TABLE RONDE DU 20 FEVRIER 2014

« QUELS DROITS POUR LES RÉSEAUX SOCIAUX ? »

RESEAUX SOCIAUX ET PROTECTION DES DONNEES PERSONNELLES

PRESENTÉ PAR

M^LLE CLÉMENCE DANI, M^LLE LAURA GARINO, M. GIANNI GIORDANO, M^LLE ELISA SICARD

RAPPORT RÉALISÉ SOUS LA DIRECTION DE M. LE PROFESSEUR JEAN FRAYSSINET ET M. LE PROFESSEUR PHILIPPE MOURON

MASTER II « DROIT DES MEDIAS ET DES TELECOMMUNICATIONS »

FACULTE DE DROIT ET DE SCIENCE POLITIQUE

UNIVERSITE D'AIX-MARSEILLE

ANNEE UNIVERSITAIRE 2013-2014

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE AIX-MARSEILLE

Aix*Marseille université

IREDIC

TABLE DES ABRÉVIATIONS

CEDH	Convention européenne des droits de l'homme
CNIL	Commission nationale de l'informatique et des libertés
CD ROM	Compact Disc Read Only Memory
DDHC	Déclaration des droits de l'Homme et du citoyen
EPIC	Electronic Privacy Information Center
G 29	Groupe de travail Article 29
IP	Internet Protocol
LCEN	Loi pour la confiance dans l'économie numérique
PDF	Portable Document Format
PIVP	Protection intégrée de la vie privée
SADP	Système automatisé de traitement des données personnelles
SMS	Short Message Service
TGI	Tribunal de grande instance
UE	Union européenne

SOMMAIRE

INTRODUCTION

Le 3 janvier 2014, la formation restreinte de la CNIL a prononcé une sanction pécuniaire de 150 000 euros à l'encontre de la société Google Inc pour avoir refusé de rendre conforme au droit français sa politique de confidentialité des données. En effet, les règles de confidentialité mises en œuvre par Google depuis le 1e mars 2012 n'étaient pas conformes à la loi « informatique et libertés». La société portait atteinte à la vie privée des internautes en croisant leurs données afin de leur proposer des publicités susceptibles de les intéresser. De plus, les utilisateurs n'étaient pas assez informés des conditions et finalités de traitement de leurs données personnelles. Cette sanction fut confirmée par le Conseil d'Etat le 7 février 2014. Les réseaux sociaux pourraient se voir infliger des sanctions similaires s'ils continuent à violer les droits de l'individu.

La loi « informatique et libertés » du 6 janvier 1978 a consacré une définition des données à caractère personnel. Elle les considère comme « toute donnée permettant d'identifier directement ou indirectement une personne physique. »[1] Celles qui permettent une identification directe et personnelle sont par exemple le nom, prénom ou encore la photo d'une personne. En revanche, sont des données personnelles indirectes, des numéros d'identification comme le numéro de sécurité sociale ou le numéro d'employé. La nécessité d'établir un cadre juridique de la protection des données personnelles est apparue dans les années 1970, avec le projet du gouvernement connu sous le nom de SAFARI. Puis la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000 a consacré le droit de la protection des données personnelles.

On parle d'une « universalisation des données » car tous les pays membres de l'Union Européenne sont dotés d'une certaine protection des données personnelles, bien qu'elle soit inégale selon les pays. C'est pourquoi, il existe un besoin d'harmonisation des règles quant à la protection des données personnelles. Le plus important, reste le critère tenant au traitement de ces données personnelles. En effet, pour bénéficier d'une protection, il faut que ces données fassent l'objet d'un traitement, pour les réseaux sociaux cela se fait par un « système automatisé ». Ce traitement doit être encadré juridiquement afin de limiter les risques d'exploitation et de détournement des données personnelles traitées. C'est pourquoi la CNIL a été instituée par la loi de 1978, afin de proposer une régulation du traitement des données personnelles via des SADP. La législation française a connu une évolution, sous l'influence européenne avec la loi du 6 août 2004 qui transpose la directive du 24 octobre 1995. Cette dernière est venue modifier la loi du 6 janvier 1978 et a notamment renforcer le rôle de la CNIL en lui accordant notamment, des pouvoirs de sanction, de contrôle a posteriori et d'appréciation. L'autorité est donc investie d'une mission de régulation, de contrôle, de protection des données personnelles des individus.[2]

Le G29, groupe des « CNIL » européennes institué par la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci est un organe consultatif européen indépendant. Il rassemble les représentants de chaque autorité indépendante de protection des données nationales. L'organisation et les missions de ce groupe de travail sont définies par les articles 29 et 30 de la directive de 1995. Il a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays hors Union Européenne et de conseiller la Commission européenne sur tout projet ayant une incidence sur la protection des données et les libertés des personnes. Le G29 se réunit à Bruxelles en séance plénière tous les deux mois environ. Il a adopté, lors de sa séance plénière des 22 et 23 mars 2012,

[1]Article 2§2 de la loi « Informatique et Libertés » du 6 juin 1978, <www.legifrance.gouv.fr>
[2]Article 11 « Loi Informatique et Libertés » du 6 janvier 1978

un avis sur les propositions de réforme présentées par la Commission Européenne le 25 janvier 2012. Ce « projet de règlement européen sur la protection des données à caractère personnel » a vocation à se substituer à la directive du 24 octobre 1995 afin de donner un cadre européen actuel de la protection des données à caractère personnel.

Plus précisément, Twitter et Facebook sont l'évolution du « contrat de confiance ».[3] Ce « contrat de confiance » est un argument solide afin de prévenir le mécontentement des clients et d'éviter que les enseignes et entreprises aient une mauvaise réputation. Les sociétés utilisent de plus en plus les réseaux sociaux pour promouvoir leurs marques, produits et services. Il en va de même pour ce qui est de l'utilisation privée de ces réseaux. Ce qui est primordial pour les internautes, c'est une relation de confiance vis-à-vis des réseaux sociaux qu'ils utilisent pour communiquer. La protection de données personnelles est même devenu un argument marketing, car elle va « rassurer » l'utilisateur afin qu'il puisse utiliser le service pleinement et en toute sérénité. L'intérêt de l'entreprise, tout comme celui des réseaux sociaux, réside dans leur nombre de « clients ». Les réseaux sociaux recherchent toujours plus de bénéfices, donc, plus ils ont de clients, plus leur rentabilité sera accrue. Ainsi cette relation de confiance, concilie à la fois les intérêts des réseaux sociaux avec ceux des utilisateurs. La transparence des réseaux sociaux devra être de rigueur. Aux Etats Unis, les données personnelles sont un produit marketing, elles ont une véritable valeur marchande. Leur commercialisation par les entreprises dans le but de gagner de l'argent est fréquente. Il appartient a chaque entreprise américaine de se réguler, de fixer sa propre règlementation en matière de protection des données personnelles. C'est pourquoi elles ont mis en place un très faible niveau de protection afin de dépenser le moins possible d'argent. Cela pose de nombreux problèmes car les utilisateurs perdent confiance en ces entreprises. Celles qui en ont conscience mettent en œuvre des moyens visant à rassurer leurs clients, les protéger. C'est une démarche de responsabilisation, « d'accountability ». Les entreprises considèrent alors que les données relatives à leurs clients sont des biens qui leur appartiennent.

En Europe, la directive de 1995 essaie de concilier la protection des droits de la personnalité et des libertés fondamentales avec la libre circulation des données personnelles. Cependant, la loi de programmation militaire du 18 décembre 2013 accroît la surveillance des internautes. Il semble donc qu'un rapprochement avec le système américain s'opère concernant la lutte contre le terrorisme, au détriment des droits de la personne. Ainsi, pour lutter contre le terrorisme il est possible de porter atteinte à la protection des données personnelles car il s'agit d'une préoccupation nationale importante de sécurité publique. Pour 57 % des internautes, cela justifie que l'on atteigne leurs droits et libertés. Il y a en Europe, comme aux Etats-Unis, une tendance de plus en plus forte à la collecte et à la commercialisation des données personnelles. Les réseaux sociaux les revendent à des annonceurs afin qu'ils ciblent davantage les besoins des consommateurs dans le but de leur soumettre une publicité plus appropriée.

Le premier enjeu réside donc dans nos libertés personnelles et individuelles. Ensuite, des intérêts économiques entrent en jeu comme la vente des informations sur les internautes, le marché des données personnelles. L'économie se nourrit de ce marketing des données personnelles commercialisées. De plus, les utilisateurs laissent de plus en plus, de façon inconsciente, des informations sur internet. Or, il est dit dans la loi que l'informatique, donc le traitement des données à caractère personnel, ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques. [4]

Lorsqu'on parle de libertés individuelles on pense aux droits de la personnalité. Tout d'abord, l'article 9 de la DDHC énonce que « chacun a le droit au respect de sa vie privée » mais aucun texte ne défini vraiment ce qu'est la vie privée. C'est le juge qui, au cas par cas, dit s'il y a eu ou non violation de la vie privée. On va retrouver cette notion de droits de la personnalité dans l'article 9

[3]BIANCHI F., « Darty : Twitter et les réseaux sociaux c'est l'évolution du contrat de confiance »
[4]Article 1er, loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

du Code civil, ainsi que dans la Charte des droits fondamentaux et dans la Convention européenne des droits de l'Homme. La vie privée regroupe donc tout ce qui se déroule, dans le domicile, les relations familiales, la santé, les rencontres, les déplacements, les convictions politiques, religieuses, syndicales... Le contenu d'un panier électronique sur un site internet relève par exemple de la vie privée. Les habitudes de vie, de consommation, les comportements, relèvent également de la vie privée. C'est une notion vaste qui évolue car ce qui aurait pu être considéré comme une atteinte à la vie privée il y a quelques années, ne l'est plus forcément aujourd'hui. Le droit à la protection des données personnelles protège des données qui relèvent de la vie privée mais aussi d'autres qui n'en relèvent pas. De plus en plus de problèmes proviennent d'informations personnelles, mais qui ne relèvent pas au sens stricto sensu de notre vie privée. L'article premier du projet de règlement européen, tient compte des évolutions et du fait que la notion de vie privée vient régulièrement supplanter et modifier la notion de protection de données personnelles. Ainsi, il ne repend plus la notion de vie privée et dit que « le présent règlement protège les libertés et droits fondamentaux des personnes physiques et en particulier leurs droits à la protection des données à caractère personnel ». Le droit de la protection des données personnelles est donc une partie des droits et libertés fondamentaux.

Bien que le droit Français et en Européen encadre le traitement des données à caractère personnel, la protection de ces données représente aujourd'hui une source de préoccupation importante chez les français. En effet, une étude du troisième baromètre de la confiance des français dans le numérique publiée par la Caisse des dépôts et consignations et par l'association de l'économie numérique en juin 2013, confirme une certaine maturité dans les usages du numérique ainsi qu'une inquiétude croissante sur la question des données personnelles[5]. Alors que 77% des internautes utilisent un ou plusieurs réseaux sociaux, le niveau de confiance auprès des opérateurs est très faible puisqu'il ne représente que 32% des utilisateurs. Cette étude nous enseigne que 92% des internautes français jugent important que la conservation de leurs données personnelles soit limitée dans le temps. Tandis que 52% des utilisateurs de réseaux sociaux manifestent quant à eux des craintes sur l'accès éventuel de tiers à leurs données[6]. On y voit donc par ces chiffres une sensibilité forte aux données personnelles et une prise de conscience des internautes quant à l'utilisation qui peut en être faite ainsi que les risques qui s'y rattachent. Le niveau de confiance envers les opérateurs demeure faible puisque de plus en plus d'utilisateurs sont informés du fait que leurs données sont conservées à long terme afin d'être réutilisées à d'autres fins. Ces données ne bénéficient donc pas d'une sécurisation suffisamment importante.

Perte de confiance, non connaissance des comportements à adopter… Pour éviter les dérives et usages abusifs de nos données, il faut mettre en place une véritable éducation du numérique à disposition des internautes. Alors que le numérique a envahi nos vies quotidiennement, un quart des français reste en marge de cette utilisation. Nombreux sont ceux qui ne disposent pas des connaissances suffisantes pour devenir de véritables citoyens du numérique, c'est-à-dire responsables et vigilants dans leurs usages. L'éducation au numérique consiste donc à diffuser auprès de tous une vraie « culture du numérique » permettant de comprendre cet univers. Reconnue grande cause nationale pour 2014, la mission d'éducation au numérique a été confiée à un collectif regroupant plus de cinquante organismes issus du monde de l'éducation, de la société civile, de l'économie numérique, et d'institutions nationales et internationales. Cela marque un signal fort et une prise de conscience des pouvoirs publics sur cette question. Tout au long de l'année seront donc proposées des actions en faveur d'une éducation numérique auprès de publics variés[7].

[5]« La protection des données personnelles : une source de préoccupation des internautes selon le 3e baromètre de la confiance des français dans le numérique », http://www.cnil.fr/

[6]Résultats de la 3e édition du baromètre Caisse des dépôts/ ACSEL sur la confiance des français dans le numérique, http://www.acsel.asso.fr./

[7]Education au numérique, http://www.educnum2014.fr/

En plus de développer des enseignements à destination des utilisateurs du numérique, une responsabilité est à mettre en œuvre du côté des entreprises et opérateurs du net. En effet, les utilisateurs étant peu confiants dans l'utilisation de leurs données personnelles, c'est aux responsables de les rassurer. L'aspect de confiance devient donc l'argument préalable pour rejoindre un réseau social mais il est également mis en avant par les entreprises pour inciter les internautes à s'y inscrire. La confiance devient donc la notion principale qui permet d'attirer, de vendre et de communiquer sur son réseau social. Avec le temps, les entreprises mais également les structures publiques ont compris que l'enjeu majeur reposait sur cette confiance envers les clients ou les administrés. L'argument commercial afin de valoriser la réputation de l'image de marque tient aujourd'hui au respect de la protection des données personnelles. Une concurrence s'instaure donc entre les entreprises puisque l'objectif est de faire venir des clients en prônant des pratiques sérieuses contrairement aux autres entreprises.

Cette convergence d'intérêts se retrouve également entre les entreprises et les utilisateurs puisque se pose la question de la maitrise des données personnelles. Qui est détenteur de nos données ? Aujourd'hui, on assiste à un conflit entre les opérateurs et les utilisateurs sur cette propriété puisque tous deux ont compris qu'elle était une source commerciale et chacun veut pouvoir en tirer un bénéfice. Alors que les entreprises des services internet revendiquent leur pleine propriété sur les données des utilisateurs, ces derniers prônent quant à eux la notion de droits de la personnalité pour justifier qu'elles leur appartiennent. Les opérateurs se sentent détenteurs des données car elles leur ont été confiées au moment de l'inscription sur le site internet et qu'ils les stockent dans leurs bases de données afin qu'elles deviennent une valeur économique. Les internautes quant à eux sont conscients de la valeur marchande de leurs données et arguent du fait qu'elles reflètent leur vie personnelle afin d'en avoir la propriété et de pouvoir les utiliser économiquement par la suite. Mais alors, comment ce bénéfice est-il partagé ? Il est difficile de reconnaitre à qui appartient la maitrise des données, bien que les entreprises aient une emprise assez importante sur leur utilisation. Une solution émerge à partir de l'idée d'un partage réciproque des données entre utilisateurs et entreprises puisque si ces dernières détiennent une information sur un individu, il doit être en mesure de l'avoir aussi. Or, actuellement les utilisateurs savent de moins en moins ce que les opérateurs détiennent comme informations sur eux[8]. Seulement, accorder un droit de propriété aux internautes sur leurs données personnelles reviendrait à dire que la protection des données n'est plus un droit fondamental, ni un droit de la personnalité. Un droit de propriété implique le droit d'être dépossédé, tandis qu'un droit de la personnalité reste inaliénable.

La question réside donc dans la qualification juridique du droit des données personnelles. Elles ont des enjeux qui leurs sont propres, ils peuvent être commerciaux ou philosophique.[9]

Google et Facebook ont demandé à l'Europe d'assouplir son régime sur les données personnelles, qu'ils considèrent trop rigide et comme étant un frein à leur activité. Cet assouplissement semble difficile suite aux derniers évènements. En effet, aux vues de l'affaire Snowden avec la NSA, l'idée d'assouplir un régime selon eux trop rigide semble plutôt ironique. Cette question à été soulevée lors des accords de libre-échange entre les États-Unis et l'Union Européenne (accords TTIP). De plus, l'Europe n'a pas encore de position sur la notion et l'étendue de la protection des données personnelles qui fait débat depuis des mois. Il est donc assez difficile de négocier sur une question à laquelle l'Europe n'a pas encore de réponse. Cette négociation entraînerait à se poser des

[8]Vie privée à l'horizon 2020, paroles d'experts, cahier IP, innovation et prospective de la CNIL, p.17, http://www.cnil.fr/

[9]http://www.internetactu.net/2014/03/17/donnees-personnelles-enjeu-commercial-ou-philosophique

questions dont la principale est, dans quel monde voulez-vous vivre ? Voulez-vous que l'on vous dise ce dont vous allez avoir envie avant même que vous ne le sachiez ? Où êtes-vous prêt à offrir toutes vos données personnelles, même les plus sensibles pour qu'elles soient récoltées à des fins positives ?

Ces questions sont largement soulevées avec l'utilisation intensive des réseaux sociaux. Nous nous sommes donc demandé quels peuvent être les enjeux de la collecte massive des données à caractère personnel par les réseaux sociaux ?

Notre développement s'appuiera sur la notion de confiance et sur le comportement des utilisateurs sur les réseaux sociaux. Nous montrerons la présence de risques et méfiances qui surviennent du fait de l'exploitation de notre identité personnelle numérique, entraînant de nouvelles problématiques juridiques (Partie I). En conséquence, nous verrons que des nouveaux engagements et des responsabilités apparaissent pour rétablir une réelle confiance des utilisateurs mais que ces engagements sont remis en cause par des revendications de plus en plus fortes (Partie II).

PARTIE 1 : Risques et méfiance au regard de l'utilisation des données personnelles sur les réseaux sociaux

Les réseaux sociaux connaissent une utilisation croissante qui entraîne des risques directement liés à l'exploitation de l'identité personnelle nécessitant des réponses juridiques face à des pratiques émergentes.

Section 1 : Les risques liés à l'exploitation de l'identité personnelle

Selon Edward Snowden « Un enfant né aujourd'hui grandira sans aucune conception de la vie privée ». Mais sur les réseaux, vie privée, identité personnelle ou même numérique ne trouve pas de définition propre. Nous verrons qu'il y a une grande imprécision face à des termes qui manquent de définitions et que l'exploitation de ces derniers crée notre E-réputation dont le réel danger est la finalité.

§1. L'imprécision face à des termes non définis

Sur Internet et particulièrement sur les réseaux sociaux on peut se créer une personnalité par la construction d'un personnage par exemple. Peut-on réellement parler d'une identité personnelle lorsque l'on crée cette personne ? L'identité personnelle relève à l'heure actuelle d'une sphère publique et privé avec l'avènement des réseaux sociaux. Si on dévoile notre vie privée on ne peut pas demander au droit de nous la protéger car « nul ne peut se prévaloir de sa propre turpitude »[10]. La notion d'identité personnelle regroupe donc la vie personnelle, la vie privée et le droit à l'image. La protection de la vie personnelle est donc englobée dans la protection de la vie privée. Aujourd'hui on distingue l'identité personnelle et l'identité numérique, même si l'identité personnelle n'est pas reconnue juridiquement. Ces mots clefs sont difficiles à définir. Il y a donc de grandes imprécisions quant à leur qualification et ces incertitudes se retrouvent tant chez le juge national, qu'européen. On distingue encore l'identité numérique et personnelle alors que l'on en voudrait qu'une seule.

L'internaute maîtrise les données qu'il publie sur les réseaux sociaux mais pas ce qui va en être fait ni ce qu'un autre pourra dire sur lui. À l'heure actuelle, l'individu est conscient des atteintes qui lui sont faites mais continu de publier des photos qui pourraient lui nuire. Il est donc nécessaire de le responsabiliser quant à la finalité de ses données. On parle ici d'une prévention des internautes et d'une protection contre soi-même. Est apparue l'idée d'imposer un certificat scolaire dans les écoles, réalisé par les gendarmes sous forme de question à choix multiples afin de protéger la vie privée des écoliers sur internet et leur permettre de connaître leurs limites. Cette solution serait applicable au jeune public mais ne sensibiliserait qu'une partie de la population. Néanmoins, cette question est un autre débat, plus sociologique que juridique.

Tout d'abord, considère-t-on que le réseau social est un espace public ou privé ?

[10] Article 1116 du Code civil : *Attendu que pour rejeter la demande en annulation de la vente, la cour d'appel énonce que, même s'il peut être admis l'existence d'une manœuvre commise de concert par les trois intimés […], il n'en reste pas moins que celui-ci s'est déterminé, […] en raison de la croyance qu'il avait de les revendre, à un prix "alléchant", à un acheteur enthousiaste, déjà client ; qu'elle considère qu'un tel comportement, "signe de cupidité", est nécessairement illicite et justifie que soit fait application de l'adage précité ; […].*

On y trouve une réponse nuancée dans la décision de la Cour de cassation du 10 avril 2013[11] concernant des injures sur le compte Facebook d'une salariée envers sa patronne. La cour d'appel avait retenu le caractère privé des propos car ils étaient destinés à un nombre restreint d'utilisateurs sélectionnés par la salariée. La Cour de cassation n'a pas retenu ces critères, estimant qu'ils ne suffisaient pas à former une communauté d'intérêts. Néanmoins, elle n'a pas saisi l'occasion pour définir la notion même de communauté d'intérêts sur les réseaux sociaux et y apporter des limites. Malgré le manque d'approfondissement de la cour à l'égard de cette décision, celle-ci a posé un attendu de principe qualifiant le mur Facebook des utilisateurs comme un lieu privé mais seulement selon deux conditions. Selon la Cour, Facebook n'est pas un lieu public mais pour qu'il soit dans la sphère privé il faut que les internautes qui ont accès aux messages diffusés soient agréés par le titulaire du compte et soient peu nombreux. Dans ce cas les utilisateurs sont reliés par « une communauté d'intérêts » et les propos échangés ne sont donc pas publics. Tout le débat sera désormais porté sur le sens de la « communauté d'intérêts » et sur la question relative au nombre « d'amis », sachant que la moyenne Française tourne autour de 200… La jurisprudence repose donc uniquement sur un principe : un profil est une communauté d'intérêts, il n'est pas public. Nous parlons ici de profil « fermé », réservé aux amis acceptés volontairement. Cela entraine la fameuse question les amis de mes amis font-ils partis de ma communauté d'intérêts sachant qu'ils ont accès à certaines de mes données privées sans même faire directement partis de mon réseau ? Il n'y a pas encore de réponse juridique claire à cette question car la Cour de cassation n'a pas défini la notion de communauté d'intérêts sur les réseaux sociaux.

Qu'on soit en présence d'espace privé ou public, la vie privée fait entièrement parti de l'identité numérique. La vie privée sur les réseaux sociaux est une notion qui existe en droit, alors que l'identité personnelle n'est pas reconnue par le droit. La vie privée est une partie de notre identité personnelle, qui elle-même est une notion conceptuelle car une identité ne peut être que personnelle. Cette vie privée sur les réseaux sociaux n'est pas protégée par l'article 9 du Code Civil mais l'est au sens de la Privacy by Design et de l'ordre public.

Le G29, groupe de CNIL européenne dans son avis du 12 juin 2009 [12] a constaté que, le plus souvent les services de réseaux sociaux présentent les caractéristiques suivantes : les utilisateurs sont invités à fournir des données à caractère personnel permettant de donner une description ou un « profil »; ils ont la possibilité, via des outils fournis par les services de réseaux sociaux, d'afficher leurs propres contenus photographiques, vidéographiques, sonores ou tout simplement textuel; enfin, ils disposent d'une liste de contacts avec lesquels ils peuvent interagir. Une résolution adoptée lors de la 30e conférence mondiale des Commissaires à la protection des données et de la vie privée d'octobre 2008[13] précise que « ces services offrent entre autres à leurs abonnés les moyens d'interagir en fonction de profils personnels qu'ils ont eux-mêmes crées et qui encouragent à révéler des informations personnelles à un niveau sans précédent sur soi et sur les autres ». Lors de cette conférence, il a également été constaté que si, « les services de réseaux sociaux offrent une nouvelle gamme de possibilités de communication et d'échanges en temps réel de toutes sortes d'information, l'utilisation de ces services peut cependant menacer la vie privée de leurs utilisateurs et d'autres personnes : des quantités sans précédent de données personnelles deviennent publiquement (et mondialement) disponibles sur ces nouveaux réseaux, y compris des images et des vidéos numériques ». C'est en contrepartie de la collecte des données à caractère personnel de leurs abonnés que les réseaux sociaux offrent leur service généralement gratuitement. En effet, leur modèle économique repose sur la publicité, la collecte de données personnelles permettant ainsi aux annonceurs de cibler leurs campagnes publicitaires en fonction des informations dévoilées sur chaque utilisateur.

[11] Cour de cassation, 1ère ch.civ., arrêt n° 344 du 10 avril 2013 (11-19.530)

[12]. G29, avis 5/2009, 12 juin 2009, les réseaux sociaux, site http://ec.europea.eu/

[13]. Résolution sur la protection de la vie privée dans les services de réseaux sociaux, 30e conférence mondiale des Commissaires à la protection des données et de la vie privée, Strasbourg, 15-17 oct. 2008

La prolifération des réseaux sociaux permet alors de constituer une « réelle identité virtuelle »[14] . Ce constat a été opéré par le G29, dans son avis du 12 juin 2009 qui relève que les services de réseaux sociaux « génèrent la plupart de leurs revenus avec la publicité diffusée sur les pages web que les utilisateurs créent et auxquelles ils accèdent. Les utilisateurs qui publient sur leurs profils beaucoup d'informations concernant leurs centres d'intérêts offrent un marché précis aux publicitaires souhaitant diffuser des publicités ciblées sur la base de ces informations ». Lors de la 30e conférence mondiale des commissaires à la protection des données et de la vie privée d'octobre 2008, il a été acté que les utilisateurs de réseaux sociaux « ignorent le plus souvent les conséquences d'une large diffusion d'informations très personnelles »[15]. Par exemple, les employeurs peuvent consulter les réseaux sociaux lors d'une procédure de recrutement. Il est difficile, voir impossible, de retirer certaines informations du web une fois qu'elles ont été publiées, ne serait-ce que sur un seul réseau social. De plus, ces données restent souvent accessibles via les moteurs de recherches.

Certains utilisateurs de réseaux sociaux commencent à exprimer leur inquiétude concernant l'exploitation de leurs données personnelles par les réseaux sociaux. Une plainte a été déposée contre Facebook par cinq utilisateurs américains, au motif que le site viole les lois californiennes en matière de respect de la vie privée. En effet, il ne permet aucun contrôle efficace sur les informations diffusées, contrairement aux affirmations de Facebook[16]. En France, à la suite de la plainte de l'évêque de Soisson, la société Facebook France a fait l'objet d'une première condamnation. Le juge des référés l'a enjoint de supprimer de son site, sous astreinte de 550 euros par jour, le groupe « Courir nu dans une église en poursuivant l'équêve » et de communiquer les données permettant l'identification des auteurs ce ces propos.[17]

§2. L'E-réputation face au principe de finalité

Un narcissisme numérique est progressivement apparu, c'est le premier souci de tension d'existence entre l'individu et le groupe. Les différents utilisateurs des réseaux sociaux ne sont pas conscients des risques liés à l'exploitation de leur image et de leur vie privée. Tout d'abord, l'objet principal d'un réseau social est la divulgation et/ou publication de photographies qui sont attentatoires à la vie privée, au droit à l'image, à notre honneur ou encore notre image de marque et donc généralement à notre identité numérique. Cette collecte massive des données à caractère personnel crée notre É-réputation qui est elle-même crée par deux entités : nous-même et les tiers. Tout d'abord nous sommes notre propre danger. On dévoile spontanément beaucoup d'information personnelle sur les réseaux sociaux. Depuis quelques années, on assiste à une tendance qui est d'en faire connaître le plus sur soi sur internet. C'est ici que l'on trouve cette notion de « narcissisme numérique ». Beaucoup de sites se créent, ils permettent de mettre en avant des informations personnelles d'internautes comme Instagram, Vine, ou encore Snapchat.

Cela a commencé par les blogs sur lesquels, seule la publication de photos intervenait. Les « bloggeurs » pouvaient les utiliser dans un but récréatif mais aussi professionnel. Aujourd'hui, un grand nombre de blogs servent à des hommes politiques, mais aussi à des avocats, ou encore à des journalistes. Par la suite, des sites, tels que « copains d'avant » ont eu pour but de retrouver des amis d'enfance répertoriés en fonctions des établissements scolaires fréquentés. D'autres comme « Linkedin », permettent de poster son curriculum vitae en ligne et de se faire repérer par des employeurs. En outre, la tendance de la société actuelle est de donner un maximum d'informations sur soi-même en ligne. Cette tendance a véritablement explosé avec l'émergence des réseaux sociaux tels que « MySpace », « Twitter », et bien-sûr « Facebook ». Le partage de ses propres données est

[14] Colloque droit de l'internet, « Données personnelles: des données personnelles à l'identité numérique »
[15]. CNIL, communiqué 22 oct 2008
[16]. « Facebook a encore des soucis avec la vie privée de ses utilisateurs », Les échos, 30 août 2009 »
[17]. Tribunal de grande instance, Paris, ord.réf.,13 avril 2010

la bible de ce dernier site, même s'il reste néanmoins possible de limiter la visibilité de son profil. Cependant, il est évident qu'une grande majorité des internautes ne se rend pas compte des risques pris en divulguant des données personnelles sur les réseaux sociaux et donc, de ce fait, sur internet. En effet, lors d'une recherche entreprise sur un moteur de recherches, tel que Google ou Yahoo, le premier résultat qui apparaît est Facebook. Si l'internaute n'a pas choisi de limiter son profil Facebook, ce ne sont pas seulement les utilisateurs du réseau qui pourront y accéder, mais bien tout le Web. Se pose alors la question de la protection des données personnelles mises en ligne sur les réseaux sociaux.

Comment peut-on partager sur les réseaux sociaux sans se sur-exposer ?

La CNIL a demandé à TNS Sofres de mener une étude auprès des internautes afin de comprendre quelle place occupent aujourd'hui les photos dans la vie numérique. Les interviews ont été effectuées par internet du 13 au 20 novembre 2012, sur un échantillon national de 1 554 personnes âgées de 13 ans et plus. Cette étude révèle une ambivalence des comportements et des perceptions, ainsi que des pratiques très différentes selon les âges. Enfin, elle souligne une demande forte de simplification des paramètres de confidentialité. De cette étude faite en 2012, on peut tirer plusieurs remarques[18]. Tout d'abord, elle a démontré que trois générations se distinguent avec des pratiques et des besoins bien différents :

- Les 13-17 ans ont un désir de s'exposer et de partager avec leurs amis. Ils sont très actifs sur les réseaux sociaux et publient beaucoup en pensant contrôler l'accès à leurs photos, ce qui n'est pas le cas.

- Les 18-24 revendiquent avant tout une liberté de s'exprimer. Ils sont cependant régulièrement gênés par les photos publiées par les tiers.

- Les 51 ans et plus publient principalement des photos de leurs vacances et de paysages, les publications sont plus neutres et moins personnelles. N'étant pas à l'aise avec les outils des réseaux sociaux, ils publient peu de photos trop personnelles.

Les tiers jouent aussi un rôle important car ils peuvent nuire à notre vie privée et donc à notre E-réputation avec leurs publications. Inconsciemment, ils peuvent porter atteinte à notre E-réputation et par conséquence à notre vie privée. 58 % des internautes déclarent publier des photos sur des sites, blogs ou réseaux sociaux (86% chez les 18-24 ans). De plus, 54 % des internautes, donc plus de la moitié d'entre eux prennent des photos dans le but de les publier. L'identification se fait surtout dans le but d'accroitre la notoriété d'une personne.

Les internautes sont donc partagés entre le respect de l'image de l'autre et l'envie de diffuser car 74 % déclarent demander l'avis des personnes photographiées avant de publier leur photo mais seuls 44% le font systématiquement. 61 % des 18 - 24 ans déclarent avoir déjà été gênés par une photo d'eux sur le net, avec 27 % qui déclarent que la publication de photo d'eux sur un réseau social a déjà eu un impact négatif sur leur vie personnelle et en général amoureuse. 80% des internautes estiment que les photos resteront sur internet, 66% pensent tout de même les supprimer plus tard et 73% estiment que cela sera difficile.

Selon donc Isabelle Falque-Pierrotin : Les photos occupent aujourd'hui une place centrale dans l'activité numérique des internautes : on les publie, on les partage, on les « like », on les commente, on tague ses amis… Elles représentent aussi un véritable enjeu économique pour les acteurs d'internet. Il est donc nécessaire d'accompagner les internautes pour les aider à mieux maîtriser la publication de leurs photos. Les réseaux sociaux doivent offrir des paramètres simples, visibles et accessibles qui répondent aux attentes exprimées par les utilisateurs.

[18]Site officiel, www.cnil.com

Cette envie de diffuser, partager porte atteinte à notre vie privée et ces atteintes vont encore plus loin grâce aux évolutions technologiques car un prototype de reconnaissance faciale a été développé[19]. Il s'agit d'un prototype de logiciel pour mobile capable de reconnaître en temps réel une personne croisée dans la rue et de retrouver des informations personnelles la concernant. Le prototype n'en est qu'à l'expérimentation mais il pourrait devenir aussi « banal que de chercher un mot sur les moteurs de recherche »[20]. Facebook et les autres réseaux sociaux n'en sont pas encore là malgré certaines pratiques contestables. En effet, on peut noter deux pratiques peu conformes aux textes de collecte des données, « le marquage des photographies » et « la reconnaissance faciale »[21]. Cette dernière consiste à identifier toutes les personnes qui apparaissent sur les photographies mises en ligne par l'un des utilisateurs du réseau. Une photographie de groupe permet ainsi de collecter de multiples renseignement (identité des personnes présentes, date, motif, circonstances) sur toutes les personnes qui ont participé à la réunion ou manifestation au cours de laquelle la photographie a été prise. À ce propos « plusieurs autorités européennes de protection de la vie privée se penchent depuis plusieurs mois sur la manière dont Facebook utilise la reconnaissance faciale. Pour « deviner » quelles sont les personnes qui apparaissent sur une photographie, Facebook a construit une gigantesque base de données biométriques. Or pour collecter ce type de données, le droit européen prévoit que le consentement de l'utilisateur doit être explicite, et l'utilisateur doit avoir la possibilité de refuser que ses données soient enregistrées. Deux points sur lesquels les CNIL européennes ont demandé des précisions à Facebook ». [22]

Le réel danger est donc la finalité de ces données, beaucoup plus que la diffusion en elle-même. Mais aujourd'hui, les internautes accordent une importance particulière à la préservation du contexte plus qu'au contenu lui-même. Ils veulent gérer le sens de leur publication : le lieu, le moment, « les destinataires ». L'exemple marquant date de fin septembre 2012, lorsque les utilisateurs de Facebook ont vu réapparaitre publiquement des informations anciennes qui avaient un caractère privé. D'anciens messages privés des années 2007, 2008 et 2009 sont apparus par erreur sur leur profil public. Il y avait donc la perte du contexte originel car les messages avaient été diffusés dans une conversation privée, et sont apparus publiquement à cause de ce « bug ». Il y a donc une réelle importance du contexte originel qui ne doit pas être modifié. Ainsi, on raconte sa vie sur Facebook, mais pas à tout le monde : on accepte sa mère et son employeur comme « amis », mais on ne leur donne pas accès aux photos de soirées arrosées. On remplit le formulaire d'un site de livraison à domicile, mais on ment sur sa date de naissance. On se confie sur des forums, mais sous pseudonyme. On multiplie les « selfies » sur Instagram (des photos de soi à partager avec sa « communauté »), mais aussi les fausses identités sur Twitter.

Peut-on imaginer qu'à l'avenir, le droit considèrera qu'il y a une fusion entre l'individu réel et le virtuel ? On aurait alors un nouvel espace économique pour l'individu réel. De plus, la personnalité fictive pourrait-elle prendre le pas sur la réalité?

[19] DERIEUX (E) et GRANCHET (A), « Réseaux sociaux en ligne : Aspects juridiques et déontologique », *Lamy Axe droit*, 2013, p182

[20]Ferran B., Facebook identifie vos amis par reconnaissance faciale, « www.lefigaro.fr, 8 juin 2011

[21]Site officiel le monde, www.lemonde.fr. 6 août 2012

[22]Site officiel le monde, www.lemonde.fr, Reconnaissance faciale: une enquête visant Facebook rouverte en Allemagne, 8 juin 2011

Section II : Des réponses juridiques à des pratiques émergentes

Les réseaux sociaux sont aujourd'hui l'un des principaux espaces de communications qu'offre l'internet, ils incitent leurs utilisateurs à donner le plus d'informations sur eux-mêmes mais aussi sur les autres. Leurs membres sont alors amenés à laisser à leur sujet, à tout âge, à tout instant de leur vie, une quantité de données et de traces les concernant directement, ou indirectement sur ces espaces de communications. Dès lors, la vie privée de chaque utilisateur devient rapidement « publique ». Nous verrons que de nouvelles pratiques néfastes pour les utilisateurs de ces réseaux sociaux sont apparues, ce qui a entrainé une perte de confiance de leur part. Ces derniers ont alors revendiqués de nouveaux droits qui sont en train de se mettre en place pour répondre à ces nouvelles attentes.

§1. Des pratiques émergentes sur les réseaux sociaux

Chaque année en France, 210 000 personnes sont victimes d'usurpation d'identité[23]. L'usurpation d'identité sur les réseaux sociaux s'est beaucoup développée ces derniers temps. Le coût total attribué aux usurpations d'identité sur internet aux Etats-Unis en 2012 s'élève à 24,6 milliards de dollars (environ 18 milliards d'euros)[24]. L'article 226-4-1 du Code pénal définit l'usurpation d'identité numérique comme le fait de faire usage, de manière réitérée, sur un réseau de communications électroniques, de l'identité d'un tiers ou de données qui lui sont personnelles, en vue de troubler la tranquillité de cette personne ou d'autrui ou de porter atteinte à son honneur ou à sa considération. C'est donc le fait pour une personne de chercher à obtenir, détenir ou utiliser les informations personnelles d'une autre personne sur Internet, sans autorisation et dans un but frauduleux. Concrètement, cette usurpation d'identité pourrait se traduire par le fait de commettre, sous l'identité d'autrui des actes répréhensibles, nuire à la réputation d'une personne en créant de faux profils, un blog, ou en rédigeant des commentaires avec l'identité de cette personne par exemple. Cette pratique est courante car n'importe qui peut se créer un profil Facebook avec le nom et le prénom qu'il souhaite. Aucune justification n'est demandée lors de l'ouverture d'un compte nominatif, que le nom utilisé soit célèbre ou qu'il ne le soit pas. De plus, les données contenues sur ces réseaux sociaux peuvent faciliter la tâche d'un usurpateur d'identité. De nombreux hommes politiques, sportifs, célébrités ou même quiconque ont été victimes, ces dernières années, d'usurpation d'identité via les réseaux sociaux et particulièrement sur Facebook.

L'article 434-23 du Code pénal sanctionne le fait de « prendre le nom d'un tiers, dans des circonstances qui ont déterminées ou auraient pu déterminer contre celui-ci des poursuites pénales». Ce délit est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Il avait pour inconvénient de ne pas prendre en compte toutes les possibilités d'usurpation d'identité numérique.

Alors que ces cas se sont multipliés avec le développement de la communication en ligne, la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) fût promulguée le 14 mars 2011. Elle créée un nouveau délit d'usurpation d'identité numérique, l'article 226-4-1 du Code pénal. Il vient renforcer le délit d'usurpation d'identité « non-numérique». Selon la CNIL, on distingue sur internet deux types d'usurpation d'identité. La plus courante est appelée le phishing, hameçonnage ou encore filoutage. Soit l'usurpateur envoi à sa victime un courrier électronique réclamant la confirmation de certaines données personnelles nous concernant, en se faisant passer pour un organisme public ou privé connu, soit il crée un faux site web destiné à

[23]Enquête du Centre de recherche pour l'étude et l'observation des conditions de vie
[24]Bureau of Justice Statistics

récolter des informations personnelles. Ces informations sont ensuite utilisées pour accéder à des comptes sécurisés et effectuer des opérations sous l'identité de la victime. Ces informations, obtenues de manière frauduleuse, peuvent également être utilisées par les usurpateurs pour pirater des comptes Facebook de particuliers et les utiliser comme support pour propager leurs arnaques. L'autre pratique consiste à créer un faux profil, un blog, ou rédiger des commentaires sous l'identité de la personne à qui l'on a volé les données personnelles et nuire à sa réputation. L'usurpation d'identité sur Internet peut avoir des conséquences très graves, notamment financières ou en termes de réputation.

L'article L226-4-1du Code pénal punit l'usurpateur d'une peine pouvant aller jusqu'à un an d'emprisonnement et 15 000 euros d'amende. Avant tout procès, il appartiendra cependant à la victime d'obtenir, sur décision judiciaire, la communication par le réseau social et/ou le FAI des éléments permettant d'identifier l'usurpateur. Il est donc important de systématiquement déposer une plainte lorsqu'une personne constate que son identité a été usurpée. Si cette identification n'a pas été possible, la victime pourra porter plainte contre X afin qu'une enquête soit menée. La prescription pour ce nouveau délit est de cinq ans.

Au-delà de l'infraction pénale, la victime peut également rechercher la responsabilité civile de l'usurpateur sur les terrains de l'atteinte à la vie privée[25] ou du droit à l'image. Par ailleurs, la loi sur la liberté de presse de 1881 s'appliquant aux réseaux sociaux reconnait différents délits. La diffamation ou l'injure pourront faire l'objet de sanctions à condition que la victime agisse dans un délai de 3 mois à compter de la première publication du propos incriminé.

Les réseaux sociaux ont une obligation de supprimer le compte ou profil usurpé après en avoir été avisés. Cependant ils ne sont pas obligés de prévenir ces usurpations. Des moyens ont été mis à la disposition des internautes pour se protéger contre une usurpation d'identité. Ils peuvent signaler une infraction ou un contenu qui leur semble illicite sur une plateforme « pharos »[26] où des conseils ciblés peuvent les guider. Concernant Facebook, il suffit d'aller sur le site[27], de cliquer sur la mention « confidentialité » puis sur « si vous avez d'autres questions concernant la protection de la vie privée ». Ensuite, il faut cliquer sur la mention « rapport d'abus » et enfin sur « j'ai besoin de faire état d'une imposture de mon profil ». On arrive directement sur un formulaire qu'il va falloir remplir et envoyer. Quelques jours plus tard, le faux profil devrait avoir été effacé. Sur la page réservée aux informations concernant la protection de la vie privée, on peut également déclarer tout autre abus qui ne serait pas mentionné dans le site. Facebook s'engage à fournir une réponse dans les 72 heures suivant la réception d'un message.

Quelques affaires connues illustrent ces cas d'usurpation d'identité sur les réseaux sociaux. C'est le cas de l'affaire « Omar Sy »[28] dans laquelle une personne avait créé une page de profil Facebook avec le nom, prénom, date de naissance et 6 photographies de l'acteur Omar Sy. De nombreuses personnes pensaient alors être en présence du vrai Omar Sy, l'ont ajouté comme « ami » et ont posté plusieurs commentaires à titre personnel. L'acteur avait alors assigné Facebook afin que les identifiants de la personne qui avait publié un faux profil à son nom lui soient communiqués. Il a fait identifier l'internaute, grâce à son adresse IP, avant de l'assigner en justice pour avoir usurpé son identité. Ce dernier a été assigné en référé sur le fondement de l'atteinte à la vie privée et au droit à l'image de l'artiste. Pour le tribunal, le prénom, nom et la date de naissance du demandeur « sont des éléments d'identité ne relevant pas de la vie privée ». En revanche la révélation d'informations concernant les goûts, le nom de certains amis de l'acteur ou la publication de photographies de celui-ci sont des éléments majeurs pour observer une violation de sa vie privée et de son droit à l'image. Par

[25]Article 9 du Code civil et article 8 de la CEDH
[26]https://www.internet-signalement.gouv.fr/
[27]https://www.facebook.com/
[28]TGI de Paris, 17ème Chambre civile, 24 novembre 2010

une ordonnance de référé, le TGI de Paris a alors condamné l'usurpateur pour atteinte à la vie privée de l'acteur ainsi qu'à son droit à l'image, à 4 000 euros dont 2 500 euros à titre de réparation. Dans cette affaire, ce n'était pas la création d'un faux profil, donc l'usurpation d'identité en elle-même qui a été sanctionnée.

Dans l'affaire Mathieu S / Twitter[29], Mathieu S avait découvert qu'un faux profil public avait été créé avec son nom, prénom, état civil et des images sur le réseau social Twitter. C'est ainsi que près de 5 000 tweets ont été postés par une personne s'étant totalement attribuée son identité. De plus, l'usurpateur allait même jusqu'à communiquer avec des « followers » par SMS. Malgré plusieurs demandes de suppression du faux profil, la société Twitter Inc a maintenu en ligne le faux profil litigieux. Matthieu S avait donc assigné la société le 20 Février 2013, pour lui faire injonction sous astreinte de supprimer ce faux profil public, de communiquer tous éléments d'identification de son auteur, outre l'allocation d'une provision de 50 000 euros en réparation du préjudice moral. Par une ordonnance, le juge des référés a condamné la société Twitter à communiquer à la victime l'ensemble des éléments d'identification de l'auteur du faux profil.

Au-delà de l'usurpation d'identité numérique, la pratique du traitement et de la commercialisation des données des utilisateurs de réseaux sociaux, à leur insu se développe. En effet, toutes les informations qu'il est possible d'avoir sur un individu sont récupérées. Facebook, par exemple stocke l'ensemble de nos données sans jamais en effacer une seule. Plus de 500 téraoctet de données sont stockées chaque jour par ses serveurs et 2,5 milliards de contenus comme les photos ou les « Like », sont quant à eux échangés tous les jours sur la plateforme. A ce propos, Max Schrems, un étudiant en droit autrichien, avait déposé 22 plaintes contre Facebook, chacune se rapportant à ce qu'il juge être une violation illégale de sa vie privée. Il avait souhaité obtenir la liste de toutes les données que Facebook possède sur lui, il a reçu un CD Rom sur lequel se trouvait un PDF de 1222 pages. Il a pu se rendre compte que tout le contenu qu'il avait cru effacé de Facebook, n'est en fait que masqué et reste inscrit pour toujours dans sa base de données. Toutes ces données récupérées servent ensuite. Une étude[30] démontre que le fait de déclarer aussi ouvertement ses goûts sur les réseaux sociaux reflète notre identité. Ainsi, ils se servent de nos données personnelles pour observer les goûts et les habitudes de consommation de chacun. Ces informations sont ensuite commercialisées aux annonceurs qui achètent des publicités sur le réseau social. Facebook a d'ailleurs affirmé son droit d'utiliser toutes les données de ses utilisateurs pour la publicité dans sa déclaration des droits et responsabilités réécrite en 2013. Le réseau social indique clairement dans sa « politique d'utilisation des données » et plus précisément dans la rubrique « principes de la publicité et des actualités sponsorisées », afin de présenter à ses utilisateurs un contenu susceptible de les intéresser, il peut utiliser l'ensemble des informations qu'il reçoit à leur sujet pour publier des publicités plus adaptées à leurs goûts. Ainsi, si un utilisateur à récemment rompu une relation, il pourra voir apparaitre des publicités de sites de rencontre.

Une autre forme de commercialisation de données des utilisateurs de réseaux sociaux se développe. Facebook a annoncé en octobre 2013 qu'il partagerait des données avec TF1 et Canal+. Les deux groupes de télévision ont donc accès à des outils d'analyse des commentaires publics sur leurs émissions publiés par les utilisateurs de Facebook en France. Ils connaissent ainsi leur popularité auprès du public.

Toutes ces nouvelles pratiques dérangent les utilisateurs, qui perdent confiance en les réseaux sociaux. L'affaire des « sponsored stories » illustre cela. Il s'agissait d'une poursuite à l'encontre de Facebook déposée le 11 Mars 2011 auprès d'un tribunal de San Francisco à l'initiative de cinq utili-

[29]TGI de Paris, Ordonnance de référé, 04 avril 2013

[30]Publiée dans le journal scientifique américain PNAS, par les chercheurs Michal Kosinski, David Stillwell et Thore Graepel

sateurs américains qui dénonçaient une atteinte à leur vie privée. Facebook avait repris, sans consentement, certains contenus comme des commentaires, leur géolocalisation ou encore les mentions « j'aime » qu'ils avaient publiées. En août 2012, le réseau social a été condamné à verser 10 millions de dollars pour frais d'avocats ainsi qu'une enveloppe de 20 millions de dollars destinée à l'indemnisation de toutes les victimes. Le montant maximal de l'indemnité est fixé à 10 dollars car 150 millions d'individus sont potentiellement intéressés. La somme pourrait ne même pas dépasser 10 cents par personne, étant donné le nombre de personnes potentiellement concernées. L'indemnisation est faible mais au moins, la décision reconnait que le réseau social porte atteinte à la vie privée de ses membres.

Pour répondre à ces nouvelles revendications de la part des utilisateurs de réseaux sociaux, le «projet de règlement européen sur les données personnelles » essaie de mettre en place de nouveaux droits répondant à ces nouveaux besoins.

§2. De nouveaux droits pour de nouveaux besoins

Le droit à l'oubli se rapproche du « droit à l'autodétermination informationnelle » consacré par la Cour Constitutionnelle fédérale allemande[31]. Il s'agit de conférer à la personne le pouvoir de décider elle-même la mesure dans laquelle les informations la concernant peuvent être traitées, communiquées, et conservées. Sur les réseaux sociaux, ce droit permettrait à tout utilisateur de pouvoir supprimer toutes les informations le concernant, qu'il aurait pu y laisser comme ses photos ou commentaires. Le droit à l'oubli numérique est une revendication nouvelle d'un droit nouveau car l'information sur le net est difficile à faire disparaitre, elle a des conséquences préjudiciables pour la personne. Alors que de nombreux pays se posent la question d'un droit à l'oubli, la Californie a fait un pas important dans ce sens. Une loi[32] permet aux mineurs de demander à l'éditeur d'un site internet d'effacer des contenus embarrassants. Si un contenu publié nuit à sa personne, il pourra le retirer lui-même ou demander simplement au service de le retirer, selon les cas. Les réseaux sociaux auront l'obligation d'accéder à la requête de l'internaute, si celui-ci est mineur au moment de la demande. Cette nouvelle loi entrera en application le premier janvier 2015 pour laisser le temps aux sites de s'organiser. En France, il n'y a pas aujourd'hui de texte du droit positif qui consacre en tant que tel le droit à l'oubli.

L'Europe cherche actuellement à se doter d'un nouveau règlement sur la protection des données personnelles. Il vise à réformer l'actuelle directive européenne de 1995 sur la protection des données personnelles qui est obsolète. Elle avait été écrite pour un autre univers, avant l'émergence d'internet et des réseaux sociaux[33]. Ce projet de règlement européen, actuellement en discussion à Bruxelles a pour vocation la mise à jour radicale des instruments juridiques de l'Union Européenne. Il tente d'établir, de consacrer un droit à l'oubli, qui figure dans son article 17 intitulé « droit à l'oubli numérique et à l'effacement ». Cet article dit que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de leur diffusion. Le droit à l'oubli ne dépendrait plus seulement du droit à la vie privée ou à être laissé tranquille, mais serait plutôt un droit à l'autodétermination informationnelle. Si le texte est voté, le droit à l'oubli sera composé de deux aspects, le droit pour l'utilisateur d'obtenir du responsable du traitement l'effacement des données à caractère personnel le concernant ou la cessation de leur diffusion. Ce droit s'appliquerait surtout aux données à caractère personnel que la personne avait rendu publique lorsqu'elle était enfant. Cet article 17 prévoit aussi un droit de suite. Lorsque

[31]Cour Constitutionnelle fédérale allemande, 15 décembre 1983
[32]Loi Senate-Bill-568 ou « Eraser Law » du 23 septembre 2013
[33]Édouard Geffray, secrétaire général de la CNIL

le responsable du traitement à rendu publiques les données à caractère personnel d'une personne, que ce soit en les transférant ou en les mettant sur internet, il devra prendre toutes les mesures raisonnables en vue d'informer les tiers qui traitent les données, que la personne veut les effacer, il faut faire suivre la demande. Lorsque la personne exercera ce droit, le responsable devra effacer les données sans délais sauf dans certains cas. Les autorités nationales de protection des données seront chargées de mettre en pratique ces règles communes. Les sanctions en cas de leur non-respect pourront aller jusqu'à un million d'euros ou 2% du chiffre d'affaires global d'une entreprise.

S'il y a une volonté de consacrer un droit à l'oubli numérique, ce droit n'existe pas en tant que tel actuellement. Or, les demandes des utilisateurs de réseaux sociaux pour faire exercer ce droit sont grandes. Le juge cherche alors à faire appliquer ce droit à l'aide des instruments juridiques dont il dispose. On trouve une référence à la limitation des données dans la Loi du 6 Janvier 1978. Elle prévoit dans son article six, cinquièmement que les données à caractère personnel doivent être conservées pendant une période limitée proportionnée à la finalité du traitement. Il existe donc déjà un droit à l'oubli numérique, dans la mesure où la loi « informatique et libertés » impose que la durée de conservation des données personnelles n'excède pas le temps strictement nécessaire à la réalisation du traitement pour lequel elles ont été collectées. Ce qui peut se traduire par l'obligation d'effacer les données, ou de les anonymiser si un particulier en fait la demande. On observe donc que la politique de conservation des données à caractère personnel de Facebook n'est pas pleinement respectueuse des modalités prévues dans cette loi. En effet, les principes du « Safe Harbor » auxquels la société Facebook a adhéré, ne prévoient pas de durée de conservation des données à caractère personnel qu'elle traite. Il appartient donc à chaque entreprise américaine d'en fixer elle-même la durée. Une entreprise américaine peut même garder indéfiniment ces informations car aucune autre législation américaine n'encadre leur durée de conservation.

Toute personne justifiant de son identité a le droit d'interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication. Il s'agit d'un « droit d'accès ». Plusieurs personnes l'ont déjà exercé sur Facebook, c'est le cas de l'étudiant autrichien Max Schrems dont nous avons parlé précédemment qui s'était vu remettre un PDF de 1222 pages le concernant. L'exercice de ce droit d'accès permet de contrôler l'exactitude des données et de les faire rectifier, compléter ou effacer. En effet, la loi « Informatique et libertés », dans son article 40 donne la possibilité à toute personne faisant l'objet d'un traitement de données à caractère personnel d'exiger du responsable d'un traitement que soient, selon les cas, « rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

L'article 38 de la loi du 6 janvier 1978 donne aussi la possibilité à toute personne de s'opposer à figurer dans un fichier ou à l'utilisation des données qui la concernent à des fins de prospection, en particulier commerciale. Pour exercer ce droit d'opposition, l'utilisateur d'un réseau social peut paramétrer son compte comme il le souhaite ou demander au réseau social de supprimer certaines données le concernant.

Parfois, le droit à l'oubli numérique peut aussi s'exercer au travers de l'article 9 du Code civil qui garantit le droit à la vie privée. C'est ce qu'illustre un arrêt Max M. / Google France, Google Inc[34] dans lequel le juge avait imposé à Google de retirer et cesser l'affichage de ses résultats de moteurs de recherches de photos attentatoires à la vie privée.

[34]TGI de Paris, 17ème chambre, 6 novembre 2013

En France, certaines personnes comme Roseline Letteron[35] rattachent le droit à l'oubli à la défense de l'intérêt public. Ce « droit d'oublier » impose collectivement le silence sur les fautes et les peines des citoyens, dans certaines circonstances, pour garantir paix et cohésion sociales. Les lois d'amnistie, les règles relatives à la prescription, ou encore l'interdiction de mentionner les condamnations ayant fait l'objet d'une réhabilitation, illustrent bien cette approche. Tout fait prescrit, ou tout fait ayant fait l'objet d'une amnistie, ne peuvent donner lieu à aucune poursuite, ni à aucune condamnation. A ce propos, la Cour de cassation a jugée dans l'affaire Devedjian contre Nice matin[36] que le journal « Nice matin » était fautif de rappeler des faits amnistiés concernant l'homme politique Patrick Devedjian qui avait siphonné de l'essence lorsqu'il était jeune.

De plus, le projet de règlement européen souhaite consacrer un droit à la portabilité des données dans son article 18. Lorsqu'un réseau social gère des données personnelles concernant l'un de ses membres et qu'il souhaite qu'elles soient transmises à un autre réseau social, il peut lui demander de les transmettre à l'autre entité. Ce projet tend aussi à créer un droit de s'opposer au profilage dans son article 20. Il s'agit pour la personne concernée de pouvoir faire interdire un traitement automatisé destiné à évaluer certains aspects personnels.

Enfin, l'Europe tend vers un renforcement de l'obligation de consentement de la personne concernée avant de traiter ses données personnelles, qui est déjà consacré par l'article 7 de la Loi Informatique et libertés. Elle va dans le sens d'une plus grande maîtrise de l'accord et de son retrait par la personne concernée.

À travers ce projet de règlement européen, nous voyons que « l'Europe a franchi un pas significatif, elle se prépare à rendre les droits sur les données personnelles à leur véritable propriétaire : la personne »[37]. Les réseaux sociaux sont cependant opposés à ce projet et pratiquent un véritable lobbying.

Nous venons de voir qu'avec le nombre d'utilisateurs de réseaux sociaux qui ne cesse d'augmenter, de nouvelles pratiques néfastes pour eux se sont développées. Ils ont alors eu de nouvelles revendications auxquelles le législateur ou le juge essaient de répondre. Il semble intéressant de s'intéresser aux engagements qu'ont pris les réseaux sociaux envers les utilisateurs pour répondre à ces nouvelles exigences.

[35]Juriste et professeur de droit public à l'Université de Paris-Sorbonne
[36]Cour de cassation, 17ème chambre, 16 mai 2013
[37]Monique Goyens, directrice du Bureau Européen des Unions de Consommateurs

PARTIE II : Engagements et responsabilité dans la gestion des données personnelles sur les réseaux sociaux

C'est parce que les internautes sont conscients des risques liés au dévoilement de leur vie privée sur les réseaux sociaux qu'ils formulent de nouvelles demandes auprès des opérateurs (Section I), lesquels tentent malgré tout de les rassurer en se responsabilisant par la mise en place d'obligations (Section II).

Section I : Les nouvelles revendications des utilisateurs

Si les utilisateurs présentent des revendications, c'est parce qu'aujourd'hui il existe des dangers et risques à une sur exposition sur les réseaux sociaux. En effet, les 18 millions de membres qui utilisent quotidiennement Facebook en France peuvent parfois connaître des déconvenues : piratage de compte, diffusion de photos gênantes, difficulté à supprimer un compte, etc.

En rendant ses informations trop accessibles, en ne les protégeant pas suffisamment dans les paramétrages, les données personnelles peuvent être par la suite utilisées à des fins non désirées ou non légales. Il faut donc faire attention à ne pas se nuire personnellement sur les réseaux sociaux et tâcher de contrôler sa réputation numérique. Cette dernière est créée par l'utilisateur lui-même en postant des informations, des photos, en partageant des liens sur les réseaux sociaux, puisque cet ensemble représente son profil numérique. La tendance aujourd'hui est au déballage de sa vie privée sur les réseaux sociaux pour toujours plus de partage avec ses contacts virtuels. Beaucoup de personnes délivrent un grand nombre d'informations dans leur profil qui sont à disposition de tout un chacun. Les nouveaux usages du numérique font donc évoluer les esprits et les comportements sur les réseaux. En oubliant de paramétrer la divulgation des données perceptibles par les autres, qu'ils soient des « amis » ou non, on omet de se protéger soi-même. Les informations peuvent être mal interprétées par la suite ou être réutilisées par l'entourage. Nombreux sont ceux dont des photos compromettantes réapparaissent des mois ou des années après, à leur insu, pour un usage tout autre que celui initial et les conséquences ne seront plus les mêmes, l'image de la personne pouvant être entachée. Un collègue de travail tombant sur une photo de soi prise lors d'une soirée arrosée peut ne pas avoir le même effet que lorsque c'est un ami proche qui la voit. Ici, c'est l'honneur et la considération de la personne qui seront entravées.

Si l'e-réputation est créée par ce que l'on décide de mettre en ligne, elle peut également être subie par la personne elle-même. En effet, en ne protégeant pas leurs données, les utilisateurs peuvent faire l'objet d'interception illégale des données personnelles ou d'usurpation d'identité numérique[38]. Jamais à court d'imagination, farceurs ou escrocs utilisent les réseaux sociaux pour usurper des identités personnelles et les conséquences peuvent parfois être très lourdes voire désastreuses sur l'entourage intime ou professionnel. Le mobile peut donc être de nuire à l'image de quelqu'un ou à celle de ses proches ou bien de violer sa vie privée en exploitant des photos ou de la correspondance ou en postant des statuts à son insu. Cette pratique peut gravement nuire à l'e-réputation de la personne concernée qui se verra très fortement affectée[39]. C'est d'ailleurs sur le fondement de l'atteinte à la vie privée et au droit à l'image que l'usurpation d'identité d'un individu a d'abord été sanctionnée[40].

[38]Infraction créée par la Loi n°2011-267 LOPPSY II 14 mars 2011, http://www.legifrance.fr/
[39]« Quels sont les risques d'usurpation d'identité numérique? », http://www.hadopi.fr/
[40]TGI Paris, 17e ch., 24 novembre 2010, Omar S. c/ Alexandre P

1§. La commercialisation des données

Pour éviter ce genre d'infraction, les internautes doivent se protéger en pensant à créer des mots de passe complexes et différents selon les utilisations, à ne jamais communiquer ces mots de passe, à éviter de se connecter sur les réseaux sociaux dans des lieux publics ainsi qu'à ne pas répondre à des mails de demande de coordonnées personnelles.

Seulement, les risques d'atteinte à la vie privée ne sont pas liés seulement à la mauvaise gestion par l'utilisateur lui-même de ses données puisque l'exploitation de nature à porter atteinte aux droits des abonnées tient notamment à la commercialisation des données.

Bien que l'article 38 de la loi de 1978 dispose que « toute personne physique (…) a le droit de s'opposer (…) à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale », on se rend compte qu'entre les principes énoncés par la loi et les pratiques des opérateurs de réseaux sociaux, un grand fossé existe[41].

Aujourd'hui, on assiste au développement d'entreprises qui se créent pour stocker, traiter et vendre nos informations. Ces entreprises en ont fait un véritable business et les données personnelles sont devenues des valeurs marchandes permettant d'opérer sur le marché des opérations de marketing et d'échange entre elles.

Les responsables de traitement sont donc confrontés au défi de l'optimisation des données pour en tirer le meilleur profit. Dans cette optique, le profilage devient un outil performant de plus en plus utilisé. Le profilage est une technique de surveillance ou d'exploitation des données qui permet de faire une comparaison entre les profils déjà établis et le profil de l'internaute grâce à une analyse comportementale. Il consiste à repérer les individus qui pourraient être sujets d'une surveillance ou d'une attention particulière. En comparant les profils entre eux, les opérateurs de réseaux sociaux dressent de véritables personnalités en fonction de leurs goûts, habitudes, loisirs. Le profilage est donc devenu une véritable réalité de l'ère numérique. Les technologies d'aujourd'hui génèrent des données sur la base desquelles il est relativement facile d'observer, d'analyser et de tracer les différentes activités des internautes afin d'orienter leurs choix sur la base du profilage. Cette méthode représente donc un intérêt économique non négligeable pour les entreprises. Cependant elle produit des conséquences négatives sur le respect du droit à l'image et de la protection des données personnelles puisque des informations sur l'utilisateur sont échangées entre les différents acteurs sans que celui-ci n'en ait conscience ni ne puisse le contrôler[42].

Si le profilage est utilisé par les entreprises c'est pour permettre par la suite de pratiquer le scoring, méthode de marketing de plus en plus développée. Il consiste en une technique de hiérarchisation des données, analysées au préalable par le profilage, qui permet d'évaluer par une note ou un score la probabilité que l'individu appartienne à la cible recherchée. Cette pratique est obtenue à partir des données quantitatives et qualitatives calculées sur les comportements de la personne, à la suite de quoi celles-ci sont classifiées afin d'être commercialisées.

Ainsi, à partir de la connaissance du contenu des messages échangés par les abonnés des réseaux sociaux et donc par conséquence de la manifestation de leurs goûts, de leurs préoccupations et domaines d'intérêt, les annonceurs peuvent orienter davantage les publicités pour les consommateurs. C'est ce qu'on appelle la publicité ciblée[43]. Les méthodes du profilage et du scoring permettent donc de faciliter et de pratiquer ce type de publicité. En offrant un accès gratuit à son service, Facebook utilise en contrepartie les données récoltées sur son site en vue de les analyser à des fins

[41]DERIEUX (E) et GRANCHET (A)., « Réseaux sociaux en ligne : Aspects juridiques et déontologique », *Lamy Axe droit*, 2013. p.164

[42]WALTER J.-P. « Le profilage des individus à l'heure du cyberespace : un défi pour le respect du droit à la protection des données », http://www.coe.int/

[43]Rapport de la CNIL, 9 février 2009, « La publicité ciblée en ligne », p. 5

commerciales étant donné que l'essentiel de son financement provient des revenus publicitaires. Les profils offrent une description assez détaillée des centres d'intérêts des abonnés grâce aux informations renseignées lors de l'inscription. Toutes ces données constituent une base importante sur les goûts des utilisateurs et les annonceurs sont prêts à payer le prix nécessaire pour y avoir accès et toucher la cible visée[44]. C'est d'ailleurs sur Facebook que depuis peu on peut voir apparaître dans le fil d'actualité des publicités personnalisées en fonction des pages qu'on suit ou des informations que l'on a renseignées ou même encore en fonction des mots-clés employés. Pour ces géants de l'internet, le fait de pouvoir suivre le comportement en ligne des internautes est une clé essentielle de leur modèle économique. Ces informations permettent de proposer de la publicité personnalisée, plus efficace que les campagnes d'affichage génériques. La publicité ciblée est donc une forme d'exploitation des données collectées et lorsqu'elle est adaptée à la navigation, à la localisation ou à l'identification des internautes, elle peut toucher à la protection de leur vie privée. D'ailleurs, bien qu'une faible majorité des internautes aient conscience que leurs données puissent être utilisées à des fins publicitaires (55%), certains le craignent et ils sont une très large majorité à en être gênés (82%)[45].

Mais si on sait que la publicité sur internet est une composante essentielle du financement des services en ligne, la loi de 1978 requiert d'informer les internautes sur le traitement de leurs données à des fins de diffusions de publicités personnalisées[46]. Or, on sait que les opérateurs respectent que très rarement à cette disposition.

La publicité ciblée est également mise en œuvre grâce à la pratique de la géolocalisation. Appelée également « suivi à la trace », elle permet aux annonceurs publicitaires et commerçants de localiser les individus et de jouer sur la proximité pour les attirer sur leurs lieux de vente. En géolocalisant les internautes, les annonceurs peuvent ainsi leur proposer des services sur internet tout près de chez eux. C'est ce qui explique que des publicités relatives aux commerces de notre ville peuvent apparaître régulièrement sur le bas ou les cotés des écrans, alors que l'on effectue une recherche tout autre. Ce mode d'exploitation des données collectées est particulièrement intrusive et attentatoire à la vie privée des personnes. D'ailleurs, la Cour de cassation, dans deux arrêts du 22 octobre 2013, a affirmé que ce procédé est une entrave au droit au respect de la vie privée, en précisant notamment que la géolocalisation constitue « une ingérence dans la vie privée ».

De plus, la CNIL a rendu un avis par une délibération du 19 décembre 2013, à l'occasion des débats parlementaires en cours sur le projet de loi relatif à la géolocalisation, dans lequel elle rappelle que l'utilisation de dispositifs de géolocalisation est très sensible au regard des libertés individuelles et s'apparente donc à une interception du contenu des communications électroniques. Ces dispositifs doivent présenter des garanties en matière de contrôle et de protection des libertés individuelles[47].

Or, aujourd'hui on assiste à une rapidité de l'adoption des services faisant appel à la géolocalisation. En effet, les usages se sont répandus à un rythme inédit essentiellement du fait de la généralisation des smartphones et la proportion des français utilisant des services ayant recours à la géolocalisation est très importante[48]. Par ailleurs, cette pratique est devenue un graal pour les spécialistes du e-commerce car elle permet d'accroitre la pertinence des propositions commerciales faites

[44]FAGET M., *Les réseaux sociaux en ligne et la vie privée*, mémoire master 2 Droit du multimédia et de l'informatique, Université Paris II – Panthéon-Assas, 2008, p.46

[45]« La protection des données personnelles : une source de préoccupation des internautes selon le 3e baromètre de la confiance des français dans le numérique », http://www.cnil.fr/

[46]DERIEUX (E) et GRANCHET (A)., « Réseaux sociaux en ligne : Aspects juridiques et déontologique », *Lamy Axe droit*, 2013, p. 165

[47]Projet de loi relatif à la géolocalisation : la CNIL publie son avis à la demande de la Commission des lois de l'Assemblée nationale, 11 février 2014, http://www.cnil.fr/

[48]Vie privée à l'horizon 2020, paroles d'experts, cahier IP, innovation et prospective de la CNIL, p.21, http://www.cnil.fr/

aux internautes. Elle pourrait par ailleurs devenir permanente car les services innovants exigeront systématiquement d'avoir recours à cette utilisation. Dans quelques années, nous serons certainement obligés de nous localiser pour avoir accès à certains services, tels que les taxis. Le problème réside dans la trace des données des utilisateurs et le traitement qui y sera effectué.

À noter que la géolocalisation n'est pas seulement subie puisqu'elle permet également de se localiser soi même sur un réseau social indiquant dans quel lieu où on se trouve en temps réel. Un phénomène pour finalement se mettre en scène et afficher une activité attractive qui entraine des fils de conversation autour du lieu ou de l'expérience. Il sera très facile d'en déduire des événements et habitudes de vie. Là aussi, nos données dévoilées sur le réseau social peuvent être par la suite captées et traitées pour une réutilisation commerciale.

La géolocalisation est passée en quelques années d'un acte exceptionnel à un acte quasi-quotidien. Cette généralisation se traduit actuellement par un degré d'acception plus important de ces technologies par les internautes. Et refuser d'être géolocalisé risque de devenir prochainement synonyme d'incivilité. Pour autant, les utilisateurs seraient sans doute gênés s'ils savaient à quel point les données obtenues grâce à la géolocalisation sont facilement transférables à certains acteurs. Avec la géolocalisation permanente, il sera beaucoup plus facile de sanctuariser les données. Si elles sont captées, enregistrées, elles pourront être diffusées et stockées dans l'hébergement en ligne puis transmises à des tiers, représentant un grand défi pour la protection de la vie privée[49].

Les données obtenues par les pratiques du profilage, du scoring ou de la géolocalisation sont par la suite stockées dans ce que l'on appelle le cloud, hébergement en ligne et même encore le Big data.

Ce big data fait référence avant tout à l'explosion du volume des données massives dans l'entreprise et des nouveaux moyens technologiques pour y répondre. Cet ensemble est tellement volumineux qu'il est difficile de le traiter avec des outils classiques. Il constitue donc le stockage de données se trouvant sur différents supports et produites en temps réel ou non depuis n'importe quelle zone géographique dans le monde. Les entreprises y ont recours afin de collecter et traiter toutes les données qu'elles détiennent sur leurs clients. Le Big data favorise le « comportementalisme numérique[50] puisqu'il permet de classifier les personnes en fonction des risques et des opportunités qu'elles représentent[51].

Ainsi, la remarque essentielle qui ressort des pratiques de la commercialisation des données par les opérateurs réside dans le fait que les données personnelles, bien qu'elles disposent d'une valeur d'usage, représentent également une forte valeur économique, portant régulièrement atteinte aux libertés des internautes.

Du fait de ces nouvelles pratiques mises en place par les administrateurs de réseaux sociaux, on voit dès lors émerger de nouvelles revendications de la part des internautes.

2§. L'émergence de nouvelles demandes

Il est vrai qu'à mesure qu'internet vampirise le monde, les inquiétudes se généralisent et on assiste alors à des contestations d'utilisateurs citoyens. En effet, les internautes réclament tout d'abord la préservation de leur vie personnelle. Les données personnelles reflètent toutes les infor-

[49]Vie privée à l'horizon 2020, paroles d'experts, cahier IP, innovation et prospective de la CNIL, p.23, http://www.cnil.fr/
[50]Vie privée à l'horizon 2020, paroles d'experts, cahier IP, innovation et prospective de la CNIL, p.20, http://www.cnil.fr/
[51]FILIPPONE D., « Qu'est-ce que le Big data ? », http://www.journaldunet.com/

mations relatives à la vie privée puisque certaines mentionnent l'identité mais également les habitudes, les goûts, les convictions, les modes de vie, l'orientation sexuelle, etc, et l'utilisation de ces données sans le consentement des utilisateurs constitue une atteinte à la vie privée. C'est la raison pour laquelle 75% des internautes disent vouloir refuser la géolocalisation puisque les services ayant recours à cette technique utilisent les données de localisation afin de les réutilisées, marque d'intrusion dans la vie personnelle des utilisateurs.

Les internautes réclament également un renforcement de la confiance qu'ils accordent aux administrateurs puisqu'aujourd'hui c'est l'argument majeur pour rejoindre un réseau social, c'est ce qui va faire qu'un internaute va décider de s'inscrire ou non sur le site. La confiance dans l'utilisation des données prime avant toute chose et c'est pour cela qu'elle doit être renforcée. Les utilisateurs doivent avoir le sentiment de maitriser la circulation de leurs informations.

Cette confiance se caractérise par une sécurisation des données personnelles en ce sens que les internautes ont besoin de s'assurer qu'aucun usage abusif n'est fait de leurs données, qu'aucune consultation par des tiers ne peut être possible. Aujourd'hui, seuls 34% des internautes ont confiance dans l'hébergement en ligne du cloud et les craintes qui ressortent sont liées à l'éventuelle perte de leurs données,[52] tandis que 73% s'inquiètent que d'autres personnes puissent avoir accès et utiliser leurs photos[53].

Cette sécurité des données passe également par la transparence des informations. En effet, les utilisateurs ont la volonté de connaitre la destination de leurs données une fois qu'elles sont sur un réseau social, ainsi que la volonté de savoir si les opérateurs respectent vraiment leurs engagements. Tant de revendications qui donnent lieu à des demandes concrètes et qui doivent être prises en compte par les administrateurs des sites.

En effet, les utilisateurs étant de plus en plus avertis des enjeux de la commercialisation des données personnelles, ils sont donc davantage sensibles à l'utilisation de celles-ci. Ils demandent aux opérateurs un renforcement du système de confidentialité ainsi qu'une simplification des critères puisqu'un grand nombre d'utilisateurs, désireux de contrôler son image numérique, souhaiterait paramétrer ses informations mais trouve cela encore trop complexe et trop difficile à comprendre. En effet, seuls 31% des internautes déclarent bien connaître ces paramètres et 60% pensent qu'ils ne leur procurent pas le niveau de confidentialité souhaité[54].

Aujourd'hui, ce système de paramétrage n'est pas encore suffisant malgré les volontés exprimées par la direction de Facebook, mais qui a cependant refusé d'instaurer un réglage par défaut totalement protecteur, réservant les données aux seuls « amis », comme l'avaient réclamé les CNIL européennes. La visibilité participe au rayonnement du réseau social et de ses possibilités commerciales, ce qui explique la réticence de Facebook. La confidentialité accordée aux utilisateurs n'est donc pas encore au point et pire encore la possibilité de verrouillage ultime du profil sur Facebook a été supprimée récemment. En l'espace de quelques années, le nombre des critères sur le réseau social a bondi, laissant ses membres désemparés ou débutants à la merci du regard public. En effet, sans réglage on peut retrouver le profil d'une personne par un moteur de recherche très facilement. Facebook est de plus en plus critiqué, on lui reproche un manque de transparence[55].

La demande tend donc vers une meilleure visibilité et accessibilité du système de paramétrage. De ce fait, on observe aujourd'hui un rapport de force entre les internautes et les opérateurs puisque les premiers deviennent actifs face aux seconds et les demandes de règles claires se font

[52]« La protection des données personnelles : une source de préoccupation des internautes selon le 3e baromètre de la confiance des français dans le numérique », http://www.cnil.fr/

[53]Etude TNS Sofres du 12 décembre 2012, « Publication des photos sur Internet : Comment partager sans se sur exposer ? », http://www.tns-sofres.com/

[54]Etude TNS Sofres du 12 décembre 2012, « Publication des photos sur Internet : Comment partager sans se sur exposer ? », http://www.tns-sofres.com/

[55]GABIZON C., « Les français veulent préserver leur vie privée », http://www.lefigaro.fr/

plus pressantes. Présente pour protéger les internautes, la CNIL soutient ces demandes en préconisant des informations à la disposition des utilisateurs pour leur expliquer les bonnes pratiques, tout comme le G29 qui considère que l'utilisateur n'est pas suffisamment averti que trop de paramètres permettant à d'autres personnes d'accéder à sont profil sont définis par défaut[56].

A ceci s'ajoute le fait que les internautes souhaiteraient également un renforcement des obligations de sécurité et d'information qui incombent aux opérateurs auprès de leurs abonnés dans les contrats d'engagement. En effet, si l'on sait que les administrateurs sont liés par des obligations protectrices des utilisateurs, la pratique montre qu'elles ne sont pas très contraignantes ou en tout cas peu respectées. La sécurité des internautes devrait pourtant primer avant tout, tout comme l'obligation d'information relative à l'utilisation des données personnelles. Mais si les opérateurs tentent de faire croire qu'ils les respectent, on sait qu'ils ont tendance à les oublier car elles limitent la pratique du traitement des informations. Il serait bon alors que ces obligations deviennent des pratiques légales pour palier le manque de confiance. D'ailleurs, le G29, dans son avis de juin 2009 avait déjà recommandé que les utilisateurs soient clairement informés des conditions d'utilisation de leurs données et des conséquences qui en résultent pour leur vie privée. Seulement, l'ensemble des règles réclamées par les CNIL européennes n'est toujours pas respecté, c'est pourquoi les internautes, du fait de toutes ces prises de conscience, ont modifié leurs habitudes.

D'après le troisième baromètre de la confiance des français dans le numérique, la protection des données personnelles est devenue une source de préoccupation importante pour les internautes français. Informés par les médias et les pouvoirs publics, les français ont davantage connaissance des risques liés au traitement des données personnelles. En effet, aujourd'hui il y a un travail d'éducation en direction des jeunes utilisateurs qui auraient tendance à trop s'exposer sur les réseaux sociaux.

On voit donc peu à peu émerger de nouvelles stratégies de la part d'internautes qui tentent de faire évoluer leurs comportements du fait des nouveaux usages du numérique. Ainsi, pour se prémunir contre les risques, les utilisateurs refusent de plus en plus de communiquer des informations sur leur vie personnelle puisqu'ils ne sont plus que 35% à le faire. Essayer de régler avec soin des paramètres de confidentialité devient également une pratique courante, 77% des utilisateurs affirment avoir modifié au moins une fois leurs paramètres sur Facebook[57]. Enfin, protéger son identité en donnant volontairement de fausses informations ou en ayant recours au pseudonymat sur les réseaux sociaux est une des méthodes utilisées afin d'échapper à la diffusion d'informations personnelles. Dès lors, on observe que les utilisateurs tentent d'anticiper les risques liés au traitement des données personnelles puisqu'ils ont connaissance des pratiques opérées par les administrateurs des réseaux sociaux. Aujourd'hui, l'internaute a tendance à agir en tant que citoyen du net responsable, en tant qu'utilisateur actif et non plus passif. Cependant, même si les attitudes évoluent, il n'en reste pas moins que les risques auxquels s'exposent les abonnées des réseaux sociaux sont de plus en plus croissants et qu'une véritable éducation doit être mise en œuvre afin de les prévenir.

Même si les utilisateurs ont conscience des dangers et tentent d'adapter leur comportement en fonction de ceux-ci, c'est également aux opérateurs d'agir en assurant plus de confidentialité et de protection des données. C'est la raison pour laquelle, les opérateurs, ayant conscience de la méfiance des internautes, ont mis en place des obligations contractuelles pour les rassurer.

[56] Avis du 12 juin 2009 sur les règles applicables aux réseaux sociaux, http://www.cnil.fr/

[57] « La protection des données personnelles : une source de préoccupation des internautes selon le 3e baromètre de la confiance des français dans le numérique », http://www.cnil.fr/

Section II : Une responsabilité pour établir la confiance des utilisateurs

Si c'est la confiance qui est recherchée par les utilisateurs, celle-ci doit s'établir notamment par désignation de responsables(s) en cas de problèmes divers. Les utilisateurs auront besoin d'un instrument légal leur permettant d'appuyer leurs revendications et ainsi faire valoir leurs droits. Le contrat va non seulement devoir lister des rappels des différents droits offerts aux utilisateurs et également des responsabilités envers ceux-ci.

§1 Les engagements contractuels comme base légale de toute revendication

Les droits reconnus sont indispensables pour construire une bonne relation contractuelle. Le contrat va devoir comporter des mentions obligatoires, mais également des obligations spécifiques à l'utilisation du réseau social. Ces obligations contractuelles vont se traduire par des conditions d'utilisation des services offerts par le réseau social et de ce fait des responsabilités de la part des utilisateurs.[58]

Les données fournies sur les réseaux sociaux par les utilisateurs, font l'objet d'une protection légale mais qui est responsable de l'utilisation de celle-ci ? Le responsable du traitement des données est définit comme « la personne, l'autorité publique, le service, l'organisme qui détermine les finalités et les moyens dudit traitement ».

Les données personnelles doivent faire l'objet d'un traitement afin que celles-ci bénéficient d'un régime de protection légale. Ce traitement désigne un responsable par la loi de 1978, cependant il existe des difficultés d'application liées au critère territorial des serveurs où sont traitées ces données.[59] Pour que soit engager la responsabilité au regard du droit français, les données doivent avoir fait l'objet de traitement sur le territoire français ou que le responsable de traitement soit établi en France. Dans le cadre des réseaux sociaux cela va dépendre de la détermination du responsable ou sous-responsable du traitement des données.

Le responsable du traitement doit procéder à un rappel explicite des obligations légales du responsable des traitements des données à caractère personnel : conservation, consentement préalable, finalité des traitements

En droit français, il existe des droits relatifs aux données personnelles confinés dans la loi Informatique et libertés de 1978. Cependant, il n'existe pas de protection des données personnelles spécifique aux réseaux sociaux. Les réseaux sociaux étant d'origine américaine pour la plupart, ils sont soumis aux principes du Safe Harbor ou Sphère de sécurité. Cependant en cas de non respect de ces droits, le Code pénal français énumère des sanctions passibles pour l'auteur des infractions liées aux données personnelles. Les réseaux sociaux ont l'obligation de rappeler dans leur contrat, les différents droits des individus inscrits à leurs services.

La notion de propriété est le fondement de toute revendication. Les réseaux sociaux ont l'obligation d'intégrer la mention et la détermination du propriétaire des données. C'est cette notion de propriété, qui va conditionner la mise en œuvre des droits accordés aux utilisateurs.

[58]Exemple Déclaration des droits et des responsabilités disponible sur Facebook
[59]Article 3 loi « Informatique et Libertés » du 6 janvier 1978

Le respect des données personnelles est englobé dans une forme particulière de respect de la vie privée. Sur les réseaux sociaux, il ne faut pas entendre le droit au respect de la vie privée, de la même manière que l'entend le droit civil. Avec l'apparition des nouvelles technologies et plus particulièrement celles afférentes aux réseaux sociaux, il est nécessaire de délimiter une nouvelle forme de protection des données personnelles. Comment répondre à ces nouvelles exigences ? On assiste à une nouvelle forme de protection de la vie privée, le concept du « privacy by design »[60].

Ce concept d'origine canadien apparu dans les années 90, signifie que la protection des données doit se faire dès la conception technologique ou protection intégrée de la vie privée (PIVP). Les données personnelles vont faire l'objet d'une protection par anticipation. Cette conception spécifique de la vie privée doit satisfaire à sept principes : [61] Ce concept doit faire partie intégrante du régime légal de protection des données personnelles. Le considérant 46 de la directive du 23 novembre 1995 comporte des exigences de protection semblables dès la conception. L'article 23 du prochain projet de règlement européen devrait toute fois imposer ce concept de manière explicite.

Cette nouvelle forme de protection va s'accompagner également d'une forme de responsabilité sous l'appellation américaine « accountability ». Cette responsabilité devant être assumée par le responsable du traitement des données va nécessiter des nouveaux engagements de la part de ces derniers. Les données personnelles vont être protégées par anticipation. Cela va nécessiter des nouveaux engagements de la part des opérateurs des réseaux sociaux et ainsi renforcer la loyauté et la confiance envers leurs utilisateurs.

Il est apparu nécessaire de concilier les principes du Safe Harbor avec les directives européennes sur la protection des données personnelles. Les principes du Safe Harbor ont été considérés comme offrant une protection adéquate quant aux données personnelles dans un accord conclu entre les Etats-unis et l'UE. Les exigences du Safe Harbor doivent répondre à sept principes.

Cependant, la législation européenne semble impuissante et inadaptées à la nouvelle ère numérique. C'est pourquoi une réévaluation des principes du Safe Harbor est à l'étude. Le projet de règlement européen, comporte en effet treize recommandations visant à renforcer l'efficacité de l'accord.[62] Récemment, la Commission européenne a indiqué que les principes du Safe Harbor doivent évoluer et faire l'objet d'une révision afin de devenir « sûrs ».[63]

La directive de 1995, prône la libre circulation des données. Ce qui signifie que le transfert de données à l'étranger est possible, sous conditions : il faut tenir compte du lieu d'accessibilité des informations, ainsi que lieu du principal établissement. La CNIL s'oppose a cette dernière conditions au motif qu'il faut prendre en compte la nationalité du plaignant.

Récemment, il émane une proposition non plus de la libre circulation des données personnelles au niveau mondial, mais vers un « espace Schengen des données personnelles ».[64]

Les obligations contractuelles imposent une obligation de mettre à disposition un système de paramétrage pour le compte des utilisateurs (obligations contractuelles) et une confidentialité des données (engagements vis-à-vis des utilisateurs).

Mais afin de garantir la transparence et une certaine loyauté envers les utilisateurs, les réseaux sociaux vont permettre aux utilisateurs de « contrôler » leurs données par l'intermédiaire d'outils de

[60]Concept canadien apparu dans les années 90
[61]CAVOUKIAN A., « Privacy by design The 7 Foundation Principles »
[62]« La Commission européenne définit les moyens de renouer la confiance dans la protection des données transférées aux Usa »
[63]AFP, « Données personnelles : Viviane Reidig critique l'accord avec les Etats-Unis », <www.lemonde.fr>
[64]KALLENBRON G., « Prism : Thierry Breton propose un espace Schengen des données personnelles »

paramétrages de leur compte. Ce contrôle doit être intégré aux services des réseaux sociaux et cette possibilité doit figurer dans les conditions contractuelles notamment dans les règles de confidentialité. Mais ce seront aux internautes de « verrouiller » leurs comptes et ainsi de sécuriser au mieux leurs données. Il apparaît dans les conditions générales d'utilisation des services, que l'usager doit sécuriser son compte. Il est le propriétaire de ses données et de ce qui se fera sur son compte, il est par conséquent responsable de son utilisation. Une limite cependant à cette responsabilité tient aux cas de piratage du compte utilisé à des fins frauduleuses.

Avec le futur règlement européen sur la protection des données personnelles, de nouveaux droits seront consacrés. Il s'agira notamment d'un droit d'opposition au profilage, d'un droit à la portabilité des données et surtout d'un droit à l'oubli et à l'effacement. Ces derniers, devront être intégrés de manière explicite dans les futures conditions d'utilisation des réseaux sociaux.[65]

L'accord contractuel constitue donc la clé de voûte du contrat car le consentement de l'utilisateur va être nécessaire à la formation du contrat. La souscription à tout service doit nécessiter le consentement de la part des utilisateurs. Sur internet et plus particulièrement pour les réseaux sociaux, il est indispensable de mettre en place un système de consentement préalable dit « opt-in ». Celui-ci doit être actif, c'est-à-dire qu'il va nécessiter une action de la part de l'utilisateur par exemple cocher la case correspondante de façon volontaire.

Lorsque l'on veut utiliser un réseau social, celui-ci doit proposer à chaque étape le consentement de l'internaute. Avec le développement des nouvelles applications toujours plus nombreuses, les internautes utilisent de plus en plus de service intégrés aux réseaux sociaux. Google est un parfait exemple de détournement du consentement des utilisateurs. À la souscription d'un compte Gmail, un compte Google+ est automatiquement créé et des informations sont rendues obligatoirement publiques.[66]

Il est important de respecter la notion de consentement « libre et éclairé ». Il est primordial de comprendre ce qui va être fait de nos données personnelles. Que ce soit Facebook, Google, ou encore Twitter l'articulation des conditions générales d'utilisation des réseaux sociaux, est extrêmement lourde et complexe. L'utilisateur est alors noyé dans des conditions contractuelles confuses, difficile de lecture. À cela on doit ajouter, les mauvaises traductions, qui dénaturent la mesure ou les clauses correspondantes.

En cas de non respect des obligations contractuelles, qui est compétent ? Quel juge ? Quel est le droit applicable ? La loi applicable de principe est la loi contractuelle.

En l'occurrence, la loi américaine aura vocation à s'appliquer. Cette dernière est beaucoup moins contraignante en ce qui concerne le traitement des données à caractère personnel, que celle que nous connaissons en France ou Europe. Certaines juridictions nationales ont déjà tenté de contrecarrer les effets de telles clauses, par exemple la Cour d'appel de Pau qui a considéré le 23 mars 2012 que les tribunaux français étaient compétents car la clause de juridiction imposée par Facebook n'est pas spécifiée de façon suffisamment apparente.

Plus récemment, le réseau social Twitter a fait l'objet d'une ordonnance le 23 janvier 2013, afin de se plier aux exigences de retraits de contenus antisémites. La responsabilité de Twitter en

[65]Voir communiqué article 17 du projet de règlement européen sur la protection des données personnelles <www.europa.par.eu>

[66]« Google la dernière technique de Google pour accroitre le nombre d'utilisateurs, <www.zdnet.fr> ttp://www.zdnet.fr/actualgoogle-la-derniere-technique-de-google-pour-accro-tre-le-nombre-d-utilisateurs-39767759.htm

tant qu'hébergeur le soumet donc aux règles applicables au statut prévu par la loi LCEN du 21 juin 2004.[67] Un point important mérite une attention particulière concernant une autre affaire celle de l' « oiseau bleu », qui a mit en exergue la question de la propriété intellectuelle des tweets de ses utilisateurs. Ceux-ci auraient été revendus pour 250 millions de dollars, des données liées aux tweets auraient ainsi été exploitées sans le consentement des utilisateurs.[68]

On s'aperçoit que les pouvoirs de sanctions offerts à la CNIL ne sont pas suffisamment puissants pour faire reculer les géants des réseaux sociaux. Il se crée alors un besoin urgent d'adaptation du cadre législatif. Certes, des sanctions sont prévues en cas de manquement aux obligations de protection des données personnelles mais celles-ci sont en réalité inadaptées aux nouveaux phénomènes.

Google a écopé en France d'une amende record de 150000€ soit le maximum autorisé par la CNIL. En outre, si l'on compare cette amende avec le chiffre d'affaires cette somme est totalement dérisoire. Elle ne produira pas un effet dissuasif assez important pour éviter de tels comportements. C'est pourquoi le futur projet de règlement européen à reçu plusieurs amendements afin d'adapter les sanctions aux géants des réseaux sociaux. Ce montant pourra atteindre 100 millions d'euros et 5 % du chiffre d'affaires mondial de l'entreprise.[69]

Cette idée se calque avec ce qui se fait déjà en matière de législation en droit de la concurrence, ce qui inciterait sans doute à une réflexion avant d'agir. Le souhait de la Commission européenne est d'harmoniser la législation européenne et éviter qu'un pays membre de l'Union européenne bénéficie de lois plus protectrices qu'un autre.

Il convient d'étudier comment la confiance peut influer sur les conditions contractuelles. Les réseaux sociaux ont tout intérêt à faire preuve de transparence afin de gagner la confiance des utilisateurs. En effet celle-ci garantira aux réseaux sociaux de conserver leurs « clients ».

§2 La confiance comme influence dans les relations contractuelles

Max Schrems, étudiant autrichien va lancer les hostilités en 2011, en annonçant avoir déposé plainte contre Facebook au motif que le réseau social ne respecte tout simplement pas la législation européenne sur la protection des données personnelles. Le groupe de militants « Europa vs facebook » a fait état de dizaines de plaintes déposées devant le Commissaire à la protection des données, dénonçant de multiples atteintes au respect de la protection des données personnelles.[70] Le contrat passé entre le réseau social et ses utilisateurs sera la base légale sur laquelle les militants pourront s'appuyer.

Les utilisateurs découvrent les scandales liés à leurs données personnelles via les médias ou encore des associations de consommateurs tels qu'UFC que choisir. Les médias s'empressent de révéler chaque nouveau scandale lié aux données personnelles sur les réseaux sociaux. Il devient quasiment impossible de ne pas savoir ce qui se passe concernant données. Profilage, commercialisation, fuite de nos données, tout est dénoncé.

Lorsque l'utilisateur va prendre connaissance que ces données vont être vendues ou être utilisées dans un but auquel il n'a pas consenti, cela va donner lieu à des contestations dans l'espérance de mettre un terme à la volonté du réseau social. Par exemple, Facebook a dû faire marche arrière

[67]Article 6 de Loi pour la confiance dans l'économie numérique 21 juin 2004
[68]MAUREL L., « Twitter vend vos 140 caractères »
[69]Article 23 alinéa 1er du Projet de règlement européen sur la protection des données personnelles
[70]Plaintes déposées par le groupe de militants « Europa Vs Facebook »

après avoir modifié ses conditions d'utilisations en toute discrétion. Elles prévoyaient notamment la propriété et la conservation des droits sur les contenus supprimés.[71]

Le réseau social spécialisé dans le partage de photos, Instagram, a évoqué le souhait de vendre les photos publiées par les utilisateurs, ce qui n'a pas manqué de susciter une vive réaction de leurs parts. En conséquence, Instagram a décidé de faire machine arrière et de renoncer à la vente initialement prévue. Car lorsqu'un réseau social émet le souhait de mettre en place une nouvelle pratique, il doit l'intégrer de manière explicite dans le contrat.

Les dispositifs de paramétrage et de sécurisation de compte vont être améliorés. Il y aura ainsi, plus de fonctionnalités, plus de paramètres offerts aux utilisateurs. De plus, les internautes vont recevoir des informations sur l'utilisation des paramètres de contrôle. On s'aperçoit que les réseaux sociaux sont plus protecteurs de la vie privée. Cela passe également par un renforcement des contrôles de paramétrages des comptes.

Les nouvelles fonctionnalités intégrées aux réseaux sociaux permettent de partager et diffuser toujours plus de contenus, qui vont nécessiter un plus grand contrôle des informations fournies par les utilisateurs. Des clauses contractuelles solides permettraient d'anticiper les risques juridiques et éviter de nombreux contentieux se regroupant autour de ceux-ci. Il a été démontré l'efficacité de la technologie Deepface de Facebook, mais aussi de sa potentielle dangerosité pour les données personnelles des individus.[72]

L'influence peut s'observer également par le biais des autorités européennes (g29) ou encore des autorités nationales. C'est le cas notamment de la CNIL qui a exigé d'ajuster les paramètres de confidentialité à législation française. Des pays comme l'Allemagne ont posés des ultimatums lourds de conséquences pour les réseaux sociaux .L'Allemagne a été très active dans l'influence du comportement des réseaux sociaux envers ses utilisateurs. En effet, Facebook constamment visé par les autorités allemandes, a du renoncer à certaines fonctionnalités, et annuler certaines de ses clauses contractuelles.[73] Il existe un décalage entre ce qui est prévu par le contrat et la pratique des administrateurs des réseaux sociaux. Les réseaux sociaux vont alors procéder à des modifications contractuelles notamment dans les politiques de confidentialité. Les réseaux sociaux prônent de plus en plus qu'ils font des efforts afin de garantir une transparence vis-à-vis de leurs utilisateurs. Certes, on assiste à une protection plus efficace et les réseaux sociaux font preuve de plus de transparence à l'instar de Twitter.[74]

La CNIL a notamment souligné que les réseaux sociaux se sont penchés sur les inquiétudes de leurs utilisateurs, et vont donc les informer des modifications prises en considération. Mais cela va conduire à une multiplication des conditions contractuelles et contraintes pour les utilisateurs. Les internautes ne vont pas à chaque modification prendre le temps nécessaire de les consulter ou bien de les comprendre. L'intégration des différents services et applications engendrent également une modification contractuelle. Toujours plus de conditions, qui ne sont toujours pas clairement établies. Les utilisateurs et les scandales révélés vont pousser les opérateurs des réseaux sociaux à modifier leurs conditions d'utilisation ainsi que leur politique de confidentialité et par conséquent de leur contrat. Bien, que les modifications aient été effectuées, le nombre grandissant de modification dans le fond ne suivent pas les modifications contractuelles dans la forme. Néanmoins, ces modifications sont décidées unilatéralement par les réseaux sociaux. Les utilisateurs ne peuvent plus exprimer leurs revendications comme cela était prévu par exemple sur Facebook et son droit de vote.

[71]NOISETTE T., « Conditions d'utilisation : Facebook recule sous les critiques », <www.zndet.fr>
[72]GRANDONI D., « Deep Face, le nouveau système de reconnaissance faciale de Facebook qui fait froid dans le dos », <www.huffingpost.fr>
[73]Voir « Déclaration des droits et responsabilités » section 17§3
[74]GALLET L. « Données personnelles : Twitter classé premier sur la transparence

Il existe cependant, un revers dans ces modifications contractuelles. Bien que les utilisateurs en exprimant leur mécontentement, poussent les opérateurs à reculer, ceux-ci font preuve d'une certaine hypocrisie. Lorsque nous entrons dans les détails de ces conditions d'utilisations, nous pouvons lire que par le contrat les inscrits consentent à une autorisation d'utilisation des données fournies pour une rémunération des opérateurs des réseaux sociaux. Avec bien sur aucune contre-partie pour l'utilisateur.[75]

Les réseaux sociaux se cachent derrière une responsabilité limitée quant au résultat attendu et quant au traitement des données personnelles. Il en résulte selon eux, une simple obligation de moyen, ce qui les décharge de toute responsabilité en cas de défaillance ou d'anomalie. Alors non seulement, les prérogatives des réseaux sociaux, sont renforcées, mais ces modifications, se font en toute discrétion, l'utilisateur n'étant pas suffisamment informé de la « mise à jour » des conditions d'utilisation. Google, comme les autres réseaux sociaux, recommandent aux utilisateurs de prendre connaissance des modifications. Cependant, cela devrait être une obligation et non plus une simple suggestion.[76]

Les réseaux sociaux par modification contractuelle, vont effectuer de nouvelles limitations de responsabilité. Facebook a récemment introduit de nouvelles modifications des conditions d'utilisations, qui lui octroient d'importantes prérogatives à l'usage commercial des données personnelles.[77] Pour exemple on peut citer la référence présente dans les conditions d'utilisation de Google. Une surprise apparaît, les conditions d'utilisation sont rédigées en minuscule contrairement à la section « Responsabilité pour nos services » qui sont écrites en majuscules.

Suite à la condamnation, de Google par la CNIL, on pourrait éventuellement s'attendre à une nouvelle modification de la politique de confidentialité ainsi que des clauses contractuelles. Mais ce changement tardif cache en réalité de nouvelles trahisons envers les utilisateurs. Récemment Google, est accusé de procéder à un scanner des données personnelles des étudiants utilisant une application des services Google.[78] L'UFC a également assigné Facebook, Google +, ainsi que Twitter sur le terrain contractuel et notamment des clauses abusives. L'illisibilité, l'incompréhension, la désorganisation des conditions contractuelles sont des problèmes perpétuels auxquels les réseaux sociaux semblent bien, ne pas vouloir remédier. Dernièrement, Facebook est accusé de conserver les messages non postés de ses usagers, en l'absence de tout consentement de leur part. Le problème se pose au niveau de l'autocensure des messages par les internautes, qui n'ont pas souhaité partager le « contenu ». De plus, la charte d'utilisation du réseau social ne fait aucune mention à cette possibilité. Facebook se défend au motif de mesurer la confiance de ses utilisateurs.

La multiplication de nouvelles fonctionnalités et de logiciels pose des sérieux problèmes d'afflux de données massives et de risques de fuites quant à l'exploitation de données personnelles. Les services de plusieurs réseaux sociaux peuvent fusionner, notamment après un rachat. De ce fait, de nombreuses données personnelles vont faire l'objet de croisement. C'est le cas de Facebook et d'Instagram, qui ont dû procéder tous deux à des modifications respectives de leurs conditions d'utilisations. Or, comme le souligne la société EPIC, ces modifications « augmenteraient les risques concernant la vie privée des utilisateurs », de plus, elles présentent un caractère contraire à la loi. Les réseaux sociaux s'appuient sur des abus de « spam et autres » et ont le souci de protéger

[75]Conditions d'utilisations « Déclaration des droits et responsabilité » section 17
[76]Voir les conditions d'utilisation de Google « Règles et principes »
[77]KALLENBORN G., « Facebook : levée de boucliers contre l'usage commercial de données privées »,< www.01net.com>
[78]De Maréschal E., « Google accusé de fouiller les données personnelles des étudiants », www.etudiant.lefigaro.fr>

leurs utilisateurs face à ces pratiques.[79] Les nouveaux logiciels et autres technologies vont utilisés les données personnelles des utilisateurs comme des ressources. On s'aperçoit que des données sont intégrées au moteur de recherche interne à l'instar de Graph Search de Facebook.[80] LA CNIL met en place des tutoriels et émet régulièrement des mises en garde contre les risquent qu'un tel service engendre.

Enfin il existe une nouvelle influence majeure sur le projet de règlement européen : le lobbying des réseaux sociaux. Ce lobby va s'exercer par des propositions de nouveaux amendements sur le règlement européen de la protection des données personnelles. Les amendements au projet de règlement européen sur la protection des données personnelles sont nombreux. Mais ils sont pour la plupart, dus à la pression exercée par les géants américains et notamment les réseaux sociaux américains. En effet, ils n'ont pas intérêt à ce que la protection soit nettement renforcée car l'enjeu économique est extrêmement important. Ils ont explicitement exposés leur souhait de voir abaisser le niveau de protection européen.[81]La Commission européenne a jugé utile d'adopter une communication sur les transferts de données transatlantiques afin de rétablir la confiance des citoyens et plus particulièrement des usagers des réseaux sociaux. Ce communiqué définit les six grands objectifs que s'est fixé la Commission européenne.[82]

Pour en conclure, « La vie privée est devenue un luxe » sur les réseaux sociaux. Allez-vous y renoncer ou êtes-vous prêt à agir?[83]

[79]ŒILLET (A), « Instagram et Facebook : des données partagées dès janvier », <www.clubic.com>
[80]SOYEZ F., « Le Graph Search de Facebook : le paradis des stalkers », <www.cnetfrance.fr>
[81]« La protection des données personnelles freinée par les lobbies » <acteurspublics.com>
[82]Voir le communiqué « Rebuilding Trustin EU-US data flows" <ec.europa.eu/justice/>
[83]Antonio Casineli

BIBLIOGRAPHIE

Ouvrages généraux et spécialisés

Cours dispensé par Jean Frayssinet de Droit des technologies de l'information et de la communication.

DERIEUX (E) et GRANCHET (A). « Réseaux sociaux en ligne : Aspects juridiques et déontologique », *Lamy Axe droit*, 2013.

FAGET M., *Les réseaux sociaux en ligne et la vie privé*, mémoire master 2 Droit du multimédia et de l'informatique, Université Paris II – Panthéon-Assas, 2008.

Revues, Articles

Cahiers IP Innovation et prospective de la CNIL « Vie privée à l'horizon 2020 ».

CNIL, « Journée d'études vie privée 2020 : quelle vision pour la protection des données personnelles de demain », 2012, Paris.

Codes

Code Civil

Code Pénal

Sites Internet

Site officiel de la Cour de cassation : www.courdecassation.fr

Site officiel de Légifrance : www.legifrance.gouv.fr

Site officiel de la CNIL : www.cnil.fr

Site officiel du Figaro : www.figaro.fr

Site officiel du Monde : www.lemonde.fr

Site officiels des Acteurs Publics : www.acteurspublics.com

Site officiel informatique et libertés : www.cil.cnrs.fr/

Site officie de Clubic : www.clubic.com

Site officiel Cnet France: www.cnetfrance.fr

Facebook: www.facebook.com

Google : www.google.fr

Journal du net : www.journaldunet.com

Site officiel Le monde informatique : www.lemondeinformatique

Site officiel de Libération : www.liberation.fr

Site officiel PC Inpact : www.pcinpact.com

Site officiel ZDNet : www.zdnet.fr

Site officiel de La Tribune : www.latribune.fr

Site officiel 01Net : www.01net.com

Site officiel Association UFC-Que-Choisir : www.quechoisir.org

Site de droit de l'Union européenne : http://eur-lex.europa.eu

Site de diffusion du droit par l'Internet : http://www.legifrance.gouv.fr

Site d’actualité de l'internet et du marché IT : http://www.zdnet.fr/actualites

Site de France Info : http://www.franceinfo.fr

Site de l’IREDIC : http://junon.univ-cezanne.fr

Site du journal d'information américain « The Huffington Post » : http://www.huffingtonpost.fr

Site de la communauté des professions du Droit : http://www.village-justice.com

HADOPI : http://www.hadopi.fr/

Éducation au numérique : http://www.educnum2014.fr/

ACSEL : http://www.acsel.asso.fr/

TNS- SOFRES : http://www.tns-sofres.com/

WALTER J.-P. « Le profilage des individus à l’heure du cyberespace : un défi pour le respect du droit à la protection des données » : http://www.coe.int/

TABLE DES MATIERES