences supplémentaires relatives à l'obligation d'information afin d'obtenir une décision suffisamment éclairée de la part de la personne concernée, portant, d'une part, sur la qualité des informations et, d'autre part, sur l'accessibilité et la visibilité des informations⁹⁵. Concernant la qualité des informations, celles-ci doivent être transmises dans un langage simple, clair et compréhensible pour tout utilisateur moyen. Ainsi, l'emploi d'un jargon juridique est à proscrire. Ensuite, les informations fournies doivent être directement visibles, faciles d'accès pour la personne concernée de sorte qu'elles ne puissent lui échapper.

⁸⁹ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 15.

⁹⁰ M. BOURGEOIS, *op.cit.*, p. 71.

⁹¹ E. KOSTA, *op.cit.*, p. 219.

⁹² Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 18.

⁹³ *Ibidem*, p. 19.

⁹⁴ *Ibidem*, p. 10.

⁹⁵ *Ibidem*, p. 21.

3.2.4. Un consentement indubitable

Outre les conditions exigées à l'article 7 de la directive, le consentement doit également être *indubitable*. Cela signifie que la manifestation de volonté de la personne concernée afin de marquer son accord ne doit laisser aucun doute quant à son intention de celle-ci⁹⁶. En conséquence, un consentement déduit de l'inaction ou du silence de la personne concernée, en particulier dans l'environnement en ligne, ne peut constituer un consentement valable.

On vise ici en particulier les démarches de marketing basées sur les concepts d'opt-in ou d'opt-out à des fins de prospection. La définition du consentement par le G29 rejette le concept de l'opt-out en ce qu'il repose sur un consentement présumé, et qui plus est, un consentement où la personne concernée reste passive. La méthode de l'opt-out inscrit par exemple un internaute à un service de manière implicite et l'oblige à se désabonner de lui-même à ce service⁹⁷. Il s'agit également des paramètres de confidentialité par défaut des réseaux sociaux, dans la mesure où l'utilisateur doit cliquer sur un bouton s'il désire que ses photos ne puissent pas être vues par les amis d'amis. S'il n'entreprend pas cette démarche, cela est considéré comme un consentement par le responsable de traitement des données. Or, l'absence de démarche de la personne concernée ne répond pas aux exigences d'un consentement indubitable. On ne peut pas affirmer, sans aucun doute, qu'il n'y a pas d'ambiguïté sur l'octroi du consentement de la personne concernée. Le groupe de travail est très clair lorsqu'il déclare, à propos de la prospection directe, qu'« un consentement présumé à recevoir des messages électroniques n'est pas non plus conforme à la définition du consentement de la directive 95/46/CE ... Dans le même ordre d'idées, les cases pré-cochées, par exemple sur des sites web, ne sont pas davantage compatibles avec la définition de la directive »⁹⁸.

L'opt-in, quant à lui, repose sur un consentement explicite et préalable, que la personne concernée doit donner avant d'être la cible d'une prospection directe⁹⁹. Prenons la situation où un commerce désire envoyer sa newsletter à un de ses clients. Pour ce faire, elle doit d'abord lui demander son consentement, par exemple en cochant une case, pour ensuite lui envoyer par courrier électronique sa publicité. Ce procédé respecte ainsi les modalités de mise en œuvre du consentement indubitable.

4) CHANGEMENTS APPORTES AU CONSENTEMENT SOUS LE NOUVEAU REGLEMENT 2016/679

⁹⁶ *Ibidem*, p. 23.

⁹⁷ P. CHRISTIAN, C. FERAL-SCHUHL, « Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique », octobre 2015, disponible à l'adresse <http://www2.assemblee-nationale.fr/documents/notice/14/rapports/r3119/>

⁹⁸ Avis 5/2004 du Groupe de travail « Article 29 » portant sur la communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE, adopté le 27 février 2004.

⁹⁹ E. KOSTA, *op.cit.*, p. 188.

Afin d'atteindre l'objectif poursuivi par la nouvelle législation, à savoir le renforcement du contrôle des citoyens sur l'utilisation qui est faite de leurs données, le nouveau règlement s'est attaché à redéfinir le consentement de manière plus stricte et détaillée.

4.1. Définition du consentement

A présent, l'article 4, 11) du Règlement définit le consentement comme : « toute manifestation de volonté, libre, spécifique, éclairée et *univoque* par laquelle la personne concernée accepte, par une déclaration ou par un *acte positif clair*, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

On constate que l'adjectif univoque vient remplacer la notion d'indubitable, jugée inadaptée dans la mesure où l'adjectif créait de l'insécurité juridique. De plus, le règlement requiert formellement une action positive de la part de la personne concernée. La législation précise la manière dont le consentement peut être donné. Ainsi, le consentement est valable lorsqu'il est demandé à la personne concernée de cocher une case ou lorsqu'elle doit opter pour certains paramètres techniques lors de la consultation d'un site internet¹⁰⁰. Il suffit d'avoir un comportement qui dans le contexte dans lequel la personne concernée se trouve, indique de manière claire que la personne concernée accepte le traitement de ses données personnelles.

Par conséquent, le règlement affirme par là clairement que le système d'opt-out, basée sur une case pré-cochée, n'est pas un procédé valable. Il ne saurait y avoir un consentement valable alors qu'il est présumé ou fondé sur le silence de la personne concernée, sur une case cochée par défaut ou sur une inactivité de la personne concernée¹⁰¹. Grâce à cette consécration juridique, les responsables de traitement de données n'ont plus la possibilité de récolter le consentement par des procédés sournois.

Le considérant 3 précise, quant à lui, les moyens par lesquels une personne concernée pourrait donner un consentement valable, ce qui n'était pas le cas dans la précédente directive. Le règlement énonce la déclaration écrite, y compris électronique ou la déclaration orale.

4.2. Charge de la preuve

L'article 7 du Règlement précise que le responsable du traitement des données doit être à présent en mesure, lorsque le traitement repose sur le consentement d'une personne, de prouver que la personne concernée a consenti au traitement de ses données¹⁰². La charge de la preuve repose alors sur le responsable du traitement.

4.3. Déséquilibre significatif

¹⁰⁰ Considérant 32 du Règlement.

¹⁰¹ *Ibidem*.

¹⁰² Voy. également le considérant 42 du Règlement.

Les rapports de pouvoirs entre les différents acteurs sont généralement déséquilibrés. Sur recommandation du groupe 29, le règlement intègre ce facteur dans la définition d'un consentement *libre*. En effet, le considérant 43 souligne qu'il ne peut y avoir de consentement valable s'il existe un déséquilibre manifeste entre le responsable du traitement et la personne concernée et précise ensuite « en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière ».

4.4. Consentement informé

La notion de consentement informé est également précisée dans les considérants 39 et 42 du règlement. Conformément au considérant 39, les informations relatives au traitement des données à caractère personnel doivent être aisément accessibles, faciles à comprendre et formulées en des termes clairs et simples. De plus, le considérant 42 précise que pour obtenir un consentement éclairé de la part de la personne concernée, les informations concernant l'identité du responsable du traitement et les finalités du traitement auxquelles sont destinées ces données doivent lui être communiquées. Les conditions supplémentaires exigées par le G29 en ce qui concerne la qualité d'un consentement informé ont été formellement concrétisées dans la réglementation.

4.5. Protection renforcée pour les personnes vulnérables

Sous son article 8, la législation européenne en matière de protection des données a pour la première fois intégré une disposition spécifique relative aux mineurs de moins de 16 ans. Le considérant 38 souligne à juste titre que les enfants sont des personnes vulnérables qui sont moins conscientes des risques et des conséquences d'exposer en ligne leurs données personnelles. Pour ces raisons, ils méritent une protection particulière que le groupe de travail 29 avait déjà mentionnée dans ces lignes directrices¹⁰³.

A présent, lorsque la personne concernée est âgée de moins de 16 ans, le traitement de ses données n'est licite que si le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. De plus, le paragraphe 2 ajoute que le responsable de traitement doit vérifier de manière raisonnable que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles. La protection de l'enfant est donc assurée par ses parents ainsi que par le responsable du traitement.

4.6. Du droit de retirer son consentement

Conformément à l'article 7 (3), la personne concernée est à présent autorisée à retirer son consentement à tout moment. Soulignons toutefois que le retrait du consentement n'a pas

¹⁰³ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 31.

d'effet rétroactif : ainsi le retrait ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. Le droit au retrait du consentement doit avoir été communiqué à la personne concernée avant qu'elle ne consente au traitement de ses données. C'est une réelle avancée car auparavant, la directive ne permettait l'effacement des données que si le traitement ne respectait pas les dispositions de la directive, notamment en raison du caractère incomplet ou inexact des données¹⁰⁴. A présent, la personne concernée ne doit plus justifier sa demande de retrait.

Cette nouvelle disposition est à mettre en parallèle avec l'article 17 du règlement qui consacre, après de longs débats en Europe et spécialement depuis la jurisprudence *Google c. Spain*¹⁰⁵, le droit à l'effacement, plus communément appelé le droit à l'oubli numérique (« Right to be forgotten »). En effet, la disposition offre la possibilité, à la personne concernée, d'obtenir l'effacement de ses données dans les meilleurs délais, dans la mesure notamment où elle a retiré son consentement sur lequel le traitement se fonde¹⁰⁶. Notons toutefois que, dans ce cas précis, le responsable du traitement des données pourra éventuellement opposer un autre fondement juridique au traitement des données¹⁰⁷. De plus, de nombreuses exceptions existent à ce principe, à commencer par le droit à la liberté d'expression¹⁰⁸. Ainsi, lorsque les informations qui sont divulguées présentent un intérêt pour le public à être publiées, le droit à l'oubli numérique cède devant le droit à la liberté d'expression et d'information^{109 110}.

B) REMISE EN QUESTION DE LA NOTION DE CONSENTEMENT COMME OUTIL DE PROTECTION À L'ÉGARD DES DONNÉES PERSONNELLES

1) REMISE EN CAUSE DU CONSENTEMENT

1.1. Les limites du consentement à l'ère numérique

¹⁰⁴ Article 12 (b), directive 95/46/CE.

¹⁰⁵ C.J.U.E., arrêt *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, 13 mai 2014, aff. C-131/12.

¹⁰⁶ L'article énonce différentes possibilités au droit à l'oubli, à côté du consentement. Ainsi, la personne concernée peut également demander le droit à l'oubli numérique lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, lorsque les données ont fait l'objet d'un traitement illicite.

¹⁰⁷ M. BOURGEOIS, *op.cit.*, p. 232.

¹⁰⁸ Article 17, § 3, du Règlement énonce comme exception : l'exercice du droit à la liberté d'expression et d'information, le respect d'une obligation légale, l'exécution d'une mission d'intérêt public, l'existence de motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, à l'exercice ou à la défense de droits en justice.

¹⁰⁹ C. DE TERWANGNE, « Chapitre 3 - Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique » in A. GROSJEAN, *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Éditions Larcier, 2015, p. 258. (245-275)

¹¹⁰ Pour plus de détails sur le sujet de la liberté d'expression face au respect de la vie privée et la protection des données personnelles, nous renvoyons le lecteur à l'ouvrage : S. CARNEROLI, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli*, Bruxelles, Larcier, 2016, pp. 77-102.

La législation s'appuie sur le consentement de l'individu comme outil de protection des données personnelles. Le consentement, en ce qu'il est l'expression d'un libre choix, est étroitement lié à l'autonomie du sujet¹¹¹. Une vulgarisation de la théorie kantienne définit l'autonomie comme le choix qui ne repose que sur la volonté propre de l'homme. Elle s'oppose à l'hétéronomie qui suppose un choix de l'individu influencé par un élément extérieur, tel qu'une contrainte, une loi, un devoir¹¹².

Toutefois, à l'heure du W.W.W. et des « Big Data » il est légitime de se demander si on peut encore prétendre à une vie privée. Christophe Lazaro et Daniel Le Métayer énoncent à juste titre à ce propos que « l'idée même de consentement est fortement questionnée, tant les développements technologiques de ces dernières années ainsi que les pratiques sociales qu'ils génèrent semblent battre en brèche la capacité, voire même la volonté, des individus d'exercer un véritable contrôle sur leurs données personnelles »¹¹³.

Dans la présente section, nous évaluons le rôle du consentement en matière de protection des données personnelles à l'aune des nouveaux défis engendrés par l'environnement numérique. Alors que certains considèrent le consentement comme la pierre angulaire de l'autonomisation de l'individu et de la protection de ses données personnelles, d'autres émettent de vives critiques à son encontre, questionnant ses vertus et allant jusqu'à dire qu'il est une démarche vaine.

1.1.1 Absence de maîtrise intellectuelle

Dans « Les principes de philosophie »¹¹⁴, Descartes souligne que « nous ne nous trompons que lorsque nous jugeons de quelque chose qui ne nous est pas assez connu ». Il relevait ensuite que « bien souvent nous donnons notre consentement à des choses dont nous n'avons jamais eu qu'une connaissance fort confuse ».

Ainsi, le premier argument avancé par tous les détracteurs du consentement est d'ordre cognitif, en ce qu'ils soulignent l'absence de maîtrise intellectuelle des personnes concernées, ne permettant pas de saisir concrètement les informations fournies¹¹⁵. Comme souligné précédemment, une des réformes entreprises par le nouveau règlement est de simplifier les informations apportées à la personne concernée, avec pour objectif de les rendre accessibles et compréhensibles, en s'abstenant de tout recours à un langage juridique abscond.

¹¹¹ Voy. en ce sens E. KOSTA, *op.cit.*, pp. 130-140.

¹¹² R. LE COADIC, « Autonomie, illusion ou projet de société ? », *Cahier internationaux de sociologie*, vol. 121, 2006, p. 318.

¹¹³ C. LAZARO, D. LE MÉTAYER, « Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet », *Revue juridique Thémis de l'Université de Montréal*, vol. 48, 2014, p. 766.

¹¹⁴ R. DESCARTES, *Les principes de philosophies*, Paris, Henry Le Gras, 1647.

¹¹⁵ J. EYNARD, « L'éthique à l'épreuve des nouvelles particularités et fonctions des informations personnelles », *Ethique publique*, vol. 14, 2013, p. 3.

Néanmoins, certains auteurs estiment qu'il est vain de penser que les utilisateurs seront de ce fait mieux à même de comprendre sur quoi repose leur consentement¹¹⁶. En effet, à l'ère numérique, il n'est plus seulement question de données relatives à l'état civil (date de naissance, nom, prénom et situation matrimoniale) mais également d'empreintes digitales, de reconnaissance faciale, de géolocalisation, d'immatriculation de véhicules et de bien d'autres matières encore. La complexité des technologies au traitement des données, les enjeux économiques, la complexité de la logique sous-jacente sont autant de facteurs qui rendent la compréhension du sujet insaisissable.

Une illustration simple mais univoque peut provenir de recherche analysant les réactions des consommateurs face aux produits électroniques : de nombreux consommateurs ne savent pas à quoi servent la plupart des boutons de leur télécommande, certains ne sont dès lors jamais utilisés. La même démonstration peut être faite à partir des machines à laver dans la mesure où les consommateurs n'utilisent pas plus d'un ou deux programmes de lessive à côté de la multitude d'options à leur portée¹¹⁷.

Les utilisateurs acquièrent seulement une compréhension limitée des technologies qui les entourent même lorsqu'il s'agit des technologies qui leur sont les plus familières¹¹⁸. Ne serait-il donc pas optimiste de penser que les utilisateurs d'internet puissent comprendre comment la publicité ciblée ou encore la reconnaissance faciale marchent à travers leur ordinateur lorsqu'ils n'arrivent même pas à utiliser de manière efficiente les fonctions de leur télécommande ? De ce postulat empirique, nous pouvons conclure que les caractéristiques intrinsèques à la technologie constituent des barrières à obtenir un véritable consentement informé, et par conséquent valable.

1.1.2. Surcharge de demande et d'information

De nos jours, il n'est plus possible de naviguer sur la toile sans être submergé par des demandes d'acceptation de conditions générales de protection des données personnelles d'un site internet. La seconde problématique provient alors de cette surcharge de requêtes et d'informations adressées aux personnes concernées, effet pervers du principe de transparence¹¹⁹.

Le champ d'application de la protection des données personnelles n'a pas cessé de s'étendre à une multitude de situations. La définition de données personnelles elle-même a été élargie depuis le nouveau règlement, ce qui conforte d'autant plus nos propos. Les utilisateurs d'internet sont confrontés à présent à une série de requêtes qu'ils ne peuvent toutes considérées. La réaction typique observée chez la plupart des internautes est une fatigue, un

¹¹⁶ E. CAROLAN, « The continuing problems with online consent under the EU's emerging data protection principles », *Computer Law & Security Review*, vol. 32, 2016, p. 472.

¹¹⁷ E. CAROLAN, *op.cit.*, p. 469.

¹¹⁸ *Ibidem*.

¹¹⁹ B. SHERMER, B. CUSTERS, S. VAN DER HOF, « The crisis of consent : how stronger legal protection may lead to weaker consent in data protection », *Ethics and Information Technology*, vol.16, 2014, p. 177.

désintérêt pour ces demandes¹²⁰. Par un geste devenu automatique, les internautes balayent ces requêtes afin de pouvoir accéder au service pour lequel ils effectuent leurs recherches.

Une étude démontre que les citoyens devraient consacrer plus de 244 heures chaque année, à la lecture des politiques de confidentialité qui leur sont fournies sans garantie de les avoir comprises de façon intelligible¹²¹. En effet, les responsables de traitement des données respectent de manière scrupuleuse les obligations de transparence prescrites par les législations, dans la mesure où ils ne souhaitent pas faire l'objet d'accusation de comportements déloyaux. En conséquence, les politiques de confidentialité (« privacy notices ») sont la plupart du temps d'une longueur assommante et d'une complexité croissante. Il est donc compréhensible que la plupart des internautes détournent le regard, et cliquent de façon non réfléchie sur « accepter ».

1.1.3. Absence de choix significatif

Un autre élément à prendre en considération est que l'individu ne se comporte pas de manière rationnelle sur la toile. Replacé dans son contexte, l'utilisateur est avant tout mû par un désir d'accéder rapidement au service qu'il convoite, que ce soit l'ouverture d'un compte sur un réseau social, une recherche internet, un achat en ligne. Ces services, fournis gratuitement, ne sont pas à même de proposer une autre alternative aux internautes lorsque ces derniers refusent les conditions générales de leur site internet dans la mesure où leurs ressources économiques se constituent de ces données¹²².

En conséquence, une place à la négociation n'est pas possible pour les services en ligne, ce qui conduit directement à une situation de « à prendre ou à laisser » pour l'utilisateur du service¹²³. Ces actions sont alors essentiellement guidées par leur motivation première : l'accès au service et non pas prioritairement à la protection de leurs données privées. Au vu de leur comportement sur le net, les avantages procurés aux internautes sur le net seraient donc plus important que la protection de leurs données personnelles.

Cette critique propre au consentement n'est pourtant pas récente. François Rigaux soulignait, déjà en 1990, l'aspect illusoire du consentement dans son célèbre ouvrage sur la protection de la vie privée¹²⁴. Il analyse toutes sortes de situations différentes, notamment la recherche d'un emploi et la conclusion d'un contrat de consommation tels que le contrat d'assurance, la location ou l'ouverture d'un crédit. Il observe alors que, « pour satisfaire à ses besoins ou obtenir certaines prestations, l'individu ne saurait manquer de contracter et d'accepter les

¹²⁰ *Ibidem.*, p. 178.

¹²¹ *Ibidem.*

¹²² P. CHRISTIAN, C. FERAL-SCHUHL, « Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique », octobre 2015, p. 42.

¹²³ B. SHERMER, B. CUSTERS, S. VAN DER HOF, *op.cit.*, p. 177.

¹²⁴ F. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990, p. 602.

conditions qui lui sont faites »¹²⁵. Il poursuit ensuite en concluant que « le traitement de données personnelles n'est qu'un aspect du combat de l'individu contre le pouvoir »¹²⁶.

1.1.4. Privacy Paradox

Depuis quelques années, spécialement avec l'avènement des réseaux sociaux tels que Facebook, Twitter, Instagram, on observe une profonde contradiction entre l'inquiétude des internautes par rapport au respect de leur vie privée et le partage de leur informations personnelles sur la toile de la manière la plus désinvolte qui soit¹²⁷. Ce phénomène que l'on nomme le paradoxe de la vie privée (« Privacy paradox ») touche particulièrement la génération Y, génération numérique née entre le début des années 1980 et le milieu des années 1990¹²⁸. Un changement comportemental est analysé dans cette génération définie comme narcissique, là où l'image de soi est omniprésente, si pas prédominante. Il faut dès lors s'interroger sur la portée véritable du consentement dans de telles circonstances.

Pour faire face à cette nouvelle philosophie des réseaux sociaux, certains avancent le remède de l'éducation aux médias¹²⁹. Sensibiliser, dès le plus jeune âge, les enfants aux notions de respect de la vie privée et de protection des données personnelles, notamment en ce qui concerne leur droit à l'image, est nécessaire. Dans une société, de plus en plus numérisée, une prise de conscience et une meilleure compréhension de nos droits ainsi que des protections mises en place par les législations, améliorerait l'efficacité du consentement.

2) RELATIVISATION DU CARACTERE ILLUSOIRE DU CONSENTEMENT

La prétendue non pertinence du consentement doit être relativisée par les autres protections offertes par la législation européenne¹³⁰. Lorsqu'une personne consent à l'utilisation de ses données, il existe toute une série de garanties qui lui sont offertes : d'une part, le respect de principes fondamentaux imposés au responsable du traitement des données et, d'autre part, les droits conférés aux utilisateurs sur l'utilisation de leurs données.

2.1. Obligations contraignantes à charge des acteurs du traitement

Plusieurs grands principes, constituant des obligations contraignantes, sont à charge du responsable du traitement des données personnelles. Même lorsque le responsable de traitement a obtenu le consentement de la personne concernée, il n'est pas exonéré de ses

¹²⁵ *Ibidem*.

¹²⁶ *Ibidem*, p. 603.

¹²⁷ C. LAZARO, D. LE MÉTAYER, *op.cit.*, p. 767.

¹²⁸ Voy. en ce sens B. PRAS, « Entreprise et vie privée. Le « privacy paradox » et comment le dépasser ? », *Revue française de gestion*, vol. 224, 2012, pp. 87-94.

¹²⁹ B. CONTE, B. HENOCQUE, « Introduction. Opportunités et menaces juridiques liées aux technologies numériques », *Les cahiers du numérique*, vol. 10, Paris, 2014, pp. 9-15.

¹³⁰ Voy. en ce sens G. ZANFIR, « Forgetting about consent : Why the focus should be on « Suitable Safeguards » in data protection law », *Reloading Data protection*, London, Springer, 2014, p. 247 et suivant.

obligations, et ne peut pas se permettre d'agir de manière abusive avec les données personnelles récoltées. Comme le rappelle le G29, le consentement est « une condition de licéité et non une renonciation à l'application d'autres principes »¹³¹.

Il est utile de rappeler qu'en cas de violation d'un de ces principes, y compris les conditions propres au consentement, le responsable de traitement des données est susceptible d'encourir des sanctions administratives allant jusqu'à 20 000 000 d'euros, et s'il s'agit d'une entreprise, allant jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent¹³². Cette disposition constitue incontestablement une avancée par rapport à la précédente législation européenne en ce qu'elle donne effet au consentement et aux principes qui l'entourent de manière effective. Nous pouvons raisonnablement penser que cette disposition aura pour conséquence une sensibilisation des entreprises et autres responsables de traitement de données personnelles relative à la manière dont ils gèrent leur politique d'exploitation des données personnelles.

2.1.1. Principes de licéité, loyauté et transparence

En premier lieu, tout traitement de données personnelles doit être licite, loyal et transparent¹³³. Un traitement licite suppose le respect des règles émises par la législation européenne. En outre, la collecte de données personnelles doit reposer sur un des fondements juridiques listés à l'article 6 du règlement, dont le consentement fait partie. Pour ce qui est de la loyauté, le responsable du traitement se doit de traiter les données de la personne concernée sans chercher à la tromper, en ce compris par omission. Par conséquent, le principe de transparence découle inévitablement du principe de loyauté.

Comme dit précédemment, la problématique du consentement est étroitement liée au principe de transparence concernant les informations fournies aux personnes concernées. Dans ces lignes directrices à propos du principe de transparence¹³⁴, le Groupe de travail 29 envisage une nouvelle façon de présenter l'information aux personnes concernées. L'innovation consiste à intégrer des icônes ou outils infographiques normalisés, dans les politiques de confidentialité des entreprises afin que les utilisateurs appréhendent, de manière compréhensible et lisible, les informations concernant le traitement prévu de leurs données personnelles ainsi que leurs droits sur ce traitement¹³⁵. Ces symboles peuvent représenter par

¹³¹ Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011, p. 8.

¹³² Article 83, §5, a), du Règlement.

¹³³ Art. 5, § 1, a), du Règlement.

¹³⁴ Lignes directrices du Groupe de travail « Article 29 » sur le principe de transparence sous le Règlement 2016/679, adoptées le 12 décembre 2017.

¹³⁵ Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques préparé par le Groupe des politiques et de la recherche du Commissariat à la protection de la vie privée du Canada, 21 décembre 2017, disponible à l'adresse https://www.priv.gc.ca/media/1807/consent_201605_f.pdf

exemple la durée de conservation des données personnelles, l'existence d'un profilage, les finalités du traitement, ou encore le droit de retirer son consentement.

L'avantage est de susciter l'attention de la personne concernée de manière plus ludique et adaptée à l'environnement numérique plutôt que par un long texte rébarbatif. Cette idée reçoit toutefois des avis défavorables, soulignant son caractère trop simpliste au niveau de l'information. Pour ne pas engendrer une désinformation, il est essentiel que l'icône constitue un outil complémentaire au politique de confidentialité¹³⁶. Il faut également ne pas se méprendre en ce qui concerne le potentiel sous-entendu de l'icône normalisé, à savoir sa caractéristique à constituer une interprétation unique car celui-ci reste dépendant de sa pertinence graphique ainsi que d'éléments factuels comme l'âge de la personne concernée¹³⁷.

2.1.2. Principe de limitation des finalités

Lorsque la personne concernée consent au traitement de ses données personnelles, ces données ne peuvent être traitées que pour des finalités « déterminées, explicites et légitimes »¹³⁸. La finalité, correspondant au but poursuivi par le responsable de traitement, doit être obligatoirement fixée avant le début du traitement des données. Dans cette optique, un traitement ultérieur mais incompatible avec les finalités prescrites est interdit sauf exceptions prévues par la législation¹³⁹. On peut ainsi constater que le principe de finalités réduit de manière significative la liberté d'action du responsable du traitement des données personnelles.

2.1.3. Principe de minimisation

Le nouveau règlement précise qu'à présent, seules les données nécessaires pour atteindre la finalité déterminée peuvent faire l'objet d'un traitement, c'est-à-dire des données adéquates et pertinentes¹⁴⁰. Cette nouvelle disposition sur la collecte des données garantit aux personnes concernées un contrôle effectif sur leurs données¹⁴¹.

2.1.4. Principe d'exactitude

Le consentement de la personne concernée ne peut porter que sur des données qui sont exactes, et si nécessaire, tenues à jour¹⁴². Le responsable du traitement devra prendre toutes

¹³⁶ E. KOSTA, *op.cit.*, p. 214.

¹³⁷ Avis 16/2011 du Groupe de travail « Article 29 » sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne, adopté le 8 décembre 2011.

¹³⁸ Article 5, § 1, b) du Règlement.

¹³⁹ Article 5, § 1, b) du Règlement prévoit comme exception à un traitement ultérieur mais à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales.

¹⁴⁰ Art. 5, § 1, c), du Règlement.

¹⁴¹ A. BENSOUSSAN, *op.cit.*, p. 88.

¹⁴² Art. 5, § 1, d), du Règlement.

les mesures raisonnables afin d'effacer ou de corriger des données inexactes, fausses ou devenues obsolètes, sans tarder.

2.1.5. Principe de conservation

Le consentement de la personne concernée n'est pas donné *ad vitam aeternam*. Lorsque l'utilisateur consent à l'utilisation de ces données, cela doit être pour une durée de conservation qui correspond à celle nécessaire pour accomplir les finalités pour lesquelles les données sont traitées¹⁴³. Le considérant 39 insiste pour que cette durée de conservation soit limitée au strict minimum. Lorsque cette durée est dépassée, les données doivent être automatiquement supprimées.

2.1.6. Principes d'intégrité et de confidentialité

Outre les différents principes énoncés précédemment, des mesures de sécurités appropriées doivent être mises en œuvre par le responsable du traitement des données, et son sous-traitant, tout au long du traitement des données¹⁴⁴.

Ces mesures de sécurité doivent assurer la confidentialité des données face aux différents risques potentiels, tels que la perte, la destruction, la divulgation, l'accès non autorisé aux données¹⁴⁵. Le règlement va jusqu'à proposer des pistes de mesures de sécurité à prendre telles que la pseudonymisation des données personnelles afin qu'elles deviennent non identifiables¹⁴⁶. Ces mesures amoindrissent les inquiétudes des individus concernant l'exploitation des données auxquelles elles ont consenti. Malheureusement, la pseudonymisation comporte des limites. Sa prétendue vertu de désidentification des données est souvent remise en cause par de nombreuses recherches¹⁴⁷. On relève qu'à l'ère du Big Data, les données ne peuvent jamais être complètement désidentifiées car il existe des informations secondaires de la personne concernée permettant, lorsqu'on les combine avec les informations pseudonymisées, de l'identifier¹⁴⁸.

2.2. Autres droits conférés aux personnes concernées

¹⁴³ Art. 5, § 1, e), du Règlement.

¹⁴⁴ Art. 5, § 1, f), du Règlement.

¹⁴⁵ Considérant 28 du Règlement.

¹⁴⁶ L'article 4, § 5, du Règlement définit la pseudonymisation comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

¹⁴⁷ Voy. l'avis 05/2014 sur les techniques d'anonymisation du Groupe de travail « article 29 » sur la protection des données, adopté le 10 avril 2014.

¹⁴⁸ Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques préparé par le Groupe des politiques et de la recherche du Commissariat à la protection de la vie privée du Canada, 21 décembre 2017, disponible à l'adresse https://www.priv.gc.ca/media/1807/consent_201605_f.pdf

L'individu est placé au cœur du nouveau dispositif législatif européen. Pour cette raison, le règlement s'est penché sur le consentement comme moyen de renforcer la maîtrise du citoyen sur l'utilisation de ses données. Toutefois, le consentement n'est pas l'unique procédé, le règlement énonce plusieurs autres possibilités. Le consentement comme appareil émancipateur de l'individu ne peut s'analyser pleinement qu'à condition d'envisager les autres droits mis à la disposition de l'individu. Certains auteurs estiment d'ailleurs qu'il est préférable de ne mettre l'accent que sur les garanties, plutôt que sur le consentement¹⁴⁹.

Certains droits constituent le corollaire direct des obligations pesant sur le responsable du traitement des données. On cite le droit à l'information du traitement entrepris sur nos données, conséquence du principe de transparence, ainsi que le droit à la rectification des données inexactes, obsolètes, déduit du principe d'exactitude¹⁵⁰.

La personne concernée dispose également du droit à l'accès à ses données¹⁵¹. Ce droit permet l'enclenchement d'autres droits, en ce qu'il permet à la personne concernée, par la connaissance du traitement de ces données, la vérification de la licéité du traitement et, si nécessaire, d'exercer ses droits¹⁵².

Comme dit précédemment, suite à l'arrêt *Google Spain*¹⁵³ de la Cour de justice de l'Union, le droit à l'oubli numérique est consacré de manière explicite dans l'ordre juridique européen. Le règlement prévoit six cas dans lesquels une personne concernée peut exiger un droit à l'effacement de ses données dont le retrait du consentement¹⁵⁴.

3) REFLEXION AUTOUR DU CONSENTEMENT

3.1. Innovations technologiques infinies et solutions juridiques limitées

Après une analyse approfondie de la notion de consentement en matière de protection des données personnelles portant tant sur les raisons qui ont amené le législateur européen à redéfinir son concept que sur les critiques cognitives et juridiques avancées au consentement, notre travail se penche sur quelques questions de réflexions et de synthèse.

Au regard de ce qui précède, il est évident qu'en matière de traitement automatisé des données personnelles, la personne concernée est considérée comme une "partie faible" par le règlement au vu de sa position et de son manque de compréhension du sujet. Par conséquent,

¹⁴⁹ G. ZANFIR, *op.cit.*, pp. 237-257.

¹⁵⁰ Le droit à l'information est consacré par l'article 12 du Règlement et le droit à la rectification par l'article 16.

¹⁵¹ Art. 15 du Règlement.

¹⁵² M. Bourgeois, *op.cit.*, p. 209.

¹⁵³ C.J.U.E., arrêt *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, 13 mai 2014, aff. C-131/12.

¹⁵⁴ Article 17, 1 du Règlement.

elle jouit de droits spécifiques ainsi que de protections particulières lorsqu'elle consent au traitement de ses données personnelles. Un rapprochement juridique peut être établi entre les différentes législations protégeant les parties faibles dans un contrat donné et les mécanismes de protection mis en place dans la réglementation de traitement des données personnelles.

Nous pensons tout d'abord au droit de la consommation dans la mesure où le consommateur bénéficie d'une protection similaire. Des règles de fond comme de forme doivent être respectées afin de pouvoir conclure un contrat¹⁵⁵. Des informations préalables et spécifiques doivent être fournies pour garantir un consentement éclairé de la part du consommateur, notamment des informations relatives aux caractéristiques des biens et services, aux prix de vente, aux délais de livraison¹⁵⁶. La communication de ces informations doit se faire de manière claire et compréhensible. Ces obligations poursuivent la même logique que le principe de consentement informé et spécifique dans le domaine de la protection des données personnelles. Le consommateur dispose également d'un droit de rétractation¹⁵⁷, qui peut s'apparenter au droit de retirer son consentement à l'utilisation de ses données personnelles pour la personne concernée. En outre, la pratique des codes de conduite se développe de plus en plus en matière de protection des données, initiative déjà entreprise largement en droit de la consommation¹⁵⁸.

Il n'est pas surprenant de constater que la doctrine émet des critiques aux protections édifiées en droit de la consommation dans le chef du consommateur qui trouvent un écho dans le consentement à l'utilisation des données personnelles. On souligne « l'effet de saturation » que le formalisme informatif engendre, aboutissant à une démarche relevant de la mauvaise foi contractuelle pour certains¹⁵⁹. En droit de la consommation, le législateur est intervenu pour améliorer l'information du consommateur en établissant des signes d'identification : labels et certifications, marquage CE¹⁶⁰. On observe en parallèle que certains pays, comme la France, le Royaume-Uni ou encore les Etats-Unis, mettent en place peu à peu des sceaux électroniques ou labels garantissant aux internautes la conformité d'un site web aux lois de protection des données personnels¹⁶¹. Ne faudrait-il pas envisager également cette solution à l'échelon européen ?

Nous pouvons également établir un parallélisme avec le droit du travail et l'ordre public social qu'il établit. En effet, on y observe pareille démarche juridique à l'encontre du travailleur salarié, notamment à travers l'obligation d'information par écrit des conditions de travail mais aussi l'obligation de sécurité à garantir par l'employeur. En outre, lorsqu'il s'agit du respect de la vie privée du travailleur sur son lieu de travail, des restrictions sont permises

¹⁵⁵ C. BIQUET-MATHIEU, « Les contrats du consommateur – Rapport de droit belge », in *Le consommateur*, Bruxelles, Bruylant, 2010, p. 45.

¹⁵⁶ J. CALAIS-AULOY, H. TEMPLE, *Droit de la consommation*, Paris, Dalloz, 2010, p. 53.

¹⁵⁷ S. PIEDELIEVRE, *Droit de la consommation*, Paris, Economica, 2008, p. 38.

¹⁵⁸ *Ibidem*, p. 25.

¹⁵⁹ *Ibidem*, p. 61.

¹⁶⁰ J. CALAIS-AULOY, H. TEMPLE, *op. cit.*, Paris, Dalloz, 2010, p. 72.

¹⁶¹ A. BELLEIL, *op. cit.*, p. 114.

pour autant que des conditions de finalité, de proportionnalité et de légalité soient respectées¹⁶².

Suite à ces constatations, on arrive à la conclusion que si les innovations technologiques se développent de manière exponentielle, les réponses juridiques classiques à apporter en matière de protection des données à caractère personnel sont limitées quant à elles par une logique similaire sous-jacente aux différentes législations concernant les rapports avec une partie faible.

Dans ces circonstances, l'intelligence artificielle pourrait renforcer l'arsenal juridique et constituer une aide précieuse pour répondre aux défis posés. C'est cette réflexion qui retient notre attention au point suivant.

3.2. L'intelligence artificielle comme complément à l'arsenal juridique ?

Nous partageons l'idée que, *the answer to the machine is in the machine*¹⁶³. A l'ère numérique, l'innovation potentielle que l'on pourrait apporter au concept de consentement serait d'utiliser l'intelligence artificielle comme outil au service de la protection des données à caractère personnel. L'intelligence artificielle est définie par l'un de ses créateurs, Marvin Lee Minsky comme « la construction de programmes informatiques qui s'adonnent à des tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des êtres humains car elles demandent des processus mentaux de haut niveau tels que : l'apprentissage perceptuel, l'organisation de la mémoire et le raisonnement critique »¹⁶⁴.

Alors que certains auteurs préconisent un abandon radical de la forme consensuelle comme fondement du traitement des données à caractère personnel, d'autres proposent des solutions, ou du moins des améliorations, à apporter à son concept. Selon nous, il ne faudrait pas faire peser la charge du consentement exclusivement sur les individus, mais plutôt élaborer une politique qui permette de faciliter et d'assister la manière de donner un consentement, un véritable consentement.

L'idée a germé aux Etats-Unis. Dans son rapport *Big Data and Privacy : A technological Perspective*, la maison blanche propose pour l'ensemble des services émis sur internet un mécanisme de gestion des préférences concernant la protection des données à caractère personnel¹⁶⁵. La personne concernée doit transmettre à un intermédiaire un ensemble standard

¹⁶² J. CLESSE, F. KEFER, *Manuel de droit du travail*, Bruxelles, Larcier, 2014, p. 365.

¹⁶³ « The answer to the machine is in the machine » est l'intitulé d'un article écrit par Charles Clarke, publié en 2005.

¹⁶⁴ M. SOULEZ, « Questions juridiques au sujet de l'intelligence artificielle », *Les annales des mines*, 2018, p. 81.

¹⁶⁵ Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques préparé par le Groupe des politiques et de la recherche du Commissariat à la protection de la vie privée du Canada, 21 décembre 2017, p. 15, disponible à l'adresse https://www.priv.gc.ca/media/1807/consent_201605_f.pdf

de préférences relatif aux modalités de protection de ses données personnelles : ce qu'elle accepte, ce qu'elle ne permet pas¹⁶⁶. Ensuite, c'est à l'intermédiaire d'approuver les différentes politiques de confidentialités des services et applications proposées sur internet par rapport au profil de la personne concernée¹⁶⁷. On pourrait même aller plus loin dans le raisonnement et imaginer que lorsque le service ou l'application ne correspond pas aux préférences de l'utilisateur, l'intermédiaire lui propose un service similaire respectant une politique de confidentialité conforme à son profil.

L'avantage est indéniable dans la mesure où la personne concernée ne doit plus systématiquement lire toutes les politiques de confidentialité, ni par conséquent les comprendre dans leur totalité¹⁶⁸. Cette solution a également le mérite à nos yeux de ne pas déresponsabiliser le citoyen vis-à-vis de la protection de ses données personnelles mais de le conscientiser dès le départ, lorsqu'il doit établir ses choix de préférence, aux conséquences d'un consentement. De façon intéressante, la perte d'autonomie, souvent soulignée par les sceptiques de l'intelligence artificielle, est ici contredite¹⁶⁹. Toutefois, peut-on toujours parler de véritable consentement ? Ne sommes-nous pas face à une mutation de la notion de consentement dans l'environnement électronique ?

¹⁶⁶ *Ibidem*.

¹⁶⁷ *Ibidem*.

¹⁶⁸ *Ibidem*.

¹⁶⁹ H. JACQUEMIN, A. DE STREEL, *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, p. 7.

CONCLUSION

A l'aube du 21ème siècle et de son univers numérique, il est opportun de s'interroger sur l'étendue de vie privée à laquelle on peut toujours prétendre. Alors que l'Union européenne sacralise la notion de consentement dans sa nouvelle réglementation de protection des données personnelles, d'autres auteurs démystifient foncièrement la capacité d'autonomisation de l'individu. Ce débat ne relève pas seulement du juridique en ce qu'il soulève également de nombreuses questions sur le plan éthique, économique et politique.

D'une part, les détracteurs du consentement blâment l'absence irrémédiable de maîtrise intellectuelle des personnes concernées à l'égard du sujet du traitement de leurs données. Ils accusent le paradoxe auquel les jeunes se livrent, un désir d'intimité contredit par un étalage grandissant de leur vie privée sur les réseaux sociaux. Face à cette tendance, ne serait-il pas plus pertinent d'éduquer les prochaines générations aux risques et abus de l'ère numérique sur leur vie privée ? Pour ces auteurs, l'ère numérique remet en cause le caractère intemporel du consentement, en ce qu'il ne peut produire pleinement tous ses effets dans cet environnement.

D'autre part, lorsqu'on retrace la genèse législative en matière de protection des données personnelles, nous constatons une clarification importante de la mise en œuvre du consentement. Ces clarifications découlent d'une prise de conscience du fait que le consentement connaît des limites dans l'environnement numérique, limites démontrées par des études économiques et psychologiques. Ces modifications nous parviennent non seulement de la nouvelle réforme, mais également de la jurisprudence de la Cour de Justice et de l'organe indépendant que constitue le Groupe 29. Par leurs interventions, le système de l'opt-out est définitivement rejeté de la pratique, la reconnaissance d'une protection particulière pour les personnes vulnérables est reconnue, les devoirs du responsable du traitement des données à caractère personnel sont aggravés. En outre, le droit à l'oubli numérique, basé sur un retrait du consentement est formellement consacré. Des lignes directrices sur l'information à fournir aux personnes concernées sont édictées.

Certains soulignent le caractère illusoire du consentement à l'aune du développement numérique mais il serait plutôt illusoire de penser à un modèle juridique dépourvu de tout consentement, ce dernier constituant un des principes fondateur du droit ? Certes, la législation énonce d'autres fondements de licéité du traitement de données personnelles et il est primordial de les utiliser le cas échéant.

Nous n'avons épuisé les ressources en matière d'innovation dans le domaine juridique et partageons l'idée que l'intelligence artificielle est un outil en devenir qui sera précieux pour assister à la mise en œuvre d'un consentement éclairé dans nos sociétés évoluant vers de nouveaux modèles de transactions, d'échanges, et de partages numérisés.

Nous terminerons notre réflexion avec les propos du professeur Jean Foyer : « Une course permanente met aux prises le droit et les faits. C'est pourquoi le droit est, par nécessité, un art d'imagination. Jusqu'à la fin des temps, la tâche des juristes sera l'application de l'encouragement donné par le poète : « Sur des penses nouveaux, faisons des vers antiques »¹⁷⁰.

¹⁷⁰ D. BOURCIER, P. HASSETT, C. ROQUILLY, *Droit et intelligence artificielle : une révolution de la connaissance juridique*, Paris, Romillat, 2000, p. 125.

BIBLIOGRAPHIE

1) Documents législatifs :

Déclaration universelle des droits de l'homme, adoptée le 10 décembre 1948 à Paris par l'Assemblée générale des Nations Unies.

Convention européenne des droits de l'Homme et des libertés fondamentales du Conseil de l'Europe, adoptée le 4 novembre 1950 à Rome, article 8.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe adoptée le 28 janvier 1981 à Strasbourg.

Charte des droits fondamentaux de l'Union européenne, adoptée le 7 décembre 2000 à Nice, article 8.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des ces données.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

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

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 (règlement général sur la protection des données), COM (2012) 11 final, 25 janvier 2012.

Lignes directrices du Groupe de travail « Article 29 » sur le principe de transparence sous le Règlement 2016/679, adoptées le 12 décembre 2017.

Avis 05/2014 du Groupe de travail « article 29 » sur les techniques d'anonymisation, adopté le 10 avril 2014.

Avis 15/2011 du Groupe de travail « Article 29 » sur la définition du consentement, adopté le 13 juillet 2011.

Avis 16/2011 du Groupe de travail « Article 29 » sur le code de bonnes pratiques de l'AEEP et de l'IAB en matière de publicité comportementale en ligne, adopté le 8 décembre 2011.

Avis 5/2004 du Groupe de travail « Article 29 » portant sur la communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE, adopté le 27 février 2004.

2) Jurisprudence :

Cour européenne des droits de l'Homme :

Cour eur. D.H., *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n° 30562/04 et 30566/04.

Cour eur. D.H., *Z c. Finlande*, 25 février 1997, req. n°22009/93.

Cour eur. D.H., *Malone c. Royaume-Uni*, 2 août 1984, req. n°8691/79.

Cour eur. D.H., *Klass et autres c. Allemagne*, 6 septembre 1978, req. n°5029/71.

Cour de Justice de l'Union européenne :

C.J.U.E., arrêt *Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, 13 mai 2014, aff. C-131/12.

C.J.U.E., arrêt *Rechnungshof*, 20 mai 2003, aff. jointes C-165/01, C-138/01 et C-139/01.

3) Doctrine :

Ouvrages :

BELLEIL, A., *E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'internet*, Paris, Dunod, 2001, 202 p.

BENSOUSSAN, A., *La protection des données personnelles de A à Z*, Bruxelles, Bruylant, 2017, 252 p.

BENSOUSSAN, A., *Règlement européen sur la protection des données*, Bruxelles, Bruylant, 2017, 759 p.

BOURCIER, D., DE FILIPPI, P., *Open data & Big Data : nouveaux défis pour la vie privée*, Paris, Mare&Martin, 2016, 269 p.

BOURCIER, D., HASSETT, P., ROQUILLY, C., *Droit et intelligence artificielle : une révolution de la connaissance juridique*, Paris, Romillat, 2000, 303 p.

- BOURGEOIS, M., *Droit de la donnée : principes théoriques et approche pratique*, Paris, LexisNexis, 2017, 543 p.
- BURGORGUE-LARSEN, L., *La Convention européenne des droits de l'homme*, Paris, Lextenso Éditions, 2012, 302 p.
- CALAIS-AULOY, J., TEMPLE, H., *Droit de la consommation*, Paris, Dalloz, 2010, 721 p.
- CARNEROLI, S., *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli*, Bruxelles, Larcier, 2016, 135 p.
- CASTETS-RENARD, C., *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015., 187 p.
- CLESSE, J., KEFER, F., *Manuel de droit du travail*, Bruxelles, Larcier, 2014, 544 p.
- DEHOUSSE, F., VERBIEST, T., ZGAJEWSKI, T., *Introduction au droit de la société de l'information*, Bruxelles, Larcier, 200, pp. 277-309.
- DOCQUIR, B., *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, 175 p.
- DOCQUIR, B., *Le droit de la vie privée*, Bruxelles, Larcier, 2008, 320 p.
- ERGEC, R., *Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2014, 1250 p.
- FAUCHOUX, V., DEPREZ, P., DUMONT, F., BRUGUIERE, J-M., *Le droit de l'internet*, Paris, Lexis Nexis, 2017, 431 p.
- GAUTHIER, C., PLATON, S., SZYMCAK, D., *Droit européen des droits de l'Homme*, Paris, Dalloz, 2017, 518 p.
- JACQUEMIN, H., DE STREEL, A., *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, 481 p.
- KOSTA, E., *Consent in European data protection law*, Leiden, Martinus Nijhoff, 2013, 441 pp.
- LELEU, Y., *Droit des personnes et des familles*, Bruxelles, Larcier, 2016, 904 p.
- PICOD, F., VAN DROOGHENBROECK, S., *Charte des droits fondamentaux de l'Union européenne*, Bruxelles, Bruylant, 2018, 1259 p.
- PIEDELIEVRE, S., *Droit de la consommation*, Paris, Economica, 2008, 665 p.
- PIERRE-BEAUSSE, C., *La protection des données personnelles*, Luxembourg, Editions Promoculture, 2004, 378 p.
- RIDEAU, J., *Les droits fondamentaux dans l'Union européenne*, Bruxelles, Bruylant, 2009, 489 p.

RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990, 849 p.

THIRION, N., *Théorie du droit : droit, pouvoir, savoir*, Bruxelles, Larcier, 2011, 302 p.

Articles :

BIQUET-MATHIEU, C., « Les contrats du consommateur – Rapport de droit belge », in *Le consommateur*, Bruxelles, Bruylant, 2010, pp. 37-54.

CAROLAN, E., « The continuing problems with online consent under the EU's emerging data protection principles », *Computer Law & Security Review*, vol. 32, 2016, pp. 462-473.

CONTE, B., HENOCQUE, B., « Introduction. Opportunités et menaces juridiques liées aux technologies numériques », *Les cahiers du numérique*, vol. 10, Paris, 2014, pp. 9-15.

DE TERWANGNE, C., « Chapitre 3 - Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique » in A. GROSJEAN, *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Éditions Larcier, 2015, pp. 245-275.

EYNARD, J., « L'éthique à l'épreuve des nouvelles particularités et fonctions des informations personnelles », *Ethique publique*, vol. 14, 2013, pp. 1-10.

FRAYSSINET, F., « La protection des données personnelles est-elle assurée sur l'Internet ? » in G. CHATILLON, *Le droit international de l'internet*, Bruxelles, Bruylant, 2003, pp. 435-444.

GEFFRAY, É., « Comment assurer l'effectivité de la protection des droits à l'ère post-Snowden ? » in A. GROSJEAN, *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Éditions Larcier, 2015, pp.19-24.

LAZARO, C., LE MÉTAYER, D., « Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet », *Revue juridique Thémis de l'Université de Montréal*, vol. 48, 2014, pp. 765-815.

LE COADIC, R., « Autonomie, illusion ou projet de société ? », *Cahier internationaux de sociologie*, vol. 121, 2006, pp. 317-340.

PRAS, B., « Entreprise et vie privée. Le « privacy paradox » et comment le dépasser ? », *Revue française de gestion*, vol. 224, 2012, pp. 87-94.

RAGOUCY, C., « Le panoptique et 1984 : confrontation de deux figures politiques d'asservissement », *Psychanalyse*, vol. 18, 2010, pp. 45-58.

RIGAUX, F., « La liberté de la vie privé », *R.D.I.D.C.*, 1991, Vol. 43, pp. 539-563.

SOULEZ, M., « Questions juridiques au sujet de l'intelligence artificielle », *Les annales des mines*, 2018, pp. 81-85.

SKOUMA, G., LEONARD, L., « Chapitre 1 - Les grands changements liés à la réglementation sur la protection des données personnelles et ses implications pratiques pour les entreprises et les professionnels » in A. GROSJEAN, *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Éditions Larcier, 2015, pp. 403-408.

SHERMER, B., CUSTERS, B., VAN DER HOF, S., « The crisis of consent : how stronger legal protection may lead to weaker consent in data protection », *Ethics and Information Technology*, vol.16, 2014, pp. 171-182.

VETOIS, J., « L'Europe redéfinit la protection des données personnelles », *Terminal*, 2013, pp. 3-6.

ZANFIR, G., « Forgetting about consent : Why the focus should be on « Suitable Safeguards » in data protection law », in *Reloading Data protection*, London, Springer, 2014, pp. 237-257.

4) Autres :

COMMISSION EUROPEENNE, Communiqué de presse du 4 novembre 2010 : « Une approche globale de la protection des données à caractère personnel dans l'Union européenne ».

COMMISSION EUROPEENNE, Communiqué de presse du 21 décembre 2015 : « Questions réponses : la réforme de la protection des données ».

GROUPE DES POLITIQUES ET DE LA RECHERCHE DU COMMISSARIAT A LA PROTECTION DE LA VIE PRIVE DU CANADA, Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électronique, 21 décembre 2017, disponible à l'adresse : https://www.priv.gc.ca/media/1807/consent_201605_f.pdf (dernière fois consulté le 27 avril 2018)

CHRISTIAN, P., FERAL-SCHUHL, C., « Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique », octobre 2015, disponible à l'adresse <http://www.assemblee-nationale.fr/14/rapports/r3119.asp> (dernière fois consulté le 27 avril 2018)

WALTER, J., « Modernisation de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) », disponible à l'adresse http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/auditionlibe_/auditionlibe_en.pdf (dernière fois consulté le 27 avril 2018)