INSTITUT DE RECHERCHE ET D'ÉTUDES EN DROIT DE L'INFORMATION ET DE LA COMMUNICATION

LE DROIT FRANÇAIS À L'ÉPREUVE DE L'USURPATION D'IDENTITÉ EN LIGNE

Mémoire de fin d'Études réalisé par Mademoiselle CASAS Marina

Sous la direction de Monsieur MOURON Philippe

Master II Droit des Médias et des Télécommunications

Année Universitaire 2013-2014

Aix-en-Provence

REMERCIEMENTS

« Les grands criminels portent avec eux une espèce de prédestination qui leur fait surmonter tous les obstacles, qui les fait échapper à tous les dangers, jusqu'au moment que la Providence, lassée, a marqué pour l'écueil de leur fortune impie. »

Les Trois Mousquetaires (1844)

Alexandre Dumas

En guise de préambule, je tenais à remercier l'ensemble du corps de l'Institut de Recherche et d'Études en Droit de l'Information et de la Communication pour les enseignements et les conseils apportés tout au long du cursus de master II.

Je tenais en outre, à remercier particulièrement Monsieur Philippe Mouron, pour son écoute et son attention afin de m'aider au mieux dans mes travaux de recherche.

Une pensée particulière pour Madame Garnier Marine et Monsieur Drillot Alan, pour m'avoir soutenu dans ce travail de réflexion.

LISTE DES ABRÉVIATIONS

Al. :	Alinéa
Ann. :	Annexe
A.N. :	Assemblée Nationale
ARSS :	Actes de la recherche en sciences sociales
Art. :	Article
CCC :	Cahiers du Conseil Constitutionnel
C. Civ. :	Code civil
C. pén. :	Code pénal
CA. :	Cour d'Appel
CAEET :	Commission des affaires économiques, de l'environnement et du territoire
Cass :	Cour de Cassation
Cass. Civ. :	Chambre civile de la Cour de Cassation
Cass. Com. :	Chambre commerciale de la Cour de Cassation
Cass. Soc. :	Chambre sociale de la Cour de Cassation
CEDH :	Cour Européenne des Droits de l'Homme
CMF :	Code monétaire et financier
CNDS :	Commission nationale de déontologie de la sécurité
CNIL :	Commission Nationale Informatique et Libertés
Coll. :	Collection

Cons. Const. :	Conseil Constitutionnel
Conv. EDH :	Convention Européenne des Droits de l'Homme
CPI :	Code de la propriété intellectuelle
CP :	Code pénal
c/ :	Contre
d. :	Décret
D. :	Dalloz
Déb. parl. :	Débat parlementaire
Dir. :	Directive
Doc. parl. :	Document parlementaire
DPSPFE :	Droit public et de la science politique en France et à l'étranger
Éd. :	Édition
Email :	*Electronic mail*
FAI :	Fournisseur d'accès à Internet
Gaz. Pal. *:*	Gazette du Palais
HADOPI :	Haute Autorité pour la diffusion des œuvres et la protection des Droits sur Internet
Ibid. :	Au même endroit
INSEE :	Institut national de la statistique et des études économiques
IP :	*Internet Protocol*
L. :	Loi
LDPA :	Lamy droit pénal des affaires
LCEN :	Loi pour la confiance dans l'économie numérique

LGDJ :	Librairie générale de droit et de jurisprudence
LOPSI :	Loi d'orientation et de programmation pour la sécurité intérieure
LOPPSI :	Loi d'orientation et de programmation pour la performance de la sécurité intérieure
LSI :	Loi pour la sécurité de l'information
LSQ :	Loi pour la sécurité quotidienne
n° :	Numéro
NCCC :	Nouveaux cahiers du Conseil Constitutionnel
OCDE :	Organisation de coopération et de développement économique
OCLCTIC :	Office de lutte contre la criminalité liée aux technologies de l'information et de la communication
Op. cit. :	Dans l'ouvrage cité
OSCP :	Observatoire de la sécurité des cartes de paiement
p. :	Page
PA :	Les Petites Affiches
PUF :	Presses universitaires de France
QE :	Question écrite
Rép. civ. :	Répertoire de droit civil
Rép. min. :	Réponse ministérielle
RLDC :	Revue Lamy droit civil
RLDI :	Revue Lamy Droit de l'Immatériel
S. :	Sénat
SACEM :	Société des auteurs, compositeurs et éditeurs de musique

SAFARI :	Système automatisé pour les fichiers administratifs et le répertoire des Individus
SCPP :	Société civile des producteurs phonographiques
TGI :	Tribunal de Grande Instance
UE :	Union Européenne
v. :	voir
vol. :	volume

SOMMAIRE

INTRODUCTION

« La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires. » Colin Rose.

La consécration d'Internet dans le début des années 2000, et l'éclosion des réseaux sociaux dix ans plus tard ont favorisé le développement de véritables nouvelles pratiques 2.0, de sorte qu'aujourd'hui, ces éléments électroniques font parties de notre vie quotidienne. La preuve d'un tel ancrage dans nos mœurs se voit principalement dans les fondements mêmes qui construisent une société : d'une part, au regard de la population il serait difficile de constater que nul n'utilise les communications électroniques quotidiennement. En effet, que cela soit pour se connecter sur les réseaux sociaux, écrire un courriel, ou même encore acheter un bien sur un site, les communications électroniques ont pris d'assaut notre mode de vie, et ont su par là-même se rendre indispensables au sein de la vie quotidienne.

En outre, en raison de la nature transfrontalière de ces communications, les États ont vu dans ces dernières une véritable aubaine pour le développement de l'économie[1]. Enfin, le dernier socle sur lequel repose les fondements d'une société réside dans la législation. En effet, le droit constitue les règles de conduite que chaque personne doit respecter. Auquel cas, cette dernière serait sanctionnée par les textes. Internet a donc été l'objet de toutes les convoitises par les professionnels du droit, dans la mesure où ces derniers ont vu dans les communications électroniques un potentiel en raison du fait qu'elles ne connaissent pas de limites géographiques matérialisées, et dématérialisées.

Ces raisons ont conduit les Etats à consacrer plusieurs libertés fondamentales au sein de ces communications : liberté de circulation des biens et des marchandises, liberté d'expression, chère à la Cour Européenne des droits de l'Homme, liberté de création et de pensée etc. En d'autres termes, la plupart des Etats, et notamment les Etats européens ont fait des

[1] CHAWKI (M.), « Essai sur la notion de cybercriminalité », juillet 2006, pp. 2-3, *pdf*, disponible sur : http://www.ie-ei.eu/IE-EI/Ressources/file/biblio/cybercrime.pdf

communications électroniques, de véritables espaces privilégiés dans lesquels les droits fondamentaux peuvent s'épanouir inéluctablement.

L'effervescence des réseaux sociaux a d'ailleurs accentué cette idée de liberté, notamment en ce qui concerne la liberté d'expression. De fait, ces mêmes réseaux sociaux constituent aujourd'hui les fervents défenseurs de cette liberté, dans la mesure où celle-ci est devenue au fil des années, un véritable principe fondamental auquel il est difficile possible de porter atteinte. En effet, la Cour Européenne des droits de l'Homme avait entre autre dès 1976 considéré que la liberté d'expression constitue « l'un des fondements essentiels dans une société démocratique.[2] »

Néanmoins, résumer la protection des communications électroniques par le biais du principe fondamental de la liberté d'expression ne serait que le fait de s'enfermer dans des idéologies utopiques. En effet, en raison de sa nature transfrontière, les États ont très vite compris que ces mêmes communications pouvaient également avoir des effets dévastateurs sur la vie quotidienne des citoyens. La proclamation d'une protection générale, voire quasi absolue de cette liberté peut laisser place à l'effet inverse que celui désiré par la Cour Européenne des droits de l'Homme. Le nombre d'utilisateurs des communications électroniques peut s'avérer être le vecteur d'abus qu'il serait possible de constater sur celles-ci.

Les États comme le législateur, ont ainsi maintes fois rappelé qu'Internet ne constituait pas une « zone de non-droit[3] », et il a paru indispensable de l'encadrer afin d'éviter toute sorte de pratique visant à porter atteinte aux libertés individuelles. Le caractère mondial de ce dernier peut rapidement amener au constat d'une globalisation de pratiques frauduleuses, que les États ne seraient plus à même de pouvoir réprimer. Par ailleurs, l'émergence de l'aspect technologique de ces mêmes communications pose également de nouveaux défis pour les législations dans la mesure où cette nature peut devenir un outil d'atteinte aux personnes redoutable[4].

[2]CEDH, Handyside c/ Royaume-Uni, 7 décembre 1976.
[3]DUPUY-BUSSON (S.), « La liberté d'expression sur Internet : les réseaux sociaux (Facebook, Twitter...) ne sont pas des zones de non-droit », *LPA*, 15 juil. 2010, n°140, p. 10.
[4]TÜRK (P.), « La souveraineté des États à l'épreuve d'Internet », *DPSPFE*, 1er nov. 2013, n°6, p. 1489.

En effet, la pleine consécration de la liberté d'expression a engendré la reconnaissance d'autres principes devenus fondamentaux comme la liberté d'information, auxquels les États ne peuvent y porter atteinte qu'en cas de respect à l'ordre public.

Or, ces nouveaux principes doivent aujourd'hui se confronter avec les nouvelles technologies en raison du caractère technique des communications électroniques. Considérés comme de véritables outils de promotion de ces libertés, il a été crée à cet effet la notion de « nouvelles technologies de l'Information et de la Communication. » Toutefois, le constat de l'importance des nouvelles technologies dans les mœurs peut également faire l'objet d'une certaine remise en cause : ces dernières peuvent en effet, également s'avérer être de véritables armes, dont l'objectif serait de porter atteinte aux droits et aux libertés individuelles.

Le danger d'Internet et des communications en ligne, réside dès lors dans l'association que des personnes mal attentionnées peuvent faire entre les nouvelles technologies, et le caractère transfrontalier d'Internet. Cette idée se traduit notamment par l'émergence d'une nouvelle forme de délinquance à l'échelle mondiale : la cybercriminalité. Cette criminalité 2.0 pose de sérieuses inquiétudes aujourd'hui, aussi bien pour les citoyens, que pour les Etats eux-mêmes. En effet, le danger de la cybercriminalité réside dans le fait qu'elle puisse tout individu. La cybercriminalité se traduit aujourd'hui, par la volonté des législations de réprimer les abus qu'elle engendre[5]. En effet, chacun d'entre nous est devenu aujourd'hui une victime potentielle de cette nouvelle forme de criminalité.

L'évolution rapide des nouvelles technologies, allant de paire avec la prolifération des pratiques frauduleuses sur les communications électroniques a mis la législation au pied d'un mur qu'elle ne saurait affronter. En effet, si les États sont amenés à légiférer sur cette question, ces derniers doivent avant tout innover, dans la mesure où l'apparition de ces nouvelles formes de fraude a crée de toute pièce un vide juridique en la matière puisque les États ne disposaient pas de textes visant à réprimer spécialement ce type d'infractions. Pourtant, l'apparition de nouvelles notions, comme notamment « les données à caractère personnel », concept issu des années 90, aurait du mettre la puce à l'oreille de la norme sur la possibilité de voir un jour, la présence de pratiques aux effets d'une bombe. Ce manque déconcertant d'anticipation est aujourd'hui l'une des raisons pour lesquelles le droit lutte

[5] BRIAT (M.), « La cybercriminalité », *LPA*, 6 févr. 2004, n°27, p. 25.

difficilement contre ce phénomène de cybercriminalité. Eu égard en effet, aux enjeux que supposent l'utilisation des communications en ligne, il est étonnant de constater le défaut de l'existence d'un droit spécifique à Internet.[6]

L'heure est à la coopération internationale, ainsi qu'à l'harmonisation et la modernisation des législations pour lutter contre la cybercriminalité. Le problème, c'est que les Etats ne sont pas dotés de textes de lutte efficaces, dans la mesure où l'incrimination et la répression des actes de cybercriminalité dépendent pour l'essentiel, de droits déjà existants, et qui n'avaient pas vocation à l'origine de s'appliquer à ces ceux-ci.

L'usurpation d'identité met en exergue à elle seule toutes ces problématiques. Phénomène florissant, notamment depuis le début des années 2000, l'usurpation d'identité est devenue aujourd'hui l'un des objectifs majeurs des États. La raison de telles inquiétudes, tient au fait notamment que cette forme de criminalité 2.0 peut toucher chacun d'entre nous. En effet, elle peut tantôt concerner une personne physique, tantôt une personne morale, que l'Administration elle-même. Notion difficile à saisir pour les législations, ce délit constitue aujourd'hui le talon d'Achille des États.

En effet, à l'heure où les communications électroniques sont devenues de véritables outils du quotidien, l'usurpation d'identité se prolifère de manière plus aisée grâce à la banalisation de ces outils au sein de notre vie quotidienne. L'évolution toujours plus rapide des moyens d'atteinte aux personnes demeure aujourd'hui, le principal souci de la législation pour lutter contre l'usurpation d'identité.

En France, de façon étonnante le constat est le même. Alors que le pays des Droits de l'Homme avait pourtant fait l'objet de modèle en matière d'innovation dès 1974 lorsque la question des données à caractère personnel a vu le jour, ce dernier fait preuve aujourd'hui d'une grande sclérosité.

[6]ARRIGO (P.), « La cybercriminalité : vers une régulation internationale de l'Internet ? », *Gaz. Pal.*, 16 oct. 2001, n°289, p. 35.

L'objectif de ce travail de réflexion sera ainsi de comprendre les raisons pour lesquelles la France lutte difficilement contre l'usurpation d'identité.

Á ce titre, la question à laquelle nous essayerons de répondre est celle de savoir comment le droit appréhende-t-il ce délit et plus précisément, il conviendra d'analyser quelles sont les armes de lutte mises à la disposition pour ce dernier. En d'autres termes, la problématique générale portera sur la question suivante *: comment le droit peut-il lutter contre l'usurpation d'identité* ?

Cette question conduit à l'étude de deux réflexions : la première, concerne d'une manière générale, le dispositif législatif mis en place pour lutter contre cette infraction (Première Partie). À ce titre, il sera possible de constater, que l'usurpation d'identité est devenue un enjeu de taille pour le droit. En effet, alors que ce phénomène criminel tend à se développer, voire à se proliférer, le droit reste impuissant face à cela. Il éprouve en effet, des difficultés à appréhender ce délit. Les raisons d'une telle difficile appréhension, réside principalement dans le fait que la notion principale d'identité ne fait l'objet d'aucune définition légale, alors même qu'elle constitue la clef de voûte du délit d'usurpation d'identité. (Chapitre 1).

Cet engrenage juridique est donc à l'origine, lié au défaut de mentions légales de l'identité. Rappelons en effet, que la répression des délits et des crimes se fait par le biais du droit pénal. Or, celui-ci tend au respect de plusieurs principes, et notamment celui d'interprétation stricte de la loi pénale. Comment peut-on imaginer une quelconque répression efficace, alors même que ce principe tend à respecter de façon littérale le dispositif mis en place. Or, si la définition de l'identité n'existe pas, comment est-il possible de réprimer une infraction qui lui porte atteinte ?

Outre ce manque de cohérence, la difficulté pour le droit de lutter contre ce délit, tient également au fait que l'identité revêt aujourd'hui diverses formes ; de sorte qu'il est possible de parler à son égard d' « identité 2.0. » Or, en l'absence de règles spécifiques en la matière, le droit s'est borné à se référer au droit commun, et principalement aux droits fondamentaux pour réprimer des infractions relatives à l'usurpation. (Chapitre 2.)

Or, il sera possible de constater que le recours à d'autres infractions tend à scléroser le droit dans son carcan juridique. L'aspect fondamental de cette notion, rend davantage complexe une lutte efficace contre l'usurpation dans la mesure où les juges doivent faire face à un

dilemme cornélien entre plusieurs droits fondamentaux qui entrent par là-même en conflit. La mise en balance de ces droits fait non seulement perdre du temps dans l'acquisition d'un dispositif de lutte performant, mais également il laisse à supposer que la législation française connait de profondes lacunes juridiques, vidant par là même de toute substance le droit.

En outre, l'impossible lutte contre ce délit réside également dans le fait que les moyens techniques utilisés pour usurper une identité progressent plus vite, que l'adoption successive de lois à l'initiative du Parlement. (Seconde partie.)

Afin d'illustrer cette idée, il sera possible de constater que le recours aux droits fondamentaux dans la lutte contre cette infraction provoque en réalité un cercle vicieux. En effet, l'usurpation d'identité, en ce qu'elle est considérée comme étant un moyen technique d'atteinte aux droits fondamentaux laisse place à un large panel de dispositifs législatifs qui ont vocation à lui être applicables. Or, l'absence de droit spécifique en la matière engendre en réalité des problèmes de cohérence de droit, dans la mesure où il est difficile réellement de savoir quel dispositif sera le plus à même pour lutter contre des atteintes aux droits patrimoniaux d'une part, et aux droits extrapatrimoniaux d'autre part (Chapitre 1).

Pour palier à son manque d'effectivité, il sera possible de noter que le droit a crée de toute pièce un nouveau délit d'usurpation d'identité. Or, ces propos sont à nuancer car nous verrons que ces tentatives d'innovation ne peuvent connaitre un succès considérable dans la mesure où les techniques de fraudes évoluent toujours plus vite, et deviennent de plus en plus performantes. De fait, le droit, et plus généralement les individus, font appel à la technique elle-même en guise de solution de lutte contre l'usurpation. (Chapitre 2.)

Première partie.

L'usurpation d'identité : un enjeu juridique de taille pour le droit

L'histoire du droit démontre que celui-ci a fait l'objet tantôt de conceptions divergentes, tantôt de conceptions communes. Néanmoins, une définition unanime du droit le décrit comme étant un « ensemble de règles de conduite socialement édictées et sanctionnées qui s'imposent aux membres de la société.[7] » Si la définition du droit est aujourd'hui formelle, en revanche, son efficacité est sans cesse remise en cause. L'usurpation d'identité met en exergue cette idée : composé de normes visant à encadrer les actions des individus afin d'assurer leur protection ou, *a contrario*, de les sanctionner, le droit doit avant tout définir formellement les normes qu'il convient d'appliquer afin de remplir ces objectifs.

Or, l'existence d'une définition de l'identité fait défaut. À l'heure où le développement des communications électroniques est à son apogée, le droit doit une nouvelle fois faire ses preuves. L'usurpation d'identité en ligne remet incontestablement en doute son efficacité dans cette lutte, en raison du fait qu'il ne prend pas en compte le caractère évolutif de l'identité, la privant de toute substance ainsi que d'un arsenal législatif de lutte redoutable au regard de son usurpation.

Cette première approche sera ainsi consacrée à la difficulté pour le droit d'encadrer l'usurpation d'identité en ligne en raison du fait qu'il n'existe pas de définition légale de la notion principale de cette infraction (chapitre 1), provoquant *in fine* des insécurités juridiques en la matière, dans la mesure où, « après tout, on ne peut protéger ce qu'on ne peut définir[8]. »

Outre le défaut de précisions matricielles sur l'identité en ligne, il sera également possible de constater que le droit éprouve des difficultés à encadrer cette notion en raison de sa nature : en effet, l'absence de définition formelle a conduit le droit à opérer une transposition du régime applicable conçu à l'origine pour l'identité personnelle. Or, cette application manque d'effectivité dans la mesure où le dispositif applicable à l'identité issue de la vie réelle n'était

[7] CORNU (G.), *Vocabulaire juridique*, Coll. Puf, 9e éd., 1093 p.
[8] OCDE, « Document exploratoire sur le vol d'identité en ligne », Réunion ministérielle de l'OCDE : le futur de l'économie Internet, organisée à Séoul, Corée, le 17 et 18 juin 2008, DSTI/CP(2007)3/FINAL p. 17, [En ligne] : http://www.oecd.org/fr/sti/40699509.pdf

pas à l'origine conçu pour le caractère pluridimensionnel de l'identité numérique. Il apparait que le caractère fondamental de l'identité numérique, à l'instar de l'identité personnelle, est vecteur de confusion juridique, de sorte que le droit manque d'efficacité dans la lutte contre l'usurpation d'identité en ligne. (Chapitre 2).

Chapitre Premier. L'identité en ligne, clef de voûte de l'usurpation d'identité

Alors qu'il est d'usage en matière juridique de définir au préalable les notions fondamentales d'un sujet donné, le droit n'a pas, de façon étonnante, donné de définition formelle de l'identité, de sorte que le cadre juridique de l'usurpation d'identité ne peut être efficace. Pourtant, le droit essaie tant bien que mal de combler ses lacunes en la matière mais ses tentatives ne sauraient être fonctionnelles aujourd'hui, dans la mesure où il n'existe toujours pas à ce jour, de définition formelle de l'identité.

Il est possible néanmoins de donner plusieurs explications de cette lacune, notamment si l'on prend en compte l'évolution des moyens de communication voire des communications elles-mêmes par lesquelles l'identité revêt une double casquette. La confrontation de la vie réelle et de la vie virtuelle a ainsi donné naissance à plusieurs formes de l'identité : l'identité personnelle issue de la vie courante, et l'identité en ligne ou numérique, directement conçue par et pour la vie virtuelle.

Cette dichotomie a mis le législateur et le juge face à une réalité complexe, de sorte qu'ils se sont retrouvés démunis de toute arme législative efficace pour encadrer cette notion. En raison d'une volonté de garder un contrôle *a minima* sur l'identité des personnes et sur tout support confondu de communication, les professionnels du droit ont dès lors transposé le dispositif classique qui trouve à s'appliquer en matière d'identité personnelle à l'identité numérique. Or, il conviendra de constater que l'adaptation du dispositif classique de l'identité a renforcé le carcan juridique en la matière parce que celui-ci, n'avait pas à l'origine, vocation à s'appliquer à l'identité en ligne.

Il sera bon d'analyser dans une première approche les raisons pour lesquelles le droit a adapté la conception de l'identité personnelle à l'identité numérique, (section 1) ce qui mènera par la suite à comprendre son manque d'innovation dans la définition légale de l'identité numérique (section 2.)

Section 1 – L'absence de définition légale de l'identité en ligne

L'absence de définition légale de l'identité en ligne peut s'expliquer par différents points : le premier concerne le caractère sclérosé du droit lui-même, qui n'a pas, au fil de ces années, changé de conception sur cette notion.

Or, les évolutions technologiques ont nécessairement fait évoluer la conception de l'identité, de sorte que celle-ci n'est plus réellement centrée autour de l'individu comme le droit a pu le penser par le passé puisqu'elle prend en considération également son aspect social. En outre, cette idée témoigne également du manque d'innovation de la matière juridique sur ce point : parce que celle-ci a conservé une conception « individualiste » de l'identité, c'est-à-dire, portée sur l'individu[9], elle n'a pas retenu les différents composants de l'identité en ligne qui ne reposent plus seulement sur l'individu puisqu'ils portent également sur ses biens. Il est donc nécessaire de distinguer ces deux formes d'identité (paragraphe 1) afin de comprendre les raisons pour lesquelles la conception juridique de l'identité personnelle a du évoluer pour s'appliquer également à l'identité en ligne, provoquant *in fine,* des insécurités juridiques (paragraphe 2.)

Paragraphe 1. La distinction entre l'identité personnelle et l'identité numérique

Il n'est possible de traiter la question de l'usurpation d'identité sans avoir au préalable analysé la notion principale de cette réflexion. Étant donné qu'il est d'usage constant en droit d'analyser les termes du sujet avant même de rentrer dans une démarche de réflexion, il convient dores et déjà de remarquer que la norme définit étonnement l'identité en ligne par une action : l'usurpation. C'est ainsi que le Code pénal, dans son article 226-4-1 définit le délit d'usurpation d'identité comme étant le : « fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération. » Force est de préciser que cette définition légale est ensevelie par des termes imprécis et bien

[9] BRUBAKER (R.), *Au-delà de « l'identité »*, ARSS, 2001, pp. 66-80.

trop larges, n'apportant *de facto* aucune précision sur la notion d'identité elle-même, alors même qu'il s'agit de la clef de voûte de l'incrimination d'une telle infraction.

Le risque d'une définition aussi large, qui pourtant, est considérée aujourd'hui comme étant la norme de référence en matière d'usurpation d'identité, est de voir la mise en œuvre de dispositifs communs, de sorte que ces deux identités seraient généralisées alors qu'elles répondent toutes deux à des régimes juridiques distincts.

De plus, il est important d'opérer une distinction entre ces deux formes dans la mesure où elles ont provoqué elles-mêmes une certaine « crise d'identité des droits de la personnalité.[10] » En effet, l'identité en ligne a remis en question les différentes catégories de ces droits fondamentaux, notamment au regard de leur caractère patrimonial et extrapatrimonial. Par exemple, l'identité personnelle repose à l'origine sur une conception juridique « individualiste », dans le sens où le droit va avoir tendance à protéger les atteintes morales d'une personne, telle que l'atteinte à la vie privée, le droit à l'image, donc sur les droits extrapatrimoniaux de l'individu.

A contrario, l'identité numérique aurait tendance à traiter davantage des droits patrimoniaux dans la mesure où elle se compose d'éléments qui peuvent être vendus ou cédés. On pense par exemple à la commercialisation des noms de domaine, ou encore, à la création d'un site Internet en vue de réaliser du commerce électronique. Or, on constate également que cette séparation, pourtant évidente à première vue, ne l'est pas pour autant si l'on donne une analyse plus poussée de cette idée : les droits extrapatrimoniaux de l'identité personnelle, peuvent devenir avec le temps, des éléments patrimoniaux. On pense ainsi notamment au nom où l'on s'est demandé si ce dernier pouvait faire l'objet d'un droit de propriété.[11] En d'autres termes, la distinction entre l'identité personnelle et l'identité numérique n'est pas chose aisée pour le droit, et pourtant, elle est nécessaire.

Par ailleurs, le défaut de mentions légales à son sujet amène en premier lieu à s'interroger sur le caractère objectif de l'identité. En effet, aucun texte législatif ne donne une définition formelle de cette notion. Celle-ci repose sur plusieurs déclinaisons, aussi différentes des unes et des autres. Or, si l'on devait esquisser les contours de son cadre légal, l'identité personnelle pourrait être considérée comme étant une entité qui regroupe un certain nombre

[10] HASSLER (T.), « La crise d'identité des droits de la personnalité », *LPA*, 7 décembre 2004, n°244, p. 3.
[11] Cass. Civ., 16 mars 1841.

d'informations relatives à une personne, c'est-à-dire des caractères qui rendent l'individu identifiable ou qui donnent la possibilité de l'identifier tel que le nom, le prénom, l'adresse du lieu de domicile, ou encore la date de naissance. En d'autres termes, tous les éléments qui constituent l'état civil d'une personne dans la vie réelle.

Or, il s'agit vraisemblablement d'éléments objectifs - dans la mesure où ils permettent l'identification d'une personne – alors que la notion d'identité est, quant à elle, subjective. Cette subjectivité est sans nul doute la cause d'une certaine insécurité juridique qui engendre plusieurs difficultés pour le droit d'en donner une définition officielle.

Enfin, le développement de ce que l'on résume vulgairement à Internet et des nouveaux modes de communication a bouleversé nos modes de vie. Ce bouleversement a en effet non seulement changé les pratiques quotidiennes en matière d'échange d'informations au sein des dites communications, mais il a également été un facteur de nouveaux risques pour la personne et ses droits fondamentaux[12]. Aussi, l'identité telle que le droit l'appréhendait dans la vie réelle s'est vue transformée par ces évolutions technologiques. Il en découle de cette évolution que l'identité a fini par revêtir plusieurs formes sur les communications électroniques, de sorte qu'il existe aujourd'hui, aussi bien l'identité classique issue de l'état civil que l'identité numérique, composée quant à elle des éléments classiques de l'état civil, mais également de nouveaux composants.

Ainsi, afin de bien distinguer l'identité personnelle de l'identité numérique, qui ont toutes deux vocation à s'exprimer sur les supports de communication en ligne, il conviendra de les généraliser par le biais de l'expression « identité(s) en ligne ». Ces aspects dénotent la nécessaire définition formelle de l'identité en ligne, afin d'éviter d'une part, toute confusion juridique, et d'autre part, toute insécurité juridique. Une hypothèse peut très bien résumer le contexte actuel du vide juridique en la matière : en effet, comment le droit peut-il protéger l'identité alors même qu'il est dans l'incapacité de saisir cette notion ?

Afin de comprendre davantage l'intérêt de différencier ces deux aspects, il convient d'analyser la retranscription de la conception juridique de l'identité personnelle à l'identité numérique.

[12] FALQUE-PIERROTIN (I.), « La Constitution et l'Internet », *NCCC*, 1er juin 2012, n° 36, p. 31.

Paragraphe 2. La conception juridique de l'identité personnelle

Bien que l'identité *lato sensu* ne fasse pas l'objet d'une définition formelle, il est tout de même possible d'en dessiner les contours, dans la mesure où ce terme ne fait pas l'objet d'une définition mais de plusieurs.

Certains philosophes en effet, rattachent l'identité à la vie sociale, c'est-à-dire que celle-ci aurait vocation à être collective. Ainsi, Jean-Paul Sartre, grand Humaniste, a-t-il dit que : « *l'enfer, c'est les autres*. »[13] Cela signifie qu'il reconnait que l'identité puisse être influencée par le regard que porte autrui sur soi. Pour d'autres penseurs, le critère du collectif constitue une forme réelle de l'identité. Ainsi, selon Monsieur Lamizet Bernard, professeur en sciences de l'information et de la communication, la vie sociale permet-elle de distinguer l'identité personnelle de l'identité virtuelle.[14] Pour lui, en effet, les sciences de l'information et de la communication ont favorisé la création de cette nouvelle facette de l'identité dans la mesure où celle-ci se rattache avant tout aux personnes qui nous entourent. Cette forme d'identité culturelle, évolue avec le temps, et, du fait de l'apparition des nouveaux supports de communication, a du, elle aussi, s'adapter aux faits culturels et sociaux.

Cette approche que l'on pourrait qualifier de « collective » est certes, évidente puisque toute personne se construit grâce à l'environnement. Mais force est de constater que d'un point de vue juridique, cet aspect collectif n'est pas le critère retenu. En effet, le droit a dès le départ adopté une conception essentialiste de l'identité[15]. Cela signifie que la norme est restée figée pour l'essentiel sur l'individu. Cette idée démontre d'autre part les raisons pour lesquelles le droit a effectué une adaptation classique des normes aux supports de communication électronique : c'est effectivement parce qu'il a un regard individualiste porté sur l'identité que celui-ci s'est attardé à utiliser les droits de la personnalité comme normes de référence pour réprimer l'usurpation.

[13] SARTRE (J.P.), *Huis Clos* suivi de *Les mouches*, Coll. Folio, éd. 2000, 245 p.
[14] LAMIZET (B.), *Politique et identité*, Coll. Puf, éd. 2002, p. 32-33.
[15] VASSEUR-LAMBRY (F.), « L'identité de la personne humaine », *LPA*, 6 mai 2004.

Par ailleurs, la conception juridique de l'identité personnelle se voit également en matière de répression en droit pénal, dans la mesure où la législation entend réprimer une infraction commise par un individu ou par un groupe. Or, le juge doit opérer une interprétation au cas par cas. L'exemple le plus probant de cette idée est sans nul doute le principe d'interprétation stricte de la loi pénale : outre le respect par le juge d'une interprétation rigoureuse de la loi, ce principe tend à différencier les différents justiciables coupables d'une infraction. C'est ainsi qu'il existe les qualifications pénales « d'auteur », de « co-auteur » ou encore de « complice. » Ces qualifications distinctes des unes des autres permettent de sanctionner les individus selon la gravité de leurs actes, et donc, de manière casuistique.

A contrario, lorsqu'un délit est commis en groupe, comme par exemple le vol en réunion, celui-ci ne suffit pas à lui seul pour constituer un délit, et on parle d'ailleurs à ce propos, de « circonstance aggravante ». En d'autres termes, la tâche est bien trop hasardeuse pour la norme de réprimer les individus dans leur ensemble. Cet exemple concret donne ainsi la possibilité de comprendre les lacunes de la législation : le droit a en effet tendance à prendre en compte seulement l'identité personnelle, ou les atteintes portées à ses droits fondamentaux, afin de lui garder un contrôle plus aisé sur les individus.

Gérard Cornu quant à lui poursuit ce même ordre d'idées puisqu'il définit l'identité comme : « ce qui fait qu'une personne est elle-même et non une autre ; par extension, ce qui permet de la reconnaître et de la distinguer des autres; l'individualité de chacun, par extension, l'ensemble des caractères qui permettent de l'identifier ».[16] De fait, cette définition se rapproche incontestablement de la description de l'état civil, à savoir que ce dernier peut s'entendre comme : « l'ensemble des éléments relatifs à la personne qui identifient un individu. »[17] L'état civil comprend ainsi le nom, le prénom, la date et le lieu de naissance, la date de décès, ou encore le lieu du domicile et cette série d'éléments permet de constituer l'identité d'une personne[18]. Le recensement de ces identifiants se fait par le biais de l'administration[19] ce qui lui permet entre autre d'avoir un véritable contrôle sur notre identité.

[16] CORNU (G.), Vocabulaire juridique, Coll. Puf, 9e éd., 1093 p.
[17] « État civil », Juritravail, [En ligne] : http://www.juritravail.com/lexique/Etatcivil.html
[18] COURBE (P.), *Droit civil, les personnes, la famille, les incapacités*, D., 7è éd., 2009, pp. 18-29.
[19] D. n°65-422 du 1er juin 1965 portant création d'un service central d'état civil au ministère des affaires étrangères.

Pour illustrer davantage la main mise des pouvoirs publics sur notre identité personnelle, il convient de rappeler que l'état civil fait l'objet d'un véritable service public.[20] En d'autres termes, la notion d'état civil étant proche de celle de l'identité personnelle, a, sans doute, laissé supposer au législateur, qu'il ne semblait pas opportun de définir très précisément ce qu'était l'identité.

Section 2 – La nécessaire définition de l'identité en ligne, gage de protection juridique des droits fondamentaux

L'application de la conception juridique de l'identité personnelle à l'identité en ligne ne semble pas surprenante dans la mesure où le caractère pluridimensionnel de l'identité en ligne aurait du inciter la loi à définir de façon précise ces deux volets.

Paragraphe 1. L'absence de définition légale de l'identité numérique

Le défaut de définition de l'identité conduit naturellement à l'absence de précisions sur les composants de l'identité en ligne. Or, il apparait aujourd'hui nécessaire de définir cette notion dans la mesure où l'identité en ligne peut tout aussi bien concerner d'une part, les personnes physiques que les personnes morales, et d'autre part, faire l'objet de différences selon qu'il s'agisse du monde réel ou du monde virtuel. À l'heure où Internet est à son apogée, et que les réseaux sociaux ont envahi nos modes de vie, la notion d'identité numérique est devenue toute aussi importante que l'identité classique. Par conséquent, l'évolution des nouvelles technologies de l'information et de la communication doit aller de paire avec la prise en compte par le droit de l'évolution de l'identité en ligne puisque les moyens d'utilisation de celle-ci ont évolué dans le même temps.

Cependant, il est possible d'apporter un début de définition si on analyse les éléments qui composent l'état civil. Ainsi, l'identité numérique s'entend-t-elle comme l'identification d'une personne grâce aux identifiants classiques mais aussi grâce à des nouveaux composants tels que le profil utilisé sur les réseaux sociaux, le pseudonyme, les articles rédigés puis

[20] INSEE , « Fichiers état civil », disponible sur : http://www.insee.fr/fr/publics/collectivites/fichier_etat_civil_pdf/IGREC.pdf

publiés sur des blogs, l'adresse IP, ou encore, le courrier électronique[21]. En d'autres termes, l'identité numérique englobe un large panel de composants : aussi bien ceux qui sont considérés comme étant de nouveaux procédés d'identification, spécifiques au monde numérique, que d'éléments qui composent l'identité personnelle. La diversité de l'identité numérique rend *in fine* une application du droit davantage complexe car ce dernier doit faire face aux nouvelles pratiques sur ces supports.

Cette forme d'identité est également un bel exemple de l'obligation pour le législateur de devoir s'adapter aux évolutions culturelles et sociales d'une société. Il est apparu à ce titre, que l'identité en ligne ne pouvait être caractérisée seulement par des éléments biologiques ou physiques d'une personne[22]. En effet, alors que la genèse de cette nouvelle notion réside dans la volonté du législateur d'adapter l'identité réelle aux nouveaux modes de communication, l'identité numérique ne doit plus, et n'aurait jamais du, être vue comme le complément de l'identité personnelle mais comme une « identité de référence ».[23]

Par ailleurs, l'hétérogénéité de l'identité en ligne accentue la difficulté de cerner ses contours. Par exemple, l'émergence des réseaux sociaux a provoqué la mise en avant de la réputation d'une personne physique ou morale ou encore, la consécration du principe de la liberté d'expression, de sorte que le caractère spontané des publications constitue un composant de notre identité en ligne à part entière. En d'autres termes, le droit a du s'adapter et changer sa conception essentialiste de l'identité afin de prendre en compte les différentes facettes de l'identité en ligne ainsi que l'aspect social qui en découle naturellement.

Pourtant, la question de l'identité numérique s'est posée bien avant l'apparition florissante des réseaux sociaux. Celle-ci avait déjà remis en cause la vision individuelle de l'identité tenue par le législateur. En effet, en 1974, une affaire au cœur de l'actualité défraie la colère des français. Il s'agit du projet « SAFARI », acronyme pour désigner le système automatisé pour les fichiers administratifs et le répertoire des individus. Il s'agissait d'un projet du Gouvernement visant à interconnecter tous les fichiers de l'Administration par un numéro INSEE, en vue d'identifier tous les citoyens par un identifiant unique. La question d'un élément d'identification unique avait fait réagir l'opinion publique, qui criait à la manipulation de leurs données personnelles. Le journal *Le Monde*, avait publié un article le 21

[21] ERTZSCHEID (O.), *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies*, Marseille OpenEdition Press, 2013, pp.13-18 [En ligne] : http://books.openedition.org/oep/332

[22] BENSOUSSAN (A.), « Vers la consécration de l'identité numérique », *Gaz. Pal.*, 23 avril 2011, n°113, p. 3.

[23] FILLIAS (E.), VILLENEUVE (A.), *E-Réputation, Stratégies d'influence sur Internet*, Coll. Ellipses, p. 54.

mars 1974 intitulé : « Safari ou la chasse aux Français »[24] dans lequel il mettait en évidence les dangers susceptibles d'être encourus pour nos libertés individuelles face à cette centralisation de fichiers. L'informatique, alors encore un secteur peu connu provoquait de la crainte des citoyens. Le projet de cet identifiant unique, géré et contrôlé par une administration électronique a été rejeté. Ce rejet a d'ailleurs été à l'origine de la loi Informatique et Libertés du 6 janvier 1978 afin de protéger les données personnelles par une structure ad hoc indépendante : la Commission Nationale Informatique et Libertés. (CNIL).

La question de l'identifiant unique s'est par la suite posée en 2002, une sorte de retour masqué au projet SAFARI rejeté quelques années plus tôt. Le discours prononcé par Michel Sapin, alors ministre de la fonction publique et de la réforme de l'État, à l'occasion de la remise du rapport intitulé : « Administration électronique et protection des données personnelles » en février 2002, a révélé explicitement le problème du critère individualiste de l'identité retenu par le droit.[25] Ce discours est d'ailleurs connu aujourd'hui pour cette raison. Ce dernier a en effet précisé que : « l'identité numérique n'est pas, et ne peut pas être unique, pas plus que l'identité au sens traditionnel des relations "papier" avec l'administration. De la même façon que nous disposons aujourd'hui, entre autres, d'un numéro de sécurité sociale, d'un numéro fiscal, d'une carte d'identité, d'un passeport, autant d'identifiants distincts les uns des autres, nous aurons demain plusieurs identifiants électroniques. Ce serait une vision naïve de la numérisation que de croire qu'elle mène naturellement à l'unicité de l'identité. » Ce discours fut révélateur de la prise de conscience sur l'impuissance du droit face aux données personnelles, et plus largement sur la relation de l'identité avec le numérique.

Si on donne une analyse plus poussée de ce projet et de ce discours, on se rend compte que le débat tournait autour de l'administration électronique, ainsi que d'un identifiant unique. Force est d'insister sur la notion « d'identifiant », dans la mesure où un identifiant ne peut, à lui-même, constituer l'identité lato sensu. En 2002, on ne parlait pas d'identité numérique mais d'identifiants numériques. La priorité de l'époque, n'était pas tant de définir l'identité numérique, mais celle de sécuriser nos identifiants sur Internet. Dès lors, il est facilement possible de réaliser que l'enjeu relevait davantage de l'ordre de la technique que du domaine juridique.

[24] V. Ann.
[25] SAPIN (M.), Discours prononcé à l'occasion de la remise du rapport *Administration électronique et protection des données personnelles*, 26 février 2002, [En ligne] : http://www.fonction-publique.gouv.fr/ministre/presse/discours-140

Puis, entre 1990 et le début des années 2000, alors même que la question de la protection de l'identité numérique n'était pas réglée, certaines notions telles que : « l'opt-in » ou « l'opt-out » on fait leur apparition. Rattachées aux identités, il est très aisé de comprendre les difficultés d'interprétations que cela menait. En tout état de cause, au cours de cette décennie, l'identité numérique n'est plus abordée sous l'angle d'identifiants numériques mais plus largement comme étant un « moyen d'identification ». Cette nuance est importante dans la mesure où elle illustre le fait que ce n'est plus l'administration qui contrôle l'identité mais l'utilisateur lui-même.

La création des réseaux sociaux a dès lors accentué la séparation de l'administration et des utilisateurs : l'utilisation massive des réseaux sociaux par les internautes lui a permis d'avoir une entière maitrise sur leur identité. Mais les réseaux sociaux ont également fait apparaitre de nouvelles formes de régulation au travers d'identifiants électroniques tels que l'adresse IP, l'email, ou encore le mot de passe.

L'identité en ligne pose un autre obstacle au législateur en raison du bouleversement des modes d'utilisation des communications électroniques par les internautes. On constate, notamment sur les réseaux sociaux, que les internautes peuvent créer plusieurs profils, gérer plusieurs comptes de sorte qu'en réalité l'identité numérique est susceptible d'en regrouper plusieurs.[26] Outre le fait qu'il n'existe pas de définition formelle de l'identité, le législateur est contraint de faire face à plusieurs identités. Autrement dit, la conception de l'identité personnelle ne trouve plus à s'appliquer aujourd'hui au regard de tous ces enjeux.

Enfin, l'adaptation du dispositif classique relatif à l'état civil cumulé au défaut de définition légale laisse supposer que le législateur a délibérément choisi de ne pas déterminer cette notion, conscient de la complexité du sujet. Cela lui permettant, *a fortiori*, de garder une parfaite maitrise sur les individus.

[26] SCHERER (E.), *La révolution numérique : glossaire*, D., 1ère éd., 2009, p. 20.

Paragraphe 2. L'absence de définition légale de l'identité en ligne : vecteur de confusion juridique

L'identité numérique découle principalement des droits de la personnalité. Sur les réseaux sociaux par exemple, le principe de la liberté d'expression, si cher à la CEDH[27] a eu pour conséquence la consécration du caractère spontané des contenus. Ce caractère spontané traduit non seulement de nouvelles formes de l'identité en ligne, mais surtout, le contrôle des individus eux-mêmes sur leur identité, ou du moins, en apparence. En d'autres termes, il semblerait que le législateur et l'administration, conscients de leur perte de contrôle sur l'identité des administrés, ont essayé de remédier à ce problème : à défaut d'avoir pu créer une définition formelle de l'identité, ces derniers ont cru bon de reconnaitre l'existence d'autres notions autour de celle-ci, comme la notion d'e-réputation ou encore, la création d'un droit à l'oubli afin de garder une maitrise partielle sur les internautes.

Néanmoins, la création de ces notions voisines n'a pas eu l'effet escompté : à l'inverse d'avoir facilité une main mise sur la notion d'identité par la création de notions voisines, la pratique a laissé place à une véritable confusion juridique entre ces différents termes. La naissance de la notion d'« e-réputation » en est une parfaite illustration. Cette confusion juridique a dès lors accentué le fossé entre le monde réel et le monde virtuel dans lequel le droit s'est aventuré. Élément marquant de la volonté du législateur d'évoluer avec les pratiques, force est d'affirmer que la création de nouvelles notions relatives à l'identité ne fait que renforcer le vide juridique en matière d'usurpation.

Par exemple, la notion d'e-réputation conçue de prime abord pour traiter la question de l'image de marque d'une personne morale, et en second plan, d'une personne physique, ne répond pas à la question de savoir ce qu'est l'identité. En effet, pour certains chercheurs, « cette notion n'apparait pas comme une révélation mais plutôt comme une découverte progressive de la technologie et de l'usage qui en est fait par les individus et les entreprises.[28] »

[27] CEDH, 7 décembre 1976, Handyside c/ Royaume-Uni.
[28] FILLIAS (E.), VILLENEUVE (A.), *E-Réputation, Stratégies d'influence sur Internet*, op.cit., pp. 29-31.

Par ailleurs, il est également possible de constater que la doctrine fait une confusion entre l'identité elle-même et l'e-réputation dans le sens où, l'e-réputation constituerait la gestion de l'identité sur Internet.[29] Or, bien que ces deux notions soient proches l'une de l'autre, les rassembler pour former qu'une seule identité ne serait pas tout à fait exact. En effet, l'identité virtuelle nécessite la prise de contrôle de l'individu sur sa propre identité, par le biais de la création d'adresses email dont il choisit le préfixe, de noms de domaine, ou encore de part sa volonté de se créer un ou plusieurs profils sur les réseaux sociaux, tandis que l'identité personnelle repose sur la gestion des données personnelles par une autorité.

Néanmoins, cette idée est à nuancer dans la mesure où la maitrise de l'internaute n'est pas totale : ce dernier garde en réalité le pouvoir sur la forme de son identité, mais il ne peut en revanche, contrôler ses effets et sa destination sur les communications électroniques. Cela signifie que sur lesdits supports de communication, l'internaute laisse des traces de son identité à son insu. Ainsi pour certains, existe-t-il trois dimensions de l'identité numérique.[30]

Madame Georges Fanny, Maître de conférences en Sciences de la communication à l'Université de la Sorbonne, explique qu'il existe trois volets de cette identité : la première réside dans l'identité « déclarative », c'est-à-dire celle que choisit l'internaute et dont il garde le contrôle total. Par exemple, l'internaute choisit d'utiliser un pseudonyme.

La seconde, appelée identité « agissante », permet de renseigner directement sur l'identité de la personne au travers de ses actions : ainsi, sera-t-il possible d'identifier un individu dès lors que ce dernier publiera un contenu sur les réseaux sociaux, ou encore, lorsqu'il s'agira de changer la photo de son profil.

Enfin, la troisième forme de l'identité numérique, appelée identité « calculée », n'est autre que le produit de l'identité agissante, effectué par le système. Dans ce dernier cas, l'identité est associée au nombre d'amis connectés sur les communications du public en ligne, ou encore à la date de dernière connexion. Ces trois dimensions définies par la doctrine permettent de percevoir non seulement le caractère complexe et hétéroclite de l'identité, mais surtout, les différents degrés de la prise de contrôle de l'individu sur sa propre identité.

[29] CAHEN (M.), « Identité numérique après le décès », Disponible sur son blog personnel : http://www.murielle-cahen.com/publications/p_deces-identite.asp
[30] GEORGES (F.), « L'identité numérique dans le web 2.0 », *Le mensuel de l'Université*, n°27, juin 2008, pdf, Disponible sur : http://fannygeorges.free.fr/doc/georgesf_mensueluniversite.pdf

A contrario, l'e-réputation peut être définie comme l'identité d'une marque, d'une personne physique, mais surtout d'une personne morale, pour laquelle la personne morale doit garder le contrôle sur son identité.[31] Ce phénomène s'explique en partie par le fait que l'e-réputation est devenue au fil des années, vulgairement un produit commercial, une marque[32] voire un droit patrimonial alors que l'identité réelle ou numérique, reste au demeurant, une valeur patrimoniale que l'on ne peut ni vendre, ni céder au même titre que les droits de la personnalité.

Cette confusion n'est pas pour autant surprenante, dans la mesure où l'usage a favorisé la création du concept d'e-réputation, tout droit inspiré de l'identité classique, puis de l'identité numérique. Conscient des divers masques de l'identité numérique, la question de l'e-réputation n'était donc pas novatrice. En revanche, ce qui peut paraitre pour le moins étonnant, est en fait l'incertitude qui règne autour des divers composants de l'identité. Rappelons en effet, que la définition légale du délit d'usurpation identité inscrite au Code pénal au sein de son article 226-4-1 traite de ces éléments par la mention de termes généraux. Cet article ainsi rédigé, définit ces composants comme étant : « une ou plusieurs données de toute nature permettant de l'identifier » [le tiers].

Acte volontaire du législateur ou simple maladresse de sa part, une chose est certaine : l'emploi de termes généraux est à l'image de ce que représente l'usurpation d'identité aujourd'hui : c'est-à-dire, un véritable carcan juridique. Le défaut de définition légale de cette notion essentielle a en outre, provoqué des incertitudes sur le statut juridique des éléments qui la composent, de sorte qu'aujourd'hui, un certain nombre d'identifiants numériques font l'objet de vifs débats ; nourrissant davantage les incertitudes qui règnent autour de la notion d'identité.

In fine, ces diverses incertitudes autour de la notion d'identité en ligne marquent définitivement la perte de contrôle des pouvoirs publics sur l'identité lato sensu. L'adaptation des droits de la personnalité aurait pu consacrer l'identité en ligne comme un droit à part entière si ces derniers avaient pris en compte par exemple, son caractère hétérogène. Ce manque de contrôle ouvre alors la porte à divers abus, privant les individus de toute protection efficace..

[31] FILLIAS (E.), VILLENEUVE (A.), *E-Réputation, Stratégies d'influence sur Internet*, op. cit., p. 80.
[32] ERTZSCHEID (O.), *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies*, op. cit., pp. 13-27.

Chapitre Second. L'identité en ligne, clef de voûte des droits fondamentaux au regard de l'usurpation

À l'origine, les attributs de l'identité relevaient principalement de l'état civil. Au regard de l'évolution des mœurs et des pratiques, ces derniers ont par la suite fait l'objet d'une interprétation extensive par les juges de façon à combler certains vides juridiques laissés en l'état. Dès lors, le développement du numérique a remis au goût du jour les divers droits de la personnalité[33]. L'exemple le plus marquant de cette idée est sans nul doute celui des données à caractère personnel. En effet, les données personnelles, sujet de polémique après l'affaire du projet « SAFARI » précédemment analysée, ont été définies de façon audacieuse dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 dans la mesure où la rédaction de ce texte a permis d'englober suffisamment de situations, qu'elles soient actuelles ou à venir.

L'article 2 de la présente loi, définit les données personnelles de la façon suivante : « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.[34]» Bien que les données personnelles soient relatives à la protection d'éléments d'ordre de la vie privée, le point de départ de ces dernières était en revanche, bel et bien la protection des identifiants, et donc, de l'identité.

Cette loi a le mérite d'utiliser des termes suffisamment larges, dont l'inspiration de la rédaction découle directement des droits fondamentaux comme le droit à la vie privée, afin d'englober des situations qui n'étaient pas encore existantes. De facto, la consécration des données personnelles, aurait pu, également, consacrer la notion d'identité et lui donner un cadre juridique à part entière. Par exemple, à l'origine ce dispositif avait vocation à sécuriser les identifiants sous le couvert de l'expression « informations nominatives » et non pas celle

[33] HASSLER (T.), « La crise d'identité des droits de la personnalité », op. cit.
[34] Art. 2 al. 2, L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

de « données à caractère personnel ». L'aspect fondamental des droits de la personnalité est tel, qu'il a été question de changer les termes de la loi. Par ailleurs, un changement significatif sur la notion principale que constitue une donnée à caractère personnelle démontre bien l'instabilité juridique sur cette question. C'est dans la recherche d'une protection plus efficace que cette opération a été effectuée. En effet, consciente des enjeux et des risques liés au traitement et à la conservation des données personnelles, la France a davantage cherché à les protéger de façon efficace : la transposition en 2004 de la Directive européenne de 1995 en la matière, a engendré la modification de l'article 2 de cette loi de sorte que l'expression « informations nominatives » fut remplacée par la notion de « données à caractère personnel »[35].

Autrement dit, ce changement d'expression met en exergue toute la complexité de la notion d'identité personnelle, puisqu'il a été question de modifier les termes de cet article en vue d'éviter des interprétations trop larges ou douteuses. La substitution de ces termes, permet *in fine* d'englober des situations plus larges, de sorte qu'aujourd'hui les données à caractère personnel ne visent pas seulement les éléments d'identification ou encore des « informations nominatives », puisqu'elles sont susceptibles de recouvrir également, des éléments liés à la vie privée. D'autre part, l'adoption de cette loi illustre parfaitement le mécanisme juridique français : l'état du droit positif est sans cesse remanié pour s'adapter aux nouvelles pratiques, à l'instar des juges, qui vont, de leur côté, adopter une interprétation extensive de ces mêmes lois afin de remédier aux problématiques juridiques nouvelles auxquelles ils doivent faire face.

Concernant l'identité, l'article susvisé donne ainsi plusieurs indices, qui ne permettent pas, il est vrai, de la définir en tant que telle mais qui offrent toutefois la possibilité de la comprendre. Selon cet article, une donnée personnelle est : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

Si l'on devait interpréter les termes « directement » et « indirectement », on pourrait supposer que le premier renvoie à tous les éléments directs permettant d'identifier un individu. Ainsi par exemple, cela concernerait tous les composants classiques de cette dernière, tels que le nom, le prénom, la nationalité. Le second quant à lui, pourrait faire référence aux nouveaux

[35] YAYON-DAUVET (A.), « Le devenir de la protection des données personnelles sur Internet », *Gaz. Pal.* 13 sept. 2001, n°256, p. 2.

moyens techniques de communication, comme par exemple, l'anonymat, le profil, ou encore l'adresse IP. Cette seconde hypothèse est davantage renforcée par la suite dudit article qui précise que : « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification. » La portée générale de cette phrase concerne de façon évidente aujourd'hui, l'identité numérique. En d'autres termes, les données à caractère personnel sont une première approche des éléments permettant d'identifier les individus. Néanmoins, il convient de nuancer cette idée : cette première approche ne suffit pas à elle seule pour déterminer les composants de l'identité numérique.

Par ailleurs, il convient de noter qu'il découle du caractère pluridimensionnel des identifiants numériques, l'aspect hétéroclite de cette même identité, de sorte que le droit a du lutter contre un nouvel obstacle juridique. Force est de préciser qu'alors même que la notion d'identité classique est elle-même imprécise et incertaine, nul ne peut douter de la difficulté pour le législateur de définir les composants de l'identité liés au numérique. Ainsi, il n'est pas possible, à l'heure actuelle, de définir tous les identifiants qui s'y rattachent, mais il conviendra toutefois d'analyser les principaux composants. Il convient dès lors de rappeler que le législateur a adapté le schéma de l'identité personnelle issue de l'état civil aux nouveaux supports de communication. Ainsi, nous tenterons essentiellement de nous concentrer autour des notions créées de toute pièce en vue de leur appliquer le dispositif classique. Il s'agira en effet d'analyser la manière dont le législateur a pu appréhender ces nouveaux obstacles juridiques.

Section 1. La protection des composants de l'identité en ligne par les droits fondamentaux

La pluralité des composants de l'identité est incontestable en raison de l'évolution de l'identité personnelle sur les communications électroniques. De surcroit, cette hétérogénéité rend difficile l'application d'un socle juridique efficace. En outre, le paradigme entre la vie réelle et la vie virtuelle n'est pas la seule raison qui rend une difficile appréhension de l'usurpation. L'aspect polymorphe des éléments d'identité qui ont vocation à s'appliquer sur Internet en est, en effet, une autre raison, et la norme tente d'appréhender ces nouvelles problématiques en exécutant ce qu'elle sait déjà faire. En d'autres termes, elle a tendance a appliqué en effet les dispositifs proches de la notion d'usurpation d'identité pour tenter de l'encadrer. Or, une application extensive des droits qui lui sont proches ne correspond pas de façon précise à ces différentes et nouvelles approches de l'identité, de sorte qu'il existe en la matière, de profondes incertitudes juridiques.

Paragraphe 1. Le nom : clef de voûte de l'identité en ligne

Le premier élément d'identification qu'il convient d'analyser est le nom, et plus précisément de façon indirecte le pseudonyme dans la mesure où celui-ci découle directement du cadre normatif applicable au nom, élément clef de l'identité personnelle. Cette idée s'explique notamment par le fait que l'usage des communications électroniques a remodelé la forme de l'identifiant pour l'adapter aux nouvelles pratiques sur les communications électroniques en ligne.

Nombreuses sont les questions qui se sont posées autour du pseudonyme, notamment au regard de ses effets en droit. La doctrine s'est interrogée en effet sur sa nature juridique : il s'agissait pour elle de savoir si celui-ci bénéficiait d'un statut légal à part entière ainsi que d'une protection ou au contraire, si l'on devait lui appliquer un dispositif déjà existant. Ainsi par exemple, la jurisprudence s'est interrogée sur le fait de savoir si le pseudonyme relevait de l'anonymat ou de la sphère privée, ou encore s'il relevait de l'ordre du droit d'auteur, (et en

particulier au regard des artistes interprètes[36]) du droit des marques (où la jurisprudence s'est prononcée en faveur de sa valeur commerciale de sorte que le pseudonyme peut être cédé, transmis, et il peut, en outre, faire l'objet d'un dépôt), et bien plus encore, en matière de droit civil où l'on s'est demandé si le pseudonyme pouvait faire l'objet d'un droit de propriété[37].

Toutes ces inquiétudes ont été liées au moment où le pseudonyme a fait son entrée au sein des communications au public en ligne, et que les professionnels du droit se sont rendus compte qu'aucun cadre juridique adéquat ne semblait être susceptible de lui être appliqué. En effet, les pouvoirs publics se sont rendus compte que son utilisation pouvait entrainer d'innombrables abus en l'absence d'encadrement juridique approprié, telle que l'usurpation d'identité. Cette constatation ainsi faite, le législateur s'est accommodé d'autres dispositifs en vue de réprimer l'usurpation d'identité. Les juges ont ainsi opté pour l'utilisation des textes applicables en matière de faux nom. Dans les deux cas, la gageure était de taille dans la mesure où un régime juridique différent avait vocation à s'appliquer. [38] Sur ce point, il semble être plus opportun de partir de l'état du droit positif d'aujourd'hui, pour comprendre les raisons pour lesquelles le législateur lui a appliqué de façon extensive d'autres régimes juridiques.

Aujourd'hui, le principe tend à la liberté d'utilisation du pseudonyme. Chacun peut, utiliser un pseudonyme sur les réseaux sociaux en vue de cacher volontairement son identité, sous réserve toutefois d'une part, de ne pas porter atteinte à l'ordre public, et d'autre part, de ne pas constituer l'emprunt du nom d'un autre[39]. Dans le second cas, l'emprunt du nom d'autrui est susceptible de constituer une usurpation d'identité.

Le point de départ du questionnement sur son statut juridique relevait de l'ordre du droit de propriété. En d'autres termes, les professionnels du droit se sont demandés si le pseudonyme pouvait faire l'objet d'un droit de propriété. À ce titre, l'article 544 du Code civil définit le droit de propriété comme étant : « le droit de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements. » Si l'on fait une interprétation littérale de cet article, le terme général de « choses » ainsi que l'expression « de la manière la plus absolue » permettent d'englober le

[36] Cass., Com., 25 avril 2006, n° 04-15641.
[37] Art. 544 C. civ.
[38] MARTIN (M.), *Le pseudonyme sur Internet : une nomination située au carrefour de l'anonymat et de la sphère privée*, Paris, éd. L'Harmattan, coll. Langue et parole, 2006, pp. 121-141.
[39] « Dans quelles conditions peut-on utiliser un pseudonyme ? », Site du SP.

pseudonyme au sein du droit de propriété. La jurisprudence a, depuis longtemps, admis ce point de vue partant du principe que le nom retrace l'histoire d'une famille entière. Dès lors, les membres de la famille qui portent ce nom disposent naturellement sur lui d'un droit de propriété.[40]

Pourquoi le pseudonyme ferait-il l'objet d'un véritable droit de propriété ? En réalité, si l'on tient compte de certains détails, on se rend compte que le droit de propriété permet de jour d'une « chose » englobant in fine le nom, de sorte que ce dernier ne peut faire l'objet d'un emprunt ou d'une usurpation.[41] La valeur extrapatrimoniale du nom se justifie dès lors par le fait que le nom est un attribut de la personnalité à part entière.

De plus, compte tenu du fait que l'identité peut également concerner les personnes morales, c'est en outre, la raison pour laquelle, l'usage du nom à titre de marque a fait l'objet d'un long processus de réflexion. En effet, l'inaliénabilité du nom patronymique s'est très souvent confrontée au caractère patrimonial de ce même nom tant il était conçu comme une marque.[42] La chambre sociale de la Cour de Cassation avait en effet consacré cette inaliénabilité, empêchant directement le porteur dudit nom d'en disposer librement en vue d'identifier une autre personne. Mais elle avait également pris le soin de préciser qu'elle ne s'opposait pas à ce que ce nom puisse faire l'objet d'une utilisation en vue de faire l'objet d'une dénomination sociale ou d'un nom commercial.[43]

Le Code de la Propriété Intellectuelle sous le couvert de son article L.713-6 a pris le soin de préciser que le nom pouvait faire l'objet d'une marque au titre d'être un « signe distinctif ». Cet article dispose en effet que : « l'enregistrement d'une marque ne fait pas obstacle à l'utilisation du même signe ou d'un signe similaire comme : a) dénomination sociale, nom commercial ou enseigne, lorsque cette utilisation est soit antérieure à l'enregistrement, soit le fait d'un tiers de bonne foi employant son nom patronymique. » Ce raisonnement s'explique par le fait que le nom permet de distinguer les personnes, de sorte que la jurisprudence a pu faire un rapprochement entre le critère du signe distinctif requis en droit des marques, et le caractère distinctif du nom.

[40]Cass. Civ., 16 mars 1841.
[41]COURBE (P.), *Droit civil, les personnes, la famille, les incapacités*, op. cit., p. 10.
[42]COURBOULAY (M.), « Panorama de jurisprudence sur les litiges impliquant les noms et le droit des marques », *Gaz. Pal.*, 29 déc. 2012, n°364, p. 7.
[43]Cass. Com., 12 mars 1985, n° 84-17163.

Par exemple, dans un arrêt du 25 avril 2006,[44] la Cour de Cassation a considéré que le dépôt de marque du pseudonyme peut constituer une fraude si cela nuit à l'activité de l'utilisateur du pseudonyme. Dans le présent cas d'espèce, une artiste interprète disposait d'un pseudonyme, que le producteur avait déposé en tant que marque postérieurement à la conclusion du contrat avec cette artiste. Dès lors, le producteur ne pouvait ignorer l'existence de l'utilisation du pseudonyme par l'artiste interprète elle-même à titre de notoriété. Ce cas d'espèce pouvait d'ailleurs faire l'objet d'une étude en matière d'usurpation de nom, car l'utilisation du pseudonyme sans le consentement de la personne concernée implique in fine une usurpation.

Ainsi, au regard des deux exemples précités, force est de constater que la norme s'accommode de notions déjà établies qui se voient confrontées à des variantes pour lesquelles on veille à leur appliquer un dispositif déjà en vigueur. Le pseudonyme étant intimement lié à la notion de nom patronymique,[45]celui-ci peut faire l'objet d'un droit de propriété ainsi que d'une protection par le CPI au même titre que le nom. En d'autres termes, le pseudonyme dispose d'un statut juridique qui ne lui est guère propre mais il est toutefois susceptible d'être protégé par plusieurs normes juridiques qui s'adaptent à son utilisation sur les communications électroniques.

À ce titre, la définition juridique de ce dernier démontre effectivement cette idée dans la mesure où elle précise que le pseudonyme est un : « nom de fantaisie librement choisi par une personne pour masquer au public sa personnalité véritable dans l'exercice d'une activité particulière.[46] » En outre, si l'on confronte le statut juridique du pseudonyme à l'usurpation d'identité, on constate que le nom reste l'élément central de ladite usurpation. En effet, l'emprunt des droits de la personnalité est omniprésent de sorte que la définition formelle du pseudonyme le décrit comme un « nom de fantaisie ». Dès lors, non seulement il convient de préciser que les droits de la personnalité sont adaptés pour réprimer l'usurpation d'identité, mais également que le nom sous toutes ses formes aspire à la consécration d'une protection générale : il inspire les juges et le législateur dans la recherche d'une interprétation extensive pour résoudre des problèmes juridiques différents.

[44]Cass., Com., 25 avr. 2006, op. cit.
[45] LAROCHE-GISSEROT (F.), « Pseudonyme », *Rép. civ*., D., avril 2014.
[46] *Ibid*.

Le droit pénal par exemple, réprimait à l'origine l'usage du faux nom sous le couvert de l'article 434-23 du Code pénal : « le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende ».[47] Or, cet article ne pallie pas au problème de la répression en cas d'usurpation, dans la mesure où il précise : « dans des circonstances qui ont déterminé ou auraient pu déterminer des poursuites pénales. » Cela signifie qu'il permet de sanctionner l'usurpateur du nom seulement qu'en cas de poursuites pénales envers celui dont le nom a été usurpé. Cette problématique est récurrente et elle se retrouve en effet pour tous les éléments de l'identité applicables sur les communications électroniques. Il faut ainsi, prouver, que la personne lésée a bel et bien fait l'objet d'une usurpation.

Or, comment prouver l'usurpation de son nom alors même qu'aucun texte ne donne d'indications sur ce point ? L'application des droits de la personnalité aux nouveaux usages sur les communications électroniques cumulée avec l'absence de définition formelle de l'identité a révélé dans la pratique des difficultés pour la victime d'une usurpation d'en apporter la preuve. L'exemple le plus courant de la difficulté de prouver son identité d'une telle idée se voit notamment au travers du vol des plaques d'immatriculation.

Une personne, supposée victime, de plusieurs infractions au code de la route, ne peut prouver qu'elle n'est pas coupable de ces dernières, ni même que ses plaques d'immatriculation lui ont été usurpées. Il existe, dans ce cas spécifique, une présomption de culpabilité, de sorte que la personne concernée est dans l'obligation de prouver son innocence. On rentre alors dans une spirale sans fin : on ne peut prouver son innocence puisqu'aucun élément, ne permet de le faire. Aucune jurisprudence n'a doté d'un véritable statut juridique aux plaques d'immatriculation. Bien plus grave encore, la preuve de l'identité fait l'objet d'interprétation divergence au sein des juridictions. Aujourd'hui, ce problème se voit notamment au travers de l'adresse IP.

[47] ITENAU (O.), « Le statut juridique du pseudo », 20 mai 2008, Disponible sur son blog personnel : http://blog.iteanu.com

Paragraphe 2. Les composants de l'identité en ligne : porteurs d'incertitudes juridiques au regard des droits fondamentaux

En raison du fait que les composants de l'identité en ligne ne font pas l'objet d'une définition à l'instar de l'identité elle-même, ces derniers sont porteurs de véritables incertitudes juridiques, voire de confusions dans la mesure où toutes ces notions tendent à une protection légitime par les droits fondamentaux. Il convient dès lors de développer cette idée. Il s'avère naturel de débuter cette analyse par un développement sur l'adresse IP, dans la mesure où cet élément met en lumière cette problématique.

A/ Les incertitudes juridiques relatives aux contenants de l'identité

1. Les incertitudes juridiques autour de la qualification juridique de l'adresse IP

L'enjeu de reconnaître une valeur juridique à l'adresse IP comme étant un élément d'identification d'une personne est double. Tout d'abord, il convient de préciser que l'adresse IP est composée d'une série de chiffres qui est attribuée par un fournisseur d'accès à Internet (FAI), en vue d'identifier la machine utilisée (tel que l'ordinateur, les tablettes, voire des imprimantes), et indirectement une personne. Si l'on confronte cette idée avec les réseaux sociaux, on comprendra dès lors l'importance de celle-ci pour reconnaître l'identité d'une personne. En effet, avec le développement de l'anonymat sur ces supports de communication, il est plus qu'essentiel de recourir à l'adresse IP pour identifier une personne responsable d'infractions pénales sur Internet. Dès lors, tout le débat actuel est de savoir si l'adresse IP est une donnée personnelle ou non. Dans le premier cas, la loi de janvier 1978 aurait vocation à s'appliquer, ce qui aurait comme conséquence première l'attribution de compétences à une autorité en vue de veiller à la bonne conservation et au traitement de l'adresse IP. Celle-ci serait davantage mieux encadrée, et ce notamment par la CNIL.

Pourtant, selon certaines juridictions, l'adresse IP ne constitue en rien une donnée à caractère personnel dans la mesure où elle ne représente qu'un simple numéro attribué par les

fournisseurs d'accès à Internet.[48] Dès lors, peut-être que le problème ne provient pas tant dans une reconnaissance indirecte d'un individu grâce à une machine, mais par le fait que la délivrance de ce numéro d'identité ne soit pas effectuée par une autorité.

A contrario, pour d'autres juridictions telles que la CNIL, l'adresse IP est considérée comme une donnée à caractère personnel puisqu'elle permet d'identifier un individu, même indirectement. Ainsi, l'autorité avait reconnu le caractère nominatif de l'adresse IP dans une délibération en date du 21 décembre 2006[49] en raison du fait que l'adresse IP est le « seul rapprochement avec la base des abonnés détenue par le fournisseur d'accès à Internet. » Par ailleurs, cette prise de position est celle retenue par le Groupe de l'article 29 qui, dans son avis rendu le 20 juin 2007[50] relatif au concept de données à caractère personnel, a précisé que l'adresse IP est une donnée puisqu'elle concerne une personne identifiable.

Certains Tribunaux de Grande Instance donnent également une force juridique à l'adresse IP. Par exemple, le TGI Paris dans un jugement du 5 mars 2009[51] a considéré que : « l'adresse IP est une donnée à caractère personnel qui permet d'identifier une personne en indiquant sans aucun doute possible un ordinateur précis et qui établit la correspondance entre l'identifiant attribué lors de la connexion et l'identité de l'abonné. » Il semblerait que cette prise de position reste toutefois timide dans la mesure où aucun juge ne consacre explicitement l'adresse IP comme étant une donnée personnelle. À plus forte raison, le juge précise très souvent qu'il s'agit d'une donnée qui permet d'établir « une correspondance » entre l'identifiant et l'abonné.

Malgré ce manque de reconnaissance explicite, le caractère nominatif indirect de l'adresse IP prend davantage de poids aujourd'hui. Néanmoins, la question de la preuve de son innocence lorsqu'un litige est ouvert par le biais de cet élément demeure actuellement sans réponse. La question que l'on pourrait se poser notamment, et au vu de l'actualité concernant la contrefaçon, serait celle de savoir pourquoi les interprétations des juges en la matière diffèrent, alors même que le législateur avait crée de toute pièce en 2009, une structure ad hoc pour lutter contre la contrefaçon sur Internet en réprimant le contrefacteur en l'identifiant

[48]TGI Saint-Brieuc 6 sept. 2007, Ministère public, SCPP, SACEM c/ JP.
[49]CNIL, Délibération n° 2006-294, 21 décembre 2006.
[50]Groupe de travail de l'Article 29 sur la protection des données, *Avis 4/2007 sur le concept de données à caractère personnel*, 20 juin 2007, pdf, disponible sur : http://www.cnpd.public.lu/fr/publications/groupe-art29/wp136_fr.pdf
[51]TGI de Paris, 5 mars 2009, Roland Magdane c/ Youtube.

grâce à son adresse IP ? Ou encore, pourquoi la loi pour la Confiance dans l'Économie Numérique oblige-t-elle les hébergeurs à identifier les internautes coupables d'un délit de presse alors même que cette identification ne saurait être possible sans l'adresse IP ?

A contrario, si on analyse la position qui tend à refuser de considérer l'adresse IP comme étant une donnée personnelle, on s'aperçoit que ce refus légitime de reconnaissance est notamment lié au nombre bien trop important d'adresses IP. En effet, si l'on reprend notamment l'exemple de la HADOPI, autorité visant à protéger les œuvres sur Internet, il convient de rappeler que sa légitimité avait été remise en cause par le passé – et même aujourd'hui – pour cette raison[52]. En effet, le développement du protocole ip V6 a engendré la création de plusieurs adresses IP pour une même machine, rendant difficile l'identification du propriétaire, susceptible d'avoir commis une infraction. Il a été constaté, notamment dans le projet de loi sur la « Création » de

S'ajoute à la pénurie du nombre d'adresses IP, la facilité pour les hackers de les pirater, ou de les brouiller afin de ne jamais être rendus identifiables. On comprend in fine la raison pour laquelle certaines autorités refusent catégoriquement la reconnaissance de l'adresse IP comme étant une donnée personnelle. L'usage de la technique utilisée par les usurpateurs est bien trop avancé par rapport au droit. Plus surprenant encore, bien souvent les victimes de détournement de leur adresse IP ne s'en rendent pas compte, de sorte qu'il leur sera difficile de prouver leur innocence en cas de répression. Le débat sur le statut juridique de l'adresse IP est donc à cœur ouvert.

Cette incertitude provoque une insécurité juridique dans la mesure où l'adresse IP permet de reconnaitre indirectement une personne au sens de l'article 2 de la loi de 1978[53]. En outre, cette incertitude est révélatrice des obstacles que rencontrent le droit concernant l'usurpation d'identité numérique. En effet, comment serait-il possible pour ce dernier d'encadrer efficacement ce délit alors même que toutes les notions précédemment analysées sont porteuses d'incertitudes ? Les juridictions devraient, sans nul doute, donner une interprétation

[52] COSTES (L.), « Le transfert CSA-Hadopi devrait passer sur une loi sur la culture en 2014 », *Lamy*, 20 septembre 2013, Disponible sur : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/123355/Le-transfert-CSA-Hadopi-devrait-passer-par-une-loi-sur-la-culture-en-2014.aspx

[53] MATTATIA (F.), « Internet face à la loi Informatique et Libertés : l'adresse IP est-elle une donnée à caractère personnel ? » *Gaz. du Pal.*, 15 janv. 2008, n°15, p. 9.

homogène afin de renforcer le dispositif en la matière[54]. D'autres composants de l'identité ont soumis le doute chez le législateur, tel est le cas du courrier électronique.

2. Les incertitudes juridiques autour du champ d'application du courrier électronique

Le courrier électronique doit faire l'objet d'une analyse dans la mesure où elle peut être considérée comme un fichier nominatif, et par ce biais, être protégée en vertu de la loi Informatique et Liberté de 1978. Ce composant de l'identité numérique a également fait l'objet d'incertitudes juridiques en raison principalement de son caractère public ou privé. En effet, au sein des communications électroniques, force est de préciser que le droit opère une distinction entre les communications privées et les communications au public en ligne. Or, selon qu'il s'agisse d'une communication privée ou d'une communication publique, le régime juridique qui trouve à s'appliquer sera différent. Dans le premier cas, par exemple, la loi du 10 juillet 1991 relative au secret des correspondances aura vocation à s'appliquer ou encore la grande loi sur la communication audiovisuelle de 1986, alors que dans la seconde hypothèse, les délits de presse issus de la loi du 29 juillet 1881 trouvent leur place à juste titre[55]. Dès lors, la jurisprudence et la doctrine se sont interrogées sur le caractère privé ou public du courrier électronique.

Par ailleurs, le droit a du faire face à un autre obstacle de taille compte tenu de la nature elle-même du courrier électronique. En effet, il saurait être difficile de distinguer le courrier électronique de l'adresse e-mail, sans avoir analysé leur rapport. L'adresse e-mail joue le rôle de « contenant », dans la mesure où elle renferme en son sein un « contenu » : le courrier électronique. Ainsi, le rapport entre « contenant » et « contenu » a rendu davantage complexe l'encadrement juridique adéquat en la matière, et a engendré in fine, un véritable carcan juridique au regard d'une part de la question de savoir si l'adresse e-mail et le courrier électronique peuvent constituer des éléments de l'identité à part entière, et d'autre part, quel régime de responsabilité pourrait avoir vocation à s'appliquer en cas de litige ou d'infraction. Par conséquent, il convient d'analyser la portée du courrier électronique, c'est-à-dire qu'il est

[54] PERRAY (R.), « Adresse IP et données personnelles : un besoin de convergence d'interprétations entre juges », *Gaz. Pal.*, 30 avril 2009, n°120, p. 6.
[55] BARBRY (E.), « Le droit du mail », *Journal du Net*, 31 oct. 2000.

nécessaire de déterminer s'il relève de la correspondance privée ou de la communication publique.

La notion de correspondance privée est issue de la loi du 30 septembre 1986 relative à la liberté de communication, période durant laquelle les supports de communication étaient en pleine mutation provoquant dès lors un nombre incalculable de litiges liés au caractère public ou privé des correspondances. Tout l'intérêt de cette loi était ainsi de définir ce terme compte tenu des enjeux qui étaient de taille. Par exemple dans le cas d'une contrefaçon au sein de ces supports caractérisée dans un courrier électronique relève-t-elle de la correspondance privée ou de la communication au public en ligne ?

Afin de faciliter la distinction entre ces deux modes de communication, une circulaire du 17 février 1998, prise en application de la grande loi relative à la liberté de communication a indirectement défini la notion de correspondance privée dans la mesure où elle est venue préciser qu': « il y a correspondance privée lorsque le message est exclusivement destiné à une (ou plusieurs) personne, physique ou morale, déterminée et individualisée. » La loi pour la confiance dans l'économie numérique du 21 juin 2004 a apporté quelques clarifications sur ce point, dans la mesure où elle a consacré expressément une définition de l'adresse email.

L'article 1 IV de cette dite loi précise en effet que l': « on entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère. » Cette définition permet dès lors de définir le courrier électronique, et in fine, de réaliser que ce dernier permet d'identifier directement ou indirectement un individu. Néanmoins, ce dispositif ne suffit pas à lui seul pour protéger efficacement les victimes d'une infraction puisqu'aucune distinction n'a été opérée entre l'email privé et celui régi par les communications au public en ligne.

Le Conseil Constitutionnel saisi de cette question a dès lors jugé que cette définition se bornait à un « simple procédé technique », et qu'il incombait au juge de prendre le soin de trancher cette question en cas de litige.[56] De ces éclaircissements en découle une certaine main mise par le juge de ce terme en cas de litige, notamment au regard de la responsabilité. En effet, si l'on applique ces textes à l'usurpation d'identité, l'usurpateur pourra voir sa responsabilité engagée pour détournement du courrier électronique considéré comme relevant

[56] Cons. Const., n° 2004-496 DC du 10 juin 2004.

du secret des correspondances en vertu de l'article L.226-15 du Code Pénal. La rédaction de cet article est intéressante dans la mesure où elle révèle l'importance de l'adresse électronique, et plus largement, elle met en exergue l'offre à la victime d'une arme de défense en cas d'usurpation d'identité. En effet, tel que l'article est rédigé, celui-ci fait apparaitre des notions importantes comme le terme de « détournement » des correspondances, laissant de facto la possibilité pour le juge en cas d'usurpation d'adresse e-mail de faire une application extensive de cette incrimination.

Malgré ces avancés jurisprudentielles, force est de constater que des incertitudes juridiques relatives au caractère public ou privé du courrier électronique ont persisté et, notamment au regard du droit social compte tenu des nombreux litiges entre l'employeur et ses salariés.[57] Par exemple, la jurisprudence s'est interrogée sur le fait de savoir si un courrier électronique envoyé par le salarié depuis l'ordinateur professionnel durant son temps de travail donnait-il droit à l'employeur de lire le courrier électronique de son salarié.[58] La Cour de Cassation a dès lors consacré la notion d'« intimité de la vie privée », issue directement des droits de la personnalité, en précisant que dans ce présent cas d'espèce, le courrier relevait de la correspondance privée ; donnant droit au salarié à son intimité de la vie privée malgré la rédaction d'un courrier litigieux depuis son lieu de travail et durant son temps de travail[59]. Pour rendre une telle décision, la Cour a opéré une application classique du droit puisqu'elle a utilisé principalement l'article 8 de la CEDH relatif au respect de la vie privée.

En d'autres termes, les droits de la personnalité sont ancrés dans la rédaction de textes relatifs aux litiges liés aux nouveaux composants de l'identité. Or, ces derniers démontrent également la difficulté pour le droit d'une part de concilier plusieurs droits fondamentaux lorsque ceux-ci sont confrontés les uns envers les autres, et d'autre part, de son incapacité à appréhender des nouvelles problématiques, notamment lorsqu'il s'agit d'infractions commises sur les communications électroniques. Pour l'heure, force est de noter que la distinction entre correspondance privée et communication au public en ligne prend de plus en plus d'ampleur aujourd'hui.

[57] RAPP (L.), *Le courrier électronique : e-mail*, Coll. Puf, Que sais-je ?, 1998, pp. 34-36.
[58] Cass. Soc., 2 oct. 2001, n° 99-42.942.
[59] RAYNOUARD (A.), « Actualité du droit des nouvelles technologies », *Defrénois*, 15 nov. 2002, n°21, p. 1407.

B/ Les incertitudes juridiques relatives aux éléments d'authentification de la personne

Parmi les mots de passe demeuraient célèbres dans la pratique, nous connaissons tous la célèbre phrase : « Sésame ouvre-toi ! », ou encore les vers de Verlaine utilisés pour annoncer le Débarquement de Normandie : « *les sanglots longs des violons de l'automne blessent mon cœur d'une langueur monotone* ». Leur but ? Permettre l'authentification d'un individu.

Si l'Histoire dénote la création de la cryptologie, ou bien encore l'invention d'outils permettant de favoriser la diffusion de messages codés tel que le langage morse, ou encore la machine appelée « Enigma » utilisée par les allemands pour crypter les messages radio émis de leurs ennemis[60], force est de préciser que la nature du mot de passe évolue, mais sa finalité quant à elle demeure intemporelle : il s'agit d'authentifier un individu.

Cette authentification permet dès lors d'identifier un individu, et une réflexion relative à l'usurpation ne saurait être efficace sans analyser l'utilisation du mot de passe sur les communications électroniques. En effet, à l'instar des autres éléments numériques, le mot de passe, n'a pas d'un point de vue juridique, une définition précise. Toutefois, ce dernier peut s'entendre par une interprétation extensive comme un élément de l'identité en ligne grâce à sa fonction d'authentification. Bien que le mot de passe ne fasse pas partie des identifiants stricto sensu de l'identité personnelle, ce dernier a cependant vocation à la protéger. En effet, tout site Internet, accès à un compte bancaire en ligne, ou à un compte sur les réseaux sociaux nécessite un mot de passe.

D'un point de vue juridique, la portée confidentielle du mot de passe permet de le rattacher au rang des droits de la personnalité de façon implicite. Dès lors, en cas d'usurpation du mot de passe, pratique la plus récurrente de surcroit pour usurper une identité, la victime dispose de plusieurs articles de défense relatifs à la vie privée, et notamment l'article 9 du Code Civil[61]. Le droit à la protection de la vie privée connait de fait, une certaine expansion. L'application des règles de droit commun en matière d'usurpation du mot de passe démontre plusieurs réalités : d'une part, à l'heure où les communications électroniques sont à leur apogée, le droit

[60] JOFFRIN (L.), « 70 ans après : les 12 mystères du Débarquement », *Le Nouvel Observateur*, 6 juin 2014.
[61] MARINO (L.), « Les nouveaux territoires des droits de la personnalité », *Gaz. Pal*, 19 mai 2007, n°139, p. 22.

ne peut pas, ou ne peut plus, se contenter d'incriminer des infractions ; il doit en outre connaitre l'aspect technique de ces dites communications afin de mieux les appréhender.

D'autre part, recouvrir le mot de passe sous le champ d'application des droits subjectifs illustre également l'idée selon laquelle il est impossible aujourd'hui de dissocier le droit de la technique. Cet aspect est essentiel car il sera possible de constater ultérieurement que la lutte du droit contre l'usurpation est rendue difficile parce qu'il ne prend pas en compte, les techniques utilisées pour usurper l'identité.

Ce dernier reste sclérosé dans un régime de droit commun calqué sur les droits fondamentaux en guise de « sûreté juridique ». En effet, on pourrait penser que le recours systématique aux droits de la personnalité est un moyen pour le législateur de contrôler ce qu'il, en réalité, ne contrôle pas. De plus, le remodelage des droits de la personnalité provoque in fine le manque de besoin pour ce dernier de définir les notions principales de ce délit. Or, l'absence de définition légale de ces différents termes engendre non seulement des difficultés dans la lutte contre l'usurpation d'identité dans la mesure où le droit pénal est d'interprétation stricte et qu'il ne peut, réprimer ce qui n'est pas définit, mais également un manque d'efficacité évident dans la mesure où la norme éprouve des difficultés à évoluer aussi vite que les techniques de fraude en matière d'usurpation en ligne.

En d'autres termes, malgré la création en 2010 du délit d'usurpation d'identité, celle-ci ne suffit pas pour lutter contre cette fraude. Pour contrer efficacement cette fraude technologique, le législateur aurait du reconnaitre l'existence d'un droit spécifique en la matière.

Section 2. Le recours aux droits fondamentaux tendant à la protection de l'identité en ligne au regard de l'usurpation

Conscient d'une lutte inefficace au regard de l'usurpation d'identité en ligne, le Gouvernement a porté une réflexion dès 2008 sur la possibilité de mettre en place un dispositif performant afin de résoudre tous les litiges relatifs aux actions malveillantes sur Internet. Lors de la présentation du plan de lutte contre la cybercriminalité le 14 février 2008, la ministre de l'Intérieur de l'époque, Michèle Alliot-Marie avait reconnu qu'il était « possible aujourd'hui d'utiliser à des fins malveillantes l'identité d'une personne physique ou morale sur Internet […]. Je veux que l'usurpation d'identité sur Internet soit punie par la loi comme un délit […]. »[62]

Cette présente section sera ainsi consacrée à la mise en place d'un dispositif visant à réprimer l'usurpation d'identité en ligne. En effet, l'absence d'une définition légale des éléments essentiels qui entourent l'usurpation d'identité engendre in fine une mauvaise application du délit d'usurpation d'identité. Il conviendra dès lors de constater que la création du délit d'usurpation d'identité ne suffit pas pour régler tous les litiges en la matière. En effet, d'une part, le principe d'interprétation stricte de la loi pénale contrevient aux évolutions des moyens techniques utilisés par les usurpateurs.

D'autre part, la consécration d'un tel délit n'a pas permis la reconnaissance d'un droit spécifique en matière d'Internet, de sorte que la jurisprudence continue à adopter une interprétation extensive d'autres régimes déjà mis en place. Enfin, il sera intéressant de mettre en avant les solutions juridiques qui ont été pensées pour lutter contre cette infraction, et de constater que celles-ci étaient vouées à l'échec, faute de prendre en compte l'aspect technique des moyens d'usurpation.

[62] ALLIOT-MARIE (M.), Discours prononcé à l'occasion de la présentation du *plan de lutte contre la cybercriminalité*, 14 fév. 2008, [En ligne] : www.interieur.gouv.fr/Archives/Archives-de-Michele-Alliot-Marie-2007-2009/Interventions/14.02.2008-Lutte-contre-la-cybercriminalite

Paragraphe 1. Les limites du recours au droit commun dans la lutte contre l'usurpation d'identité en ligne

L'absence de définition légale des principaux termes n'est pas le seul facteur d'une protection inadéquate de l'identité en ligne. En effet, compte tenu d'une jurisprudence incertaine en la matière, et de l'existence d'une confusion juridique entre ces diverses notions, il a semblé bon au législateur, ainsi qu'au Gouvernement de créer en 2010, un délit relatif à l'usurpation d'identité sur Internet. Or, au sein du droit positif il existait déjà un tel délit inséré au sein de l'article 434-23 du Code pénal. Néanmoins, celui-ci s'est avéré inutile dans la mesure où les pouvoirs publics se sont aperçus qu'il ne permettait pas d'une part, de lutter contre les techniques de fraude utilisées pour voler l'identité d'un individu, d'autre part, qu'il restreignait en réalité sensiblement le champ d'application du droit pénal.

En effet, l'impuissance législative est également liée au principe d'interprétation stricte de la loi pénale[63] dans la mesure où l'article 434-23 du Code pénal ne prend pas en compte toutes les évolutions techniques de fraude en ligne. En outre, cette inefficacité s'explique également, par le fait que le délit mis en place par ledit article, ne suffit pas à lui seul pour réprimer l'usurpateur: en effet, ce dernier étant considéré comme étant un délit préparatoire, d'autres droits ont dès lors vocation à s'appliquer.

[63] PRUD'HOMME (M.), « L'usurpation d'identité numérique : bientôt un nouveau délit », *Gaz. Pal.*, 24 avril 2010, n° 114, p. 8.

A/ Les limites du principe d'interprétation stricte de la loi pénale dans la lutte contre l'usurpation d'identité en ligne

La reconnaissance de délits au sein du droit pénal n'est pas anodine, dans la mesure où ce droit est considéré comme étant l'un des « moyens les plus sûrs afin de mesurer le degré de civilisation d'une société[64]. » Si les lacunes en matière d'usurpation d'identité sont liées au principe d'interprétation stricte de la loi pénale, il convient de préciser qu'il serait nécessaire de réformer ce principe. En effet, le principe d'interprétation stricte de la loi pénale, traduit du l'adage latin « *nullum crimen, nulla poena sine lege*[65] » découle directement d'une interprétation de la loi. Or, si la loi elle-même manque d'efficacité dans la mise en place d'un dispositif pour lutter contre l'usurpation, comment le principe de légalité pourrait-il être effectif à son tour ? En outre, ce principe tend à mettre en lumière le raisonnement juridique, si précieux aux « Hommes de Loi », or, le caractère quasi sacré de ce principe ne peut aujourd'hui être optimal dans la pratique, compte tenu de l'évolution toujours plus rapide et croissante des communications électroniques. Ces différents aspects permettent dès lors de comprendre le manque d'effectivité pour les juges de lutter contre les techniques d'usurpation en ligne.

En outre, s'ajoute à cette problématique celle de l'insertion dans le Code pénal d'un deuxième article relatif à l'usurpation d'identité, rajoutant une part supplémentaire de difficulté pour le juge de trancher un litige sur la question. Il convient ainsi de traiter successivement les défaillances du premier article qui traite de l'usurpation d'identité puis du second inséré en 2010 portant création du délit d'usurpation d'identité.

L'article 434-23 du Code pénal introduit par une loi du 5 août 1899[66] précise expressément que : « le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 € d'amende ». En vertu de ce principe, il n'est possible de sanctionner l'usurpateur que si le nom d'un tiers a été usurpé et dans des circonstances qui

[64] GHICA-LEMARCHAND (C.), « L'interprétation de la loi pénale par le juge », Paris, Colloque organisé au Palais du Luxembourg, les 29 et 30 septembre 2006, [En ligne] : www.senat.fr/colloques/office_du_juge/office_du_juge9.html
[65] BOULOC (B.), *Droit pénal général*, D., éd. 2011, p. 56.
[66] Projet de la LOPSI, *Doc. parl. S.*, n° 517, 2009-2010.

auraient pu entrainer ou qui entrainent contre la victime des poursuites pénales. En d'autres termes, cet article restreint sensiblement le champ d'application du juge et de la loi en matière d'usurpation d'identité[67]. En effet, au regard du caractère hétérogène de l'identité ainsi que de tous les éléments qui la composent et qui ont vocation à s'exprimer sur les communications électroniques, l'usurpation du nom n'est qu'une partie infime des cas d'usurpation en ligne. En outre, cet article révèle entre autre le vide juridique en la matière, dans la mesure où le simple fait d'usurper une identité, et ce, sans commettre une autre infraction pénale ne peut pas faire l'objet d'une sanction. Un rapport parlementaire rendu en juin 2010 à l'initiative de Monsieur Courtois, représentant de la Commission des Lois a parfaitement résumé la situation en disant expressément qu'il s'agit d'un « droit positif partiellement inadapté[68]. »

En tout état de cause, le champ d'application de cet article vise essentiellement les délits de presse issus de la loi du 29 juillet 1881, de sorte que le juge peut constater l'usurpation de l'identité personnelle qu'en cas de révélation de faits diffamatoires ou injurieux sous un nom d'emprunt. Il en découle que cet article n'est qu'un délit accessoire à un autre premier délit[69].

Par ailleurs, l'inadaptation du droit s'agissant de ce délit se voit également au travers de l'appellation donnée par les parlementaires à l'usurpation d'identité prévue par cet article puisque ces derniers traitent de « l'identité d'état civil ». Or, comme nous l'avons vu précédemment, l'application classique du droit en matière d'état civil ne prend pas en compte les différentes évolutions techniques et technologiques de l'identité. En d'autres termes, cette expression donne matière à comprendre la sclérosité du droit et donne également l'impression que celui-ci se borne à ne pas prendre en compte délibérément les évolutions de l'identité.

Outre ces diverses difficultés, le principe d'interprétation stricte de la loi pénale se heurte à un autre obstacle et non pas des moindres qui rend davantage complexe l'appréhension dudit délit. En effet, le principe de légalité tend à se confronter au principe de non cumul des peines,[70] dans la mesure où il faut nécessairement une autre infraction pour reconnaitre une usurpation. Cet aspect a d'ailleurs fait l'objet de débats parlementaires, puisque l'on s'est demandé si l'article 434-23 du Code pénal pouvait donner lieu à une reconnaissance autonome et ne pas être simplement considéré comme une infraction connexe, en vue de ne

[67] MONNET (Y.), Note sous Cass., 30 mai 2007, *Gaz. Pal.*, 8 mars 2008, n°68, p. 23.
[68] *Doc. parl. S.*, n° 517, 2009-2010, op.cit.
[69] PASOTTI (M.), « Défendre son e-réputation grâce au droit pénal », op.cit.
[70] *Ibid*.

pas violer le principe de non cumul des peines.[71] Il en ressort que l'alinéa 2 dudit article constitue une exception à ce principe[72]. Cela signifie que le délit posé à l'article 434-23 du Code pénal donne la possibilité au juge de cumuler plusieurs infractions, le restreignant ainsi de toute substance pénale, puisqu'il est considéré simplement comme un délit préparatoire, par exemple, comme un élément constitutif d'une infraction de violence.[73]

Pourtant, le refus de reconnaitre l'usurpation d'identité comme une infraction autonome n'a pas fait l'unanimité, et une proposition de loi en 2005[74] tendait à pénaliser l'usurpation d'identité en ligne. En effet, le sénateur monsieur Michel Dreyfus mettait en évidence le vide juridique en la matière, dans la mesure où aucun texte ne permettait de sanctionner l'usurpation d'identité lorsque les moyens frauduleux employés ont été constatés sur les supports de communication en ligne. Le souhait de ces parlementaires était donc d'insérer dans le Code pénal, une nouvelle infraction appelée « usurpation d'identité numérique » au sein d'un article 323-8 qui aurait permis de punir d'un an de prison ainsi que d'une peine de 15 000 euros d'amende : « le fait d'usurper sur tout réseau informatique de communication l'identité d'un particulier, d'une entreprise ou d'une autorité publique. » Cette insertion aurait permis de consacrer l'usurpation d'identité en ligne, dans la mesure où l'article susvisé englobait un certain nombre de situations de façon large. Cette consécration aurait également été visible de par la suite de cet article, qui venait préciser l'exception du principe de non cumul des peines puisqu'il indiquait que : « les peines prononcées se cumulent, sans possibilité de confusion, avec celles qui auront été prononcées pour l'infraction à l'occasion de laquelle l'usurpation a été commise. »

En d'autres termes, cela signifie que l'usurpation d'identité aurait été reconnue comme une infraction autonome, et non connexe, permettant in fine de protéger la victime d'une usurpation d'identité stricto sensu. Toutefois, force est de préciser que cette proposition de loi n'a pas été adoptée, agrandissant dès lors le gouffre dans lequel le droit s'était immiscé, et privant dès lors la victime d'un dispositif de protection efficace. En tout état de cause, le refus clairement catégorique de prendre en compte les évolutions technologiques se voit notamment au travers du fait que le délit d'usurpation d'identité ne reste qu'une infraction connexe. En

[71] Rép.min. à la QE n°61615 du 20 octobre 2009, J.*O. déb. parl. A.N* (Q.) du 27 avril 2010, p. 4783.
[72] BOULOC (B.), *Droit pénal général*, op.cit., p. 559.
[73]BARBRY (E.), DUFIEF (V.), Note sous TGI de Carcassonne, 16 juin 2006, *Gaz. Pal.*, 19 oct. 2006, n°292, p. 36.
[74] Proposition de loi tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques, *Doc. parl. S.*, n° 452, 2004-2005.

effet, nonobstant la prise de position de certains sénateurs qui allait dans le sens d'une modernisation du dispositif, le législateur et la jurisprudence ont continué à appliquer le régime de droit commun, c'est-à-dire, des droits de la personnalité, pour lutter contre ce fléau juridique. Les solutions qui s'offrent alors à la victime sont effectivement calquées sur une application classique du droit, ne la permettant pas ainsi d'être protégée en cas d'usurpation d'identité stricto sensu.

B/ Les limites de la reconnaissance du délit d'usurpation d'identité comme infraction connexe dans l'application du droit commun

Les années 2000 ont été porteuses de grandes mutations puisque les autorités se sont rendues compte de l'ampleur des infractions commises sur les communications électroniques, principalement lorsque celles-ci attrayaient à l'identité des individus. Toutefois, l'impuissance des professionnels du droit sur cette question s'est faite ressentir dès lors que l'usurpation d'identité de l'article 343-23 du Code pénal, demeurait une infraction connexe. Il s'agira ainsi dans un premier temps, de constater que le droit fait un recours systématique aux droits de la personnalité pour lutter contre ces nouvelles infractions, et qu'il a, par la suite, essayé de combler ses lacunes par l'adoption de plusieurs projets de loi, notamment la Loi pour la Confiance dans l'économie numérique, la Loi d'orientation et de programmation relative à la sécurité intérieure[75] (LOPSI 1), puis la nouvelle loi d'orientation et de programmation pour la performance de la sécurité intérieure[76] (LOPPSI 2) . Ce paragraphe tentera ainsi, de retracer chronologiquement les difficultés pour le droit de lutter contre ledit délit et d'en comprendre les raisons.

L'aspect fondamental des droits de la personnalité reprend toute sa substance ici car ces derniers sont véritablement au cœur du raisonnement juridique en la matière. En effet, les droits de la personnalité ont donné matière au juge pour recourir systématiquement aux incriminations traditionnelles pour réprimer les cas d'usurpation d'identité. Il s'agit donc d'analyser succinctement les normes de référence utilisées pour ce délit en vue de conclure à

[75] L. n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure
[76] L. n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

l'importance des droits de la personnalité, préconisés afin d'instaurer une sûreté juridique en apparence.

Comme il a été mentionné précédemment, l'article 343-23 du Code pénal constitue le droit commun applicable en matière d'usurpation d'identité. Toutefois, il conviendrait de nuancer ces propos et de revenir sur la notion même d' « usurpation » dans la mesure où cet article a vocation à s'appliquer, seulement en cas de poursuites pénales. En effet, s'il s'agissait d'une « usurpation » au sens strict, les conséquences pénales seraient plus importantes. En réalité en effet, cet article tend incriminer la « dissimulation » de l'identité,[77] de sorte qu'il est nécessaire d'utiliser d'autres normes en complément pour incriminer ce cas d'espèce.

L'élément central de toutes ces différentes formes d'incrimination est l'usurpation du nom. En effet, il s'agit d'une des violations les plus graves puisqu'elle touche à la personnalité du porteur. Dès lors, le nom, tant protégé par les textes internes qu'internationaux sert de référence aux infractions que nous allons analyser. Cette idée favorise en outre une meilleure compréhension d'une application classique des textes en matière d'usurpation d'identité, puisque nous avons vu que le nom est en quelque sorte le certificat d'authentification d'un individu. Dès lors, le nom est le maillon essentiel de la chaine des diverses incriminations existantes. C'est-à-dire que le nom a été la source d''inspiration de la rédaction de plusieurs incriminations, qui elles-mêmes, ont par la suite servies de modèles de référence pour mettre en œuvre l'article 343-23 du Code pénal.

Toutefois, la référence au nom ne suffit pas au regard de l'usurpation dans la mesure où l'identité relève sur une multitude de composants. En effet, afin de disposer d'un cadre juridique adéquat et adapté aux nouvelles problématiques posées par les nouvelles technologies, il est apparu nécessaire dans la pratique d'utiliser un droit de référence. Et quoi de plus sûr que le recours aux droits de la personnalité ?

L'utilisation d'autres droits de la personnalité est sans aucun doute liée aux réponses qu'elles ont su apporter aux nouveaux usages frauduleux en ligne. Néanmoins, le recours à ces diverses formes d'incrimination ne suffit pas à lui seul pour lutter contre l'usurpation d'identité. Ces dernières disposent en effet de certaines limites, dans la mesure où celles-ci n'avaient pas, à l'origine, vocation à être appliquées pour l'usurpation d'identité en ligne.

[77] MOURON (P.), « L'identité virtuelle et le droit "sur" l'identité », *Lamy Droit de l'immatériel 2010*, n°64, oct. 2010.

Les poursuites pénales visées par l'article 343-23 du Code pénal concernent tout d'abord, le délit d'escroquerie de l'article 313-1 du même code. Il parait intéressant de noter la similarité du contexte de ces deux incriminations dans la mesure où celles-ci ont toutes deux été introduites dans le Code pénal en raison d'un nombre important d'infractions liées aux nouvelles techniques de fraudes issues des nouvelles technologies. Au terme de cet article, l'escroquerie se définit comme étant notamment « l'usage d'un faux nom ou d'une fausse qualité » permettant « soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale […]. » Tout d'abord, force est de préciser que la référence au nom est incontournable pour reconnaitre une responsabilité pénale au profit de la victime. Mais ce qui est intéressant ici, c'est que le nom peut s'entendre de façon large : faute de définition formelle du nom au sein de cet article, les communications électroniques ont permis, non seulement d'englober le nom pour réprimer un usurpateur (dans le cas où on arrive à l'identifier) mais également d'autres éléments d'identification autour de ce premier élément.

La jurisprudence a interprété cet article en vue de lui donner davantage de clarté et a jugé que le faux nom pouvait s'entendre comme le nom patronymique ou le pseudonyme[78]. Dès lors, l'usage du nom est limité aux seules personnes physiques et ne rentre pas dans le cadre du délit d'escroquerie, l'usage frauduleuse du prénom sauf en cas de confusion avec une autre personne[79].

Eu égard au champ restreint de cet article, le délit d'escroquerie fait, au même titre que le délit d'usurpation d'identité, référence à d'autres incriminations, de sorte que le nom puisse s'entendre de façon large. Ainsi par exemple, le délit d'escroquerie est souvent utilisé en cas de fraude à la carte bancaire. En effet, la carte bancaire peut constituer un élément de l'identité, dans la mesure où le nom de son titulaire est inscrit dessus, qu'elle bénéficie d'un mot de passe en guise de certificat d'authentification de son porteur, et qu'elle dispose, en outre, du numéro de compte de ladite personne. Les cartes bancaires ont connu un succès flamboyant dès les années 1990, destinées à être une autre alternative de moyen de paiement que le chèque. Informatisées, celles-ci connaissent aujourd'hui une notoriété planétaire, mais les communications en ligne ont dès lors octroyé une multitude de pratiques frauduleuses,

[78] Cass. crim., 27 oct. 1999, n° 98-86.017.
[79] Anonyme, « Notion de nom » *LDPA*, n° 219.

visant notamment à usurper ces cartes[80]. Si le recours aux infractions classiques du droit pénal tel que l'article 313-1 dudit Code semble inévitable, il est apparu nécessaire de moderniser le dispositif de lutte mis en place, compte tenu des nouvelles techniques de fraudes en ligne. C'est la raison pour laquelle, une loi relative à la sécurité quotidienne adoptée en 2001[81] a mis en exergue le désir du législateur de prendre en compte l'aspect technique de ces problématiques en créant une structure ad hoc[82], capable d'assurer le « suivi des mesures de sécurisation entreprises par les émetteurs et les commerçants, à établir des statistiques de la fraude, et à proposer des moyens de lutte contre les atteintes d'ordre technologique à la sécurité des cartes de paiement. »[83]

De plus, les communications électroniques ont favorisé la création de nouvelles formes d'escroquerie, à l'image de la création des nouveaux contours de l'identité, de sorte qu'il est apparu la notion d' « escroquerie informatique[84]. » Cette nouvelle technique de fraude, aussi appelée « phishing » que nous analyserons ultérieurement semble imposer une limite au délit d'escroquerie, dans la mesure où la référence au nom ne peut valoir pour les personnes morales, victimes d'une tentative de phishing. De fait, le délit d'escroquerie couvre en son seing un certain nombre d'incriminations, afin d'offrir à la victime une protection large. Par exemple, l'escroquerie peut se caractériser par des manœuvres frauduleuses telles que l'utilisation frauduleuse d'un moyen de paiement obtenu par des fins frauduleuses, pouvant dès lors caractériser un abus de confiance,[85] ou encore, lorsque ce moyen de paiement a été falsifié ou contrefait[86]. Dans le cas où le délit d'escroquerie ne suffirait pas à condamner le présumé coupable, le juge peut trancher un litige par le biais d'incriminations distinctes, comme l'utilisation frauduleuse d'un moyen de paiement précité.

Si l'on applique l'incrimination posée à l'article 313-1 du Code pénal à l'usurpation d'identité, on comprend significativement le manque d'effectivité de cet article. En effet, bien que ces deux dispositions bénéficient de points communs relatifs aux évolutions des techniques de fraude en ligne, le délit d'escroquerie, ne peut, en aucun cas, résoudre un litige relatif à l'usurpation. D'une part, car l'identité regroupe non seulement le nom, mais aussi

[80] MOREL-MAROGER (J.), « La répression des fraudes à la carte bancaire », *Gaz. Pal.*, 2 juin 2012, n°154, p. 12.
[81] L. n° 2001-1062 du 15 nov. 2001 relative à la sécurité quotidienne.
[82] L'OSCP.
[83] MOREL-MAROGER (J.), « La répression des fraudes à la carte bancaire », op. cit.
[84] « Notion de nom » *LDPA*, n°250.
[85] Cass. crim., 25 janvier 2012, n° 10-83.350.
[86] Cass. crim., 8 avril 2009, n° 08-86.481.

d'autres éléments qui n'ont pas vocation à être appliqué en matière d'escroquerie, d'autre part et surtout, parce que l'identité peut concerner aussi bien une personne physique qu'une personne morale. Or, comme nous l'avons vu, en matière d'escroquerie, la jurisprudence est venue préciser que le faux nom ne peut concerner une personne morale, victime d'une usurpation d'identité. Cela explique par conséquent les raisons pour lesquelles l'article 343-23 du Code pénal tend à prendre en compte d'autres incriminations.

En somme, la référence au nom se voit également au travers du délit de faux public de l'article 433-19 du Code pénal, en vertu duquel il est puni de six mois d'emprisonnement et de 7 500 euros d'amende : « le fait, dans un acte public ou authentique ou dans un document administratif destiné à l'autorité publique [...]: 1° De prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil ; 2° De changer, altérer ou modifier le nom ou l'accessoire du nom assigné par l'état civil. »

Dès lors, la commission de l'infraction du faux public illustre parfaitement le critère retenu pour caractériser le délit d'usurpation d'identité. En effet, l'utilisation d'un faux nom peut s'apparenter à une usurpation dans le cas où l'emprunt de celui-ci engendre contre la victime des poursuites pénales. Mais de la même matière que pour l'escroquerie, l'article 433-19 du Code pénal connait bien des limites au regard de l'usurpation, dans la mesure où il est fait référence au nom de l'état civil.

Or, comme nous l'avons vu, l'identité nécessite aujourd'hui, une plus grande vision que celle retenue par l'état civil, dans la mesure où le nom constitue qu'une petite partie des composants de l'identité en ligne. Dès lors par exemple, en cas d'utilisation, d'une fausse adresse électronique visant à usurper des données, la victime ne pourra se prévaloir en guise d'infraction connexe de l'usurpation, celui de l'escroquerie pour se protéger. Il en va de même pour l'article 781 du Code pénal, auquel l'article 313-1 du même code a vocation à se référer, dans la mesure où ce premier article traite de la demande frauduleuse d'extrait de casier judiciaire.

Ces limites constituent en réalité un cercle vicieux au regard de l'usurpation puisque le délit posé à l'article 313-1 du Code pénal nécessite le recours à ces diverses infractions afin de protéger davantage la victime, mais dans le même temps, celles-ci ne peuvent pas réprimer l'usurpateur de manière efficace puisqu'elles n'avaient pas vocation à s'appliquer en matière d'usurpation d'identité en ligne au moment de leur création et de leur promulgation. Ainsi,

par exemple, la constitution d'un faux profil d'une entreprise ou d'un particulier sur les réseaux sociaux peut leur être préjudiciable mais sans que cela soit possible d'être réprimé sur la base de ces articles, notamment lorsque cela porte atteinte à leur e-réputation. Par exemple, une célèbre affaire de 2010 met en exergue toutes ces problématiques : il s'agit de l'ordonnance de référé du 24 novembre 2010, dans laquelle le Tribunal de Grande Instance de Paris a sanctionné un internaute pour avoir crée sur le réseau social Facebook un faux profil du célèbre humoriste Omar[87]. L'internaute se faisait passer pour l'humoriste, et répondait entre autre, aux commentaires de fan. Il avait également utilisé ses photos personnelles. La victime a assigné l'usurpateur en justice au motif que la mise en ligne d'un faux profil Facebook constitutif d'un "avatar fictif qui parasite sa vie privée" lui cause un préjudice et viole également son droit à l'image. La juridiction de second degré a donné gain de cause à la victime en précisant que : « toute personne, quelle que soit sa notoriété, a droit, en application de l'article 9 du Code civil, au respect de sa vie privée et est fondée à en obtenir la protection en fixant elle-même les limites de ce qui peut être divulgué à ce sujet. Toute personne dispose également, en application du même texte, d'un droit exclusif qui lui permet de s'opposer à la reproduction de son image, sans son consentement préalable. » Faute de texte d'incrimination en matière d'usurpation d'identité, le juge a semblé judicieux de faire référence aux droits de la personnalité[88].

En d'autres termes, le statut du délit d'usurpation d'identité en ce qu'il est considéré comme un délit préparatoire, ou accessoire, laisse une nouvelle fois, un vide juridique en la matière. Bien que les autorités aient pu en effet faire référence au droit du nom, droit de la personnalité à part entière, pour lutter contre l'usurpation d'identité, et nonobstant la référence à d'autres incriminations, ce mécanisme n'a pas suffit à être efficace, compte tenu de l'évolution des techniques de fraudes en la matière. Le droit a donc essayé de combler ses lacunes en la matière par deux projets visant à lutter contre l'usurpation d'identité, mais ceux-ci ayant également fait référence aux droits de la personnalité dans une conception classique, ont été submergés par des obstacles également.

Le vide juridique qu'a laissé place la pratique d'usurper l'identité, ou encore la création de faux profil sur les réseaux sociaux ont amené les pouvoirs publics à s'interroger sur une nécessaire modernisation et harmonisation du dispositif mis en place pour lutter contre

[87] TGI de Paris, 24 novembre 2010, Omar S. c/ Alexandre P.
[88] BEM (A.), « L'usurpation d'identité sur Facebook constitue une atteinte à la vie privée et au droit à l'image. », *Legavox.fr*, 8 décembre 2010

l'usurpation d'identité en ligne. En effet, on entend par « modernisation » le fait de ne plus se référer seulement aux infractions traditionnelles, le droit, doit pouvoir créer des normes nouvelles afin de lutter efficacement contre l'usurpateur. Or de ce point de vue, celui-ci a rencontré un bon nombre d'obstacles sur sa volonté de moderniser le droit positif, notamment, la question de la responsabilité. Qui doit être condamné pour usurpation d'identité au regard de la victime ? Où retrouver l'usurpateur ? Comment la victime peut-t-elle prouver qu'elle a fait l'objet d'une usurpation ?

Paragraphe 2. Les prémisses d'une reconnaissance d'un droit spécifique applicable en matière d'usurpation d'identité ?

Tant de questions auxquelles le droit a tenté tant bien que mal à apporter des réponses. Ces réponses se voient notamment par l'adoption de plusieurs projets de loi, nécessaires pour donner un goût de renouveau à la législation en vigueur. Cependant, il convient de préciser que malgré la mise en place de ces nouvelles lois, il est apparu que cela n'était pas suffisant pour réprimer efficacement le fraudeur, faute de véritable texte d'incrimination. C'est ainsi qu'en 2009, les pouvoirs publics se sont remis activement à rechercher un dispositif de lutte susceptible d'être efficace au regard de l'usurpation en ligne de l'identité, puis, l'adoption de la Loi d'orientation et de programmation pour la performance de la sécurité intérieure a crée en 2011 de toute pièce, un nouvel article dans le Code pénal, visant à pénaliser ce délit. Néanmoins, ces propos sont à nuancer car nous verrons que la pénalisation de ce délit connait toutefois des limites, et qu'il faut nécessairement aller vers la consécration d'un droit spécifique en matière d'Internet pour appréhender cette forme de cybercriminalité.

L'usurpation d'identité en ligne implique non seulement un regard nouveau sur les problématiques qu'elle engendre, mais également une nécessaire modernisation des dispositifs mis en place en matière de lutte. De ce point de vue, il est apparu nécessaire pour la norme de ne plus simplement avoir recours aux incriminations traditionnelles, directement inspirées des atteintes aux droits de la personnalité classiques. Elle a du, en effet, s'efforcer de trouver des solutions notamment au regard de la responsabilité : c'est-à-dire que dans la plupart des cas, l'usurpateur est difficilement retrouvable de sorte que les internautes ont abandonné leur confiance dans Internet.

A/ L'adoption successive de lois relatives à l'usurpation d'identité

L'impuissance du droit face aux nouvelles formes de cybercriminalité ont donné le ton, notamment au regard de la preuve de l'identité. En effet, comment la victime d'une usurpation peut-elle prouver qu'elle est bel et bien victime de cette infraction, dans la mesure où le véritable responsable n'est pas identifiable ? Ces diverses complexités ont amené les pouvoirs publics à adopter plusieurs projets de loi de 2002 à aujourd'hui, en vue d'améliorer ses lacunes en la matière. La notion de « sécurité » en matière d'informatique a pris son essence dans ces mêmes défaillances de sorte qu'il est possible de constater que la norme a tenté de moderniser son dispositif, afin d'évoluer, dans le même temps, que les communications électroniques. Mais comme nous le verrons, cet essai n'a pas eu l'effet escompté. En effet, le problème récurrent de ces dernières années est de savoir comment retrouver l'usurpateur car celui-ci, parfait connaisseur des nouvelles technologies est peu de fois identifiable. Le régime probatoire en matière d'usurpation d'identité a donc du être remanié afin de combler ce vide juridique.

Outre l'émergence des réseaux sociaux et d'Internet, le début des années 2000 a été marqué par de nombreux évènements liés à la criminalité. On pensera ainsi aux attentats du 11 septembre, la guerre en Afghanistan. Soucieux de la sécurité de leurs citoyens, les États n'ont de cesse pensé à la question de la « sécurité », et l'enjeu pour ces derniers était donc de limiter les crimes et la délinquance. Cette notion a été en France, l'objet d'une véritable réflexion afin d'assurer non seulement la sécurité des personnes, en vertu du principe « sécurité et de salubrité publiques », mais également la « sécurité informatique », car la montée en puissance des communications électroniques a également accru le nombre d'infractions commises en ligne. Véritable priorité pour les pouvoirs publics, la question de la sécurité a provoqué l'effet d'une bombe : celle-ci a engendré en effet, l'adoption de lois successives, preuve incontestable du fait que la législation éprouve des difficultés à encadrer les nouvelles formes de criminalité.

Ainsi, en 1995, une première loi est venue confirmer le caractère fondamental de cette notion afin de la garantir dans toute sa substance. En effet, la loi d'orientation et de programmation

relative à la sécurité du 21 janvier 1995[89] dispose dans son article premier que la sécurité est un droit fondamental, considérée de fait comme étant « une condition de l'exercice des libertés. » Si l'adoption de cette loi semble être un début de solution, il convient toutefois de préciser qu'elle n'a pas pour autant défini ce qu'était la sécurité, à l'instar de la notion d'identité. En d'autres termes, bien que ce dispositif permette de cerner les effets de la sécurité, à savoir, protéger les libertés individuelles des personnes contre un éventuel risque, le défaut de définition expresse va renforcer les lacunes du droit dans l'appréhension des nouvelles formes de criminalité.

Cet aspect s'est d'ailleurs notamment fait ressentir par la création d'une structure ad hoc,[90] susceptible de garantir le respect de la déontologie des personnes exerçant une activité dans le secteur de la « sécurité sur le territoire de la République »[91]. On pourrait penser que la création de cette autorité administrative indépendante était sans nul doute un moyen pour l'administration de se conforter dans l'idée selon laquelle une structure serait capable de gérer cet impératif de sécurité. En raison de ce sujet jugé comme étant sensible et du caractère fondamental de la sécurité, l'État n'était pas le mieux placé pour gérer les questions relatives aux libertés individuelles.

Rappelons en effet que celui-ci avait scandalisé les français dans sa volonté de créer un identifiant unique géré par l'informatique centralisée. Ce n'est donc qu'un an plus tard que l'on s'est véritablement intéressé à la question de la sécurité informatique, mise en avant par un projet de loi déposé devant le Parlement en 2001[92] relative à la sécurité quotidienne[93] qui consacrait en effet pour la première fois cette notion. Elle constitue la traduction de toutes les réactions de l'époque issues de l'accroissement de l'utilisation des systèmes informatiques et des risques de fraude qui y sont liés.[94] On pense notamment aux virus, capables de détruire tout un système et par conséquent, des milliers de fichiers relatifs aux données personnelles.

[89] L. n° 95-73 du 21 janv. 1995 d'orientation et de programmation relative à la sécurité.
[90] La CNDS.
[91] CNDS : www.defenseurdesdroits.fr/connaitre-son-action/la-deontologie-de-la-securite
[92] Projet de loi sur la société de l'information, Doc. parl. *A.N.*, n°3143, le 14 juin 2001
[93] L. n° 2001-1062 du 15 nov. 2001 pour la sécurité quotidienne
[94]BENSOUSSAN (A.), TESSALONIKOS (A.), « Risque informatique et sécurité juridique », *Gaz. Pal.*, 18 avr. 2002, n°108, p. 12.

Outre cette loi, un autre projet de loi d'orientation et de programmation pour la sécurité intérieure[95] a été présenté devant le Conseil des ministres en 2002 par le ministre de l'Intérieur de l'époque, et adopté par le Parlement quelques jours plus tard.

Concernant l'Informatique, cette mesure législative a eu pour effet de faire fusionner les fichiers respectifs de la police nationale et de la gendarmerie sur des informations relatives aux données personnelles des citoyens dans un seul et même système informatique : l'Ariane. Cette mesure a fait l'objet de vives critiques par les français, qui y voyaient une violation de leur vie privée, au même titre que le projet SAFARI des années 1970. En outre, la fusion de ces fichiers a provoqué le mélange de plusieurs données informatiques, cet accident ayant effrayé la population dans la mesure où une personne fichée pour avoir commis une infraction pouvait se retrouver innocente alors qu'une personne coupable d'aucun crime pouvait dès lors être accusée de meurtre à cause de cela.

Les pouvoirs publics ont dès lors crée l'effet inverse de ce qu'ils souhaitaient : plutôt que de rassurer les citoyens par le biais de mesures de « sécurité », ces derniers ont vraisemblablement crée de nouveaux risques pour les individus. Cette volonté de l'Etat d'accroitre son contrôle dans un domaine qu'elle ne saisit pas a fait l'objet de vives critiques de la part des citoyens lorsqu'une loi en date du 18 mars 2003[96] pour la sécurité intérieure a été adoptée. En effet, cette disposition a renforcé le contrôle des autorités judiciaires afin de lutter contre la criminalité. En matière informatique, celle-ci a introduit l'article 57-1 du Code pénal, afin d'autoriser le corps de police judiciaire à effectuer des perquisitions informatiques en vue de récupérer les données qui seraient susceptibles d'intéresser l'enquête.

Outre le fait de s'interroger sur le caractère liberticide de cette mesure, il convient d'annoter que cette loi tente de dissimuler les véritables obstacles que rencontre l'Etat en matière de sécurité informatique : l'adoption de toutes ces lois n'est en effet que le résultat de son impossibilité à pouvoir identifier le responsable d'une infraction commise sur les communications électroniques. C'est dans cet ordre d'idées que la loi de 2003 a crée et renforcé les pouvoirs de contrôle du corps policier en matière de nouvelles technologies[97]. Elle instaure une véritable collaboration avec les opérateurs de télécommunication. Ceux-ci, devront en effet, d'une part, communiquer les informations qui se retrouvent au sein du

[95] L. n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure.
[96] L. n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.
[97] CHARBONNEAU (C.), PANSIER (F.J.), « Présentation de la loi : de la LSQ à la LSI », *Gaz. Pal.*, 27 mars 2003, n°86, p. 2.

système informatique perquisitionné ou qui font l'objet d'un traitement (on pense principalement aux données nominatives) dans le cas où un officier de police judiciaire qui en fait la demande l'aura justifié pour « la manifestation de la vérité ». D'autre part, les opérateurs seront tenus de préserver « des informations consultées par les personnes utilisatrices des services fournis[98]. »

En effet, les obligations à la charge des opérateurs puis des hébergeurs de sites Internet ont vu le jour par un souci, non pas de sécurité informatique mais de sécurité juridique. C'est par ce point de vue que la Loi pour la Confiance dans l'économie numérique du 21 juin 2004 a vu le jour[99].

B/ Le réaménagement des droits de la personnalité sur les communications électroniques au regard de l'usurpation d'identité

Afin de renforcer la confiance des internautes concernant les communications électroniques, la loi pour la confiance dans l'économie numérique envisage de redonner cette confiance aux utilisateurs. De fait, elle a réorganisé les structures des communications électroniques, en précisant que certaines se rattachaient aux communications audiovisuelles, mais elle a également mis en place un régime de responsabilité pour les acteurs d'Internet, notamment au regard des hébergeurs de sites. Toutefois, cette loi n'a pas fait l'unanimité dans le cœur des français qui ont expressément soulevé leur mécontentement à l'égard de celle-ci alors même qu'elle est aujourd'hui encore considérée comme étant le socle d'un droit spécifique applicable à Internet[100]. Un rapport d'information déposé par la Commission des affaires économiques, de l'environnement et du territoire effectué par des députés explique notamment que la LCEN : « est d'abord la loi fondatrice de l'autonomie juridique de l'Internet. »

Les échos que cette loi a provoqué ont été notamment constitués au regard de l'article 6 de la LCEN, qui détermine le régime de responsabilité des fournisseurs d'accès à Internet et des

[98] Art. 60-1 CPP.
[99] L. n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[100] DIONIS (J.), ERHEL (C.), rapp. d'information, n° 627 déposé à l'A.N par la CAEET, *sur la mise en application de la LCEN*, 23 janv. 2008.

hébergeurs. Toujours dans l'idée de protéger les libertés individuelles caractérisées par les données personnelles, le législateur voulait marquer une nouvelle forme de responsabilité des acteurs de l'Internet en cas de violation des données personnelles. Or, le problème c'est que la responsabilité pénale de ces derniers ne peut être engagée que si un certain nombre de conditions sont remplies. Ces conditions sont, dans l'article 6 expressément mentionnées mais elles reposent sur des termes flous, au terme duquel, personne ne saurait agir efficacement. Par exemple, en cas de constatation illicite d'un contenu, les hébergeurs sont dans l'obligation d'agir « promptement » pour retirer ces contenus litigieux. Or, rien ne déterminait ce terme.

Ce n'est que très récemment que cette disposition a été timidement clarifiée : en 2011, la jurisprudence est intervenue pour préciser que l'obligation d'agir promptement signifiait que l'hébergeur devait agir le jour même de la notification du contenu illicite. Puis, La Cour d'Appel de Paris est venue rallonger ce délai à deux semaines[101]. Il en est ressorti que l'hébergeur, acteur privé pouvait être considéré comme étant un « juge », appréciant lui-même le caractère illicite ou non du contenu. La complexité de l'article 6 a naturellement conduit le Conseil Constitutionnel à se prononcer sur sa conformité à la Constitution[102]. Il a ainsi déclaré conforme sur certains points, et a apportée quelques précisions sur le régime particulier des hébergeurs.

Hormis ce défaut de précision, les critiques concernaient également la qualification du statut de l'hébergeur, dans la mesure où aucun texte ne définissait exactement ce statut. Par exemple, on ne savait pas si les acteurs de plateformes de vidéo pouvaient être considérés comme des hébergeurs et in fine, répondre à leur obligation posée audit article 6. Ce n'est qu'en février 2011, que la Cour de Cassation a pu répondre par l'affirmative sur ce point.[103] Cela signifie qu'il aura fallu près de 7 ans pour la jurisprudence de se prononcer sur les dispositions d'une loi, considérée pourtant aujourd'hui comme étant la consécration du droit de l'Internet. La mise en place d'un régime de responsabilité des hébergeurs a en outre provoqué la colère des professionnels du droit dans la mesure où cette loi est venue insérée un régime de responsabilité plus favorable[104] à leur égard dans la mesure où il s'agit d'une

[101] CA Paris, n°09/21941, 4 févr. 2011, Google France c/ Aufeminin.com et autres.
[102] Cons. Const., Commentaire de la décision n° 2004-496 DC du 10 juin 2004, *CCC.*
[103] Cass, n° 09-13.202, 17 février 2011, Dailymotion, Fuzz et Amen.
[104] LACHAUSSÉE (S.), « Le régime de l'hébergeur de données, 10 ans après sa création », *Le journal du Net*, 9 juil. 2013.

responsabilité limitée[105] mais sans pour autant définir les points essentiels tel que le statut de l'hébergeur[106].

Au regard de l'usurpation d'identité, cette loi est importante dans la mesure où elle oblige les acteurs d'Internet à conserver les données personnelles, et donc, des éléments qui permettent d'identifier les usurpateurs. Alors que cet aspect est primordial afin de ne pas porter atteinte aux libertés individuelles, la LCEN prive les hébergeurs d'une obligation de surveillance des informations transmises et stockées. Bien que cet aspect soit compréhensible parce qu'on ne pourrait imaginer que les hébergeurs voient leur responsabilité civile engagée systématiquement, la loi leur est favorable dans la mesure où ils verront leur responsabilité pénale engagée que s'ils ne remplissent pas leurs obligations précédemment citées.

Or, en matière d'usurpation d'identité, il y a un véritable paradoxe entre la rapidité des techniques de fraudes utilisées, et l'identification des données à la charge des acteurs de l'Internet. En d'autres termes, les pirates 2.0 auront déjà fait en sorte de « disparaitre » des communications électroniques avant même que les hébergeurs n'aient eu le temps d'identifier leurs données nominatives. Le retard du droit français face à l'évolution technique des communications électroniques l'a invité à créer de toute pièce un nouveau délit d'usurpation d'identité à l'image de ses voisins sensé être plus adapté à cette croissance rapide des moyens techniques de fraude.

Par ailleurs, le réaménagement des droits de la personnalité se traduit également par l'adoption du projet de la loi LOPPSI II qui permettra in fine d'introduire un article relatif à l'usurpation d'identité dans le code pénal. En effet, au moment de l'examen de cette loi, le Sénat avait annoncé dans un rapport d'information, sa volonté était en effet d'insérer le nouveau délit d'usurpation d'identité dans la partie du Code pénal consacrée aux atteintes à la personnalité et à la vie privée et non pas au sein de la partie consacrée la violence faite aux personnes[107].

[105] DIONIS (J.), ERHEL (C.), rapp. d'information, op.,cit.
[106] BARBRY (E.), « Internet est devenu au fil des années, un "droit spécial" », *Gaz. Pal*., 23 oct. 2010, n°296, p. 14.
[107] *S*., Rapp.d'information sur le projet de La LOPPSI 2 – chap. II, « Lutte contre la cybercriminalité ».

Seconde partie.

L'usurpation d'identité : un défi technique considérable pour le droit

Cette partie fera office d'analyse du rapport qui existe entre le droit et la technique. En effet, au fil du raisonnement, il sera plausible de constater que l'ineffectivité du droit au regard de l'usurpation d'identité en ligne est intimement liée à son manque de prise en considération de l'aspect technique.

La technique, en effet, constitue au sein des communications électroniques, leur pilier : elle peut tant produire des effets positifs sur la vie quotidienne, que devenir le vecteur principal d'abus. C'est de par l'amplification du nombre de victimes d'usurpation d'identité que le droit s'est véritablement intéressé à la technique. En effet, concernant ses effets négatifs, la technique permet aux cybercriminels d'abuser à leur guise des données nominatives relatives à d'autres personnes.

Ces cybercriminels connaissent toutes les failles techniques qu'il est possible de constituer sur les communications électroniques. Or, les professionnels du droit ne disposent pas de connaissances suffisamment précises dans ce domaine pour trouver un dispositif de lutte efficace.

En outre, la cybercriminalité est beaucoup plus rapide à se manifester que le droit lui-même. L'adoption successive de lois relatives à la sécurité que nous avons pu analyser précédemment est d'ailleurs significative du caractère désuet du droit. L'usurpation d'identité est devenue une priorité pour les pouvoirs publics : c'est parce qu'elle porte atteinte aux droits fondamentaux que ces derniers désirent plus que tout de la réprimer.

Ces derniers, se sont ainsi rendus compte que l'usurpation d'identité en ligne ne saurait être freinée s'ils ne devaient pas prendre en compte son aspect technique. En effet, rappelons que l'usurpation d'identité constitue un véritable moyen technique d'atteinte aux droits fondamentaux. (Chapitre 1).

Or, en guise de lutte contre cette dernière, le droit s'est entaché à créer un dispositif juridique, sensé combler ses lacunes en la matière. On verra que cette idée n'a pas suffi pour la norme de contrer ce délit et que les internautes se sont ainsi tout naturellement orientés vers la technique elle-même, considérée dès lors comme étant la seule solution de lutte contre l'usurpation d'identité aujourd'hui. (Chapitre 2.)

Chapitre Premier. L'usurpation d'identité en ligne, un outil technique d'atteinte aux droits fondamentaux

L'évolution croissante des moyens techniques de fraudes utilisés sur Internet a amené le législateur à créer de toute pièce un dispositif visant à lutter contre l'usurpation d'identité. Cette idée se retrouve principalement dans le titre même de la loi qui en est à l'origine, appelée Loi d'orientation et de programmation pour la *performance* de la sécurité intérieure.[108]

Cette loi trouve sa substance dans la LOPSI 1 adoptée quelques années auparavant, mais qui n'était pas suffisante pour offrir un arsenal juridique de lutte efficace, dans la mesure où elle ne prenait pas en compte l'aspect évolutif des moyens techniques de la cybercriminalité. Le terme de « performance », utilisé dans le titre même de la loi marque de fait la volonté des pouvoirs publics de prendre en compte ces dites évolutions, afin de réprimer efficacement ce délit.[109] Or, les méthodes employées par les cybercriminels s'avèrent plus rapides que la mise en place de ce nouveau dispositif de lutte. Il sera également possible de constater que les limites de ce nouveau dispositif ne sont pas seulement liées au critère temporel. En effet, la création du délit d'identité met en exergue le carcan juridique dans lequel les professionnels du droit se sont engouffrés. Plus largement, la mise en œuvre de cette norme est sensée réprimer les atteintes à la personne et donc in fine à protéger les internautes. Or, il s'avère que le droit s'est retrouvé face à un dilemme cornélien : protéger les droits fondamentaux d'une atteinte, ou protéger l'individu de ce cyber délit même si cela l'amène à porter une atteinte aux droits fondamentaux. Ce cercle vicieux constitue le cœur de l'impossibilité pour le droit de lutter contre l'usurpation d'identité.

[108] L. n° 2011-267 du 14 mars 2011 LOPPSI II.
[109] KLEITZ (C.), « LOPPSI 2 ou l'art de la surenchère », *Gaz. Pal.*, 16 sept. 2010, n°259, p. 3.

Section 1 - La création du délit d'usurpation d'identité : la prise en compte de la technique dans les moyens d'atteinte aux droits fondamentaux

Au moment de la présentation de cet énième projet de loi visant à lutter contre la cybercriminalité, Michèle Alliot-Marie avait notamment déclaré que : « l'adaptation du droit passera aussi par la création de nouvelles formes d'incrimination. »[110] Ainsi, cette nouvelle loi apporte en apparence de nouvelles formes d'incrimination, afin de limiter le recours au droit commun comme le juge avait pu le faire auparavant.[111]

Paragraphe 1. La création d'un délit visant à pénaliser l'usurpation d'identité

Ce nouvel aspect a été introduit dans l'article 226-4-1 du Code pénal, le but étant de réprimer des infractions qui ne sont pas susceptibles de tomber sous le couvert de l'article 434-23 du Code pénal. Il est apparu en effet essentiel pour les pouvoirs publics de réprimer les infractions commises sur les communications électroniques, de plus en plus nombreuses au regard de certains « cyber délits », notamment la pédopornographie, et dans ce présent cas : l'usurpation d'identité. En contradiction de cette idée, à l'occasion des débats parlementaires sur cette loi, le ministre de l'Intérieur de l'époque, Monsieur Brice Hortefeux a déclaré que : « le chemin parcouru depuis 2002 en matière de sécurité, n'est pas le fruit du hasard. L'amélioration constante, année après année, des chiffres de la délinquance globale, qui font incontestablement apparaître une tendance régulière à la baisse même s'il y a de nombreux points sur lesquels il faudrait, naturellement, que l'on progresse encore, est le résultat de mesures concrètes, de lois complémentaires et de textes ciblés[112]. » C'est dans cette optique que le nouveau délit d'usurpation d'identité a été introduit dans le Code pénal.

[110] ALLIOT-MARIE (M.), Discours prononcé à l'occasion de la présentation du plan de lutte contre la cybercriminalité, 14 février 2008, op., cit.
[111] MATTATIA (F.), « La création d'un délit d'usurpation d'identité sur Internet », *Gaz. Pal.*, 26 juill. 2008, n°208, p. 6.
[112] Déb. parl. S (CR) intégral des débats du 8 fév. 2011.

Il vient en quelque sorte compléter ce premier dispositif qui posait des problèmes de clarification et d'application de la règle, notamment en matière de fraudes liées à l'usurpation d'identité. Lors de l'examen de ce projet de loi, le Sénat a clairement fait comprendre sa prise de position sur le sujet, puisqu'il a en effet précisé que cette mesure : « reprend en substance les termes d'une proposition de loi déposée en juin 2005 par notre regretté collègue Michel Dreyfus-Schmidt.[113] » Pour rappel, la proposition de loi de juin 2005 à l'initiative de Michel Dreyfus-Schimdt tendait à la pénalisation de l'identité, et qui permettait également *in fine* de donner une force juridique à la notion d'identité numérique, afin de combler le vide juridique en la matière. Ainsi, le Ministre de l'Intérieur a-t-il déclaré à cet égard que le projet de loi a vocation à renforcer « la réponse pénale.[114]»

La nouvelle rédaction de ce délit porte sur des termes généraux qui ont vocation à s'appliquer également pour l'avenir. Cette rédaction est révélatrice de la volonté des professionnels du droit de s'adapter aux évolutions techniques au sein des communications électroniques. Plus précisément encore, cela permet de marquer une véritable prise de conscience de l'importance de la technique aujourd'hui.

Ainsi, cet article dispose-t-il que : « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature […] est puni d'un an d'emprisonnement et de 15 000 € d'amende. » Cependant, bien qu'il a été considéré que ce nouveau dispositif une sorte de consécration du droit à Internet, mais aussi d'un droit spécifique applicable en matière d'usurpation, il convient de noter qu'il ne définit pas à l'instar de l'article 434-23 du Code pénal, l'identité. Comment serait-il alors possible de consacrer un droit d'Internet alors que la notion fondamentale qu'est l'identité n'est toujours pas définie par ce nouvel article ?

Il est vrai que l'insertion de ce nouvel article dans le Code pénal constitue une création d'un délit susceptible de réprimer de nouvelles infractions, en tenant compte des évolutions techniques de moyens de fraude, mais il ne s'agit pas pour autant d'une consécration. Cet article tend plutôt *a fortiori* à une reconnaissance de l'aspect technique de l'usurpation d'identité que d'une consécration en tant que telle[115]. Cela signifie qu'au terme de cet article,

[113] S. Rapport d'information sur le projet de La LOPPSI 2 – chap. II, « Lutte contre la cybercriminalité », op., cit.
[114] S., (CR) rendu analytique officiel du 18 janv. 2011, LOPPSI, 2ème lecture.
[115] MARICHEZ (R.), « Une analyse technique du projet de loi LOPPSI à l'usage des professionnels de la sécurité de l'information », *Gaz. Pal.*, 23 juil. 2009, n°204, p. 22.

on comprend seulement que l'identité sur Internet peut évoluer au gré de la jurisprudence ainsi que par le biais du temps.

Paragraphe 2. Les limites du nouveau délit d'usurpation d'identité

Nonobstant cette tentative de consécration d'un nouveau droit applicable à la cybercriminalité, et tendant à la reconnaissance d'une protection de l'identité, la LOPPSI 2 a été vivement critiquée par les professionnels du droit, dans la mesure où elle accentue la volonté des pouvoirs publics d'user d'un système répressif pour les infractions commises sur les communications électroniques.

En réalité, la nouveauté de cet article tend en apparence à protéger davantage les droits de la personnalité, puisqu'il est question de réprimer l'usurpation d'identité lorsque celle-ci trouble d'une part la tranquillité de la personne victime de ladite usurpation ou celle d'autrui, ou lorsque celle-ci porte atteinte à son honneur ou à sa considération.[116] L'insertion de ce nouveau dispositif permet dès lors d'élargir la notion d'identité, de la délimiter bien qu'il ne fasse pas mention d'une définition formelle à son sujet. En effet, à la lecture de l'article 226-4-1 du Code pénal, il apparait que l'identité peut tout aussi bien concerner une personne physique qu'une personne morale. À titre d'exemple, il convient de rappeler que l'e-réputation faisait l'objet d'une confusion juridique lorsque l'on se référait à l'article 434-23 du Code pénal dans le sens où il n'était nullement mentionné un cas d'atteinte à ladite e-réputation. Dès lors, le principe d'interprétation stricte de la loi pénale empêchait une quelconque référence à l'e-réputation. Ce nouvel article tend à clarifier ce point de vue.

Hormis cette idée, les critères d'incrimination de l'usurpation d'identité rappellent les conditions de la diffamation,[117]qui reposent, également sur une atteinte à l'honneur ou à la considération de la personne, mais surtout sur une intention de nuire. C'est donc de manière déguisée que le législateur fait référence aux délits de presse, tendant ainsi plus précisément à réprimer de façon plus sévère un comportement qui aurait commis un tel délit.

[116] Art. 226-4-1 CP.
[117] Art 29 de la L. du 29 juillet 1881 sur la liberté de la presse.

L'aspect répressif qui est mis en avant par cette nouvelle disposition a d'ailleurs fait l'objet de vives critiques, dans la mesure où la doctrine a mis en garde d'une part sur une pénalisation qui tend à devenir un système « liberticide » des droits fondamentaux, d'autre part sur le fait que cette loi ne constitue en rien une innovation de la part du législateur, et qu'au contraire, elle tend à vider les droits de la personnalité de leur substance. Son incohérence est ainsi jugée du doigt, et la doctrine craint que ce dispositif aille renforcer les lacunes du droit en la matière au lieu de protéger les droits de la personnalité d'un côté, et les individus de l'autre.[118]

En outre, le ton général employé par cet article laisse une marge de manœuvre au juge dans l'appréciation de ce qui peut constituer une usurpation d'identité ou non.[119] On sait combien il est difficile pour le juge de trancher un litige lorsque deux droits fondamentaux sont en collision, il n'est ainsi impossible d'imaginer la difficulté par laquelle il devra juger un conflit sur la mise en balance de l'identité et d'un droit fondamental. Par exemple, lorsqu'une photo est publiée sur un réseau social à l'insu de la personne visible sur cette photo, et dans le cas où celle-ci souhaiterait la faire supprimer alors même que cette photo n'est pas préjudiciable, le juge optera-t-il pour la suppression au titre d'une usurpation d'identité au risque de porter atteinte à la liberté d'expression ?

Cette loi très controversée, notamment au regard de son article 4 a mis en exergue les inquiétudes de certaines associations concernant l'aspect liberticide de cette loi, notamment Reporter Sans Frontières qui déplore en effet qu'une autorité administrative puisse demander aux acteurs d'Internet de filtrer des contenus illicites (et précisément des sites à caractère pédopornographique.) L'association revendique en effet le mécanisme de filtrage qui, non seulement pourrait ouvrir la porte à d'autres atteintes aux droits fondamentaux, mais également parce que ce même filtrage est opéré par une autorité administrative[120], une autorité privée qui n'a pas compétence pour juger de la licéité ou non d'un contenu litigieux[121] contrairement à une autorité judiciaire ou publique. De la même façon, il est tout à fait plausible d'imaginer des atteintes à la liberté d'expression, dans le cas où la publication d'une photo d'un individu pourrait nuire à son honneur ou à sa réputation.

[118] DARSONVILLE (A.), « Décision n° 201 - 625 DC du 10 mars 2011 : une censure sévère de la LOPPSI 2 ? », *Constitutions*, 2011 p. 223.
[119] CHAMPEAU (G.), « Le gouvernement confirme la très grande largesse du délit d'usurpation d'identité », *Numerama*, 31 oct. 2011
[120] L'OCLCTIC
[121] MANENTI (B.), « Avec Loppsi, " la liberté d'expression est en danger " », Interview de Lucie Morillon, responsable du bureau Internet et Liberté chez RSF, *Le Nouvel Observateur*, 30 sept. 2010.

En d'autres termes, il semblerait en réalité que cette nouvelle disposition n'a pas pour effet de consacrer l'identité numérique, ni même le délit d'usurpation : elle confère aux pouvoirs publics le moyen de retrouver un véritable contrôle sur l'identité ainsi que sur les données personnelles des individus dans la mesure où le texte parle de « données de toute nature ». En outre, ce caractère général n'est pas vu d'un très bon œil, et c'est à l'occasion d'une question posée au Ministère de l'Intérieur par une sénatrice que les intentions du Gouvernement visant à contrôler les données personnelles ont été mises au grand jour. En effet, dans sa réponse[122], celui-ci parle du délit « d'utilisation malveillante » de l'identité ou des données personnelles. Ce terme a fait l'objet de vives critiques car il ne saurait possible de définir avec précision ce qu'est une utilisation malveillante.

Toutes ces raisons ont amené l'opposition à déposer un recours devant le Conseil Constitutionnel pour atteinte aux principes constitutionnels notamment au regard de l'article 4 du projet de loi relatif au filtrage opéré par une autorité privée.[123] Cet aspect avait fait l'objet d'une question prioritaire de constitutionnalité lorsqu'il a été question de savoir si la HADOPI était compétente pour suspendre la connexion Internet des internautes. Rappelons ainsi que l'appréhension des éventuelles atteintes à la personne ne date pas de cette loi. Pour démontrer cette difficulté, c'est pour cette raison que le Conseil Constitutionnel a censuré treize dispositions de cette loi.[124] Bien que l'objet de cette loi n'ait pas seule vocation à s'appliquer en matière d'identité, celle-ci met en lumière toutefois, le problème de la répression lorsqu'il s'agit de violer une liberté individuelle en vue de réprimer un comportement frauduleux.

Si pour certains, cette loi a été apparentée comme la consécration du délit d'usurpation d'identité, pour d'autres en revanche, la Loppsi 2 constitue un véritable « retour…en arrière. »[125] La censure de ce texte a sonné comme une mise en garde, dans le sens où la législation ne peut combattre l'usurpation d'identité par un système juridique répressif. Cette censure n'a été qu'une réponse de la part du Conseil des Sages au législateur de créer un dispositif cohérent, qui ne se réfèrerait plus aux anciennes incriminations pour en créer des nouvelles. Cela signifie en partie en effet, que le droit doit tenir en compte des véritables obstacles à l'encontre de l'identité afin de trouver un dispositif adéquat qui puisse lutter contre son usurpation. La législation aurait du prendre en compte en effet, la technicité des

[122] Rép.min. à la QE n°18540 du 15 mai 2011, J.*O. déb. parl. S.* (Q.) du 27 oct. 2011, p. 2762.
[123] Cons. Const. Commentaire de la décision n° 2011-625 DC sur la LOPPSI 2, *CCC*, 10 mars 2011.
[124] Anonyme, « LOPPSI II, acte final », *D. Étudiant, Actualité*, 18 mars 2011.
[125] KLEITZ (C.), « LOPPSI II, le retour…en arrière », *Gaz. Pal.*, 17 mars 2011, n°76, p. 3.

moyens de fraude utilisés au sein des communications électroniques, et d'apporter des solutions pour lutter dans ce sens. (*In fine*, les critiques opérées à l'égard de ce nouveau délit d'usurpation d'identité a provoqué une perte de confiance absolue de la part des français, qui ont fini par abandonner l'idée de disposer d'une protection efficace face à ce cyber délit. Par ailleurs, cette perte de confiance s'est très incontestablement accrue du fait qu'il est rarement possible d'identité l'usurpateur, et in fine, de le sanctionner[126].

Cette défaillance est d'autant plus visible dans le cas où l'usurpateur se situerait dans un pays étranger, entrainant ainsi de nouvelles complexités relatives aux règles de droit international privé, car deux normes opposées pourraient très facilement rentrées en conflit. De ce point de vue, il est donc nécessaire aujourd'hui d'appeler à une harmonisation des textes de lois de chaque pays, et précisément de mener une coopération internationale de lutte. Pour l'heure, le délit d'usurpation d'identité inscrit aussi bien dans l'article 434-23 du Code pénal que dans l'article 226-4-1 du même Code est remis en cause en raison de l'évolution technique des moyens de fraudes sur Internet, qui se prolifèrent plus rapidement que le droit.

[126] MATTHIOS (FJ.), « La création d'un délit d'usurpation d'identité sur l'Internet », *Gaz. Pal.*, 26 juillet 2008 n° 208, p. 6.

Section 2 - La remise en cause du délit d'usurpation d'identité au regard de l'évolution technique des moyens d'atteinte aux droits fondamentaux

L'adoption de lois successives n'est qu'un premier indice de la difficulté pour le droit d'appréhender les atteintes aux droits de la personne en raison du caractère évolutif des moyens d'usurpation. La difficulté réside en effet, non seulement au regard de ce critère temporal, mais également à cause de la technique elle-même. Les nouvelles technologies cumulées aux communications électroniques ont offert une véritable panoplie d'outils techniques visant à nuire aux internautes. Or, malgré cet argument de taille, les pouvoirs publics se sclérosent dans ce qu'ils connaissent, à savoir le droit, sans prendre en compte l'aspect technique des moyens d'infraction. L'adage populaire « œil pour œil, dent pour dent » illustre bien cette idée : le droit peut, et doit, combattre les moyens techniques d'usurpation d'identité en prenant lui aussi, des mesures à visée technique.

Cette section sera ainsi consacrée à l'aspect technique des moyens de fraude utilisés par les usurpateurs. La gageure est donc de taille pour le législateur, dans la mesure où les moyens techniques utilisés en vue d'usurper l'identité d'une personne constituent non seulement des atteintes aux droits patrimoniaux (paragraphe 1), mais également des atteintes à leurs droits extrapatrimoniaux[127]. (Paragraphe 2.)

[127] CNIL, « L'usurpation d'identité en questions », disponible sur le *site officiel de la CNIL*, www.cnil.fr, 17 mars 2011.

Paragraphe 1. L'usurpation d'identité en ligne, un outil technique d'atteinte aux droits patrimoniaux

Le véritable défi pour les pouvoirs publics n'est pas tant à consacrer un délit visant à pénaliser l'usurpation d'identité, mais bel et bien d'identifier l'usurpateur pour le réprimer. Or, bien souvent, le cybercriminel n'est pas identifiable, dans la mesure où ce dernier connait parfaitement les techniques pour se dissimuler au sein des communications électroniques. Les conséquences d'une atteinte à la personne sont dévastatrices : bien souvent, le criminel tend à usurper l'identité d'une personne afin de porter atteinte à ses droits extrapatrimoniaux. On pense principalement à l'usurpation des coordonnées bancaires, en vue d'opérer des paiements frauduleux. La plus célèbre de ces techniques est appelée « phishing », ou « hameçonnage » en français. Cette pratique réside dans le fait que l'usurpateur se fait passer pour une personne morale, généralement une grande entreprise, une marque, une administration ou une banque, ou pour une personne physique, et récupère à partir de sites factices les données personnelles des internautes. Les données personnelles permettent dès lors au pirate en ligne d'utiliser ces données pour effectuer des opérations frauduleuses sous le nom de la victime. Les données usurpées lui permettent également de pirater des boites de messagerie ou des comptes sur les réseaux sociaux dans le but de réaliser des arnaques.[128]

Les pouvoirs publics pensaient pouvoir réprimer cette pratique par le biais de l'article 313-1 du Code pénal, il convient de préciser que cette pratique est toujours aussi importante aujourd'hui, en raison du fait que les techniques employées pour détourner les données personnelles sont renouvelées, et de plus en plus perfectionnées. Par exemple, les banques sont les plus touchées par ce phénomène[129] ; dans la mesure où les pirates imitent à la perfection leur site Internet. Ils envoient ensuite un courrier électronique à des milliers de personnes sans pour autant les cibler précisément, afin de leurs demander de mettre à jour leurs coordonnées bancaires. Les plus crédules deviennent alors victimes de cette pratique et impuissantes face à la vitesse à laquelle leur compte bancaire débite. Afin de se faire indemniser auprès de leur banque, les victimes ont la possibilité de porter plainte, bien que cela ne soit pas obligatoire dans le cas où elles n'auraient bien entendu pas divulguer leur

[128] CNIL, « L'usurpation d'identité en questions », op., cit.
[129] FILLIAS (E.), VILLENEUVE (A.), *E-Réputation, Stratégies d'influence sur Internet*, op. cit., p. 231.

code à l'usurpateur. Elles pourront ainsi invoquer l'article L133-19 du Code monétaire et financier[130]. Or, deux problématiques se posent : la première concerne la preuve d'une usurpation d'identité : comment les victimes peuvent-elles prouver qu'elles ont bel et bien été victimes ? Si en matière d'état civil la preuve de l'identité se fait par tous moyens, il en découle que cela serait le cas également pour prouver son identité en ligne. Mais une pratique courante a été développée par les autorités de refuser le remboursement en cas de non présentation d'une preuve irréfutable d'une usurpation. Le remboursement est très souvent difficile à recevoir, d'autant plus que les banques exigent dans la pratique que les victimes aillent porter plainte en vue de retarder le processus d'indemnisation, alors que le ministère de la justice en août 2011 avait précisé aux services de l'ordre de ne plus enregistrer ces plaintes.[131] D'autre part, le second problème réside dans le fait qu'il n'existe pas de texte législatif qui définit et encadre expressément cette pratique. C'est donc par le biais du recours à d'autres infractions relatives au détournement des données personnes qu'il sera possible de lutter contre l'usurpateur, dans le cas où il est identifié. Mais cela n'arrive que peu souvent.

Outre cette technique, il existe des variantes du *phishing* : l'usurpateur ne va pas demander à l'internaute de lui délivrer des informations, mais il va en revanche, lui proposer de télécharger des logiciels qui sont en réalité des virus comme le Cheval de Troie. Le danger de ces virus est qu'ils permettent d'avoir accès aux mots de passes ainsi qu'aux codes de leur victime sans que celle-ci s'en rende compte immédiatement. Ce virus est en réalité un véritable outil d'espionnage que seul un professionnel en informatique sera susceptible de détruire. Or dans tous ces cas, et au regard de tout ce que l'on a pu dire auparavant, les cybercriminels, sont peu de fois identifiés ; de sorte que le droit ne peut rien faire contre ces pratiques.

En d'autres termes, les textes répressifs en la matière sont d'ores et déjà désuets. Ce n'est pas tant dans la répression que les professionnels du droit devraient s'orienter, mais au contraire, sur de la prévention. Ou du moins, créer des dispositifs législatifs visant à protéger en priorité les atteintes aux droits extrapatrimoniaux, et se mettre en conformité avec les pratiques dont il a connaissance. Par exemple, prévoir des lois qui favorisent la preuve de l'identité, par exemple par le biais d'une adresse IP qui aurait fait l'objet d'un vol et avec laquelle un usurpateur se serait amusé à envoyer des spams. Les juges devraient se mettre en

[130] MOREL-MAROGER (J.), « La répression des fraudes à la carte bancaire », op., cit.
[131] DARRIERE (R.), « "Phishing": que risquent les auteurs et leurs victimes ? », *Journal du Net*, 30 avr. 2013.

accord sur les éléments susceptibles d'être considérés comme une preuve d'usurpation. Après tout, l'usurpation peut toucher n'importe qui : personne morale, comme personne physique, bien comme droits de la personnalité. En 2013, il a été recensé plus de 60 000 tentatives signalées en matière de *phishing*, ainsi que le vol de plus de 800 000 données personnelles.[132]

Face à ce nouvel enjeu de taille, n'est-t-il pas temps pour le droit de penser à la protection des individus par le biais de textes moins répressifs mais plus en faveur des victimes ?

Enfin, il convient également d'analyser que l'usurpation d'identité ne touche pas seulement les droits patrimoniaux, puisqu'elle est également susceptible d'entrainer des atteintes aux droits extrapatrimoniaux.

Il existe également une autre pratique, située à la limite entre une atteinte aux droits patrimoniaux et extrapatrimoniaux qui concerne le « cybersquatting. » Cette pratique consiste à enregistrer un nom de domaine afin de le revendre de façon abusive. Le cybersquatteur va en effet déposer le nom d'une marque de renom afin de la faire chanter pour lui faire payer une somme inconsidérée et dans le but de retrouver le nom de domaine. La plus célèbre affaire de cybersquatting concernait le nom de domaine « wallstreet.com », enregistré en 1994 pour 70 dollars et revendu en 1999 pour la somme d'un million de dollars. Cette pratique est dangereuse dans la mesure où elle constitue une atteinte au carrefour de plusieurs droits : atteinte au droit de la propriété intellectuelle en vertu de l'article 731-1 du Code de la propriété intellectuelle et contrefaçon, de concurrence déloyale, d'atteinte au nom et à l'image de la marque, ou elle constitue une atteinte à l'identité. Cette pratique s'est proliférée en raison du fait que peu de formalités étaient à remplir pour enregistrer un nom de domaine. Dans les années 90 en effet, ce genre de pratique n'était pas monnaie courante.

La dangerosité tient également au fait que plusieurs dispositifs législatifs ont vocation à s'exprimer, de sorte qu'il faut remplir un certain nombre de conditions cumulatives selon le dispositif que l'on invoque pour se défendre[133]. Par exemple, il est possible pour la victime d'invoquer la contrefaçon, cumulée avec la concurrence déloyale. Mais les juges devront alors constater s'il existe un risque de confusion dans l'esprit de la clientèle. Le cumul de ces deux dispositifs nécessite la preuve d'une faute, d'un préjudice, et d'un lien de causalité. Ore cette

[132]MONDOLONI (M.), « Cinq conseils pour ne pas être victime de phishing », *Franceinfo*, 3 fév. 2014.
[133]HADDAD (S.), « Conditions liées aux actions civiles et sanctions du cybersquatting », *Legavox.fr*, 9 novembre 2010.

analyse prend du temps, et les entreprises ont besoin d'agir rapidement. En effet, la pratique démontre que le cybersquatting utilise des noms de domaine se terminant en « .com », de sorte que ces derniers ont la possibilité d'avoir une audience à l'échelle internationale[134]. De fait, le cumul d'incriminations rend en réalité une certaine incohérence, aussi bien pour déterminer quel sera le dispositif le plus adéquat à appliquer, et également en matière procédurale. Afin de lutter contre ces pratiques, il est nécessaire d'avoir une connaissance technique et parfaite des communications électroniques, savoir anticiper quels nouveaux obstacles ces dernières pourront mettre en place.

De plus, en matière de droits patrimoniaux, Internet a généré une véritable activité économique, qui se voit également notamment dans l'intitulé de la LCEN « loi pour la confiance dans l'*économie* numérique. » En conséquence, les juristes sont invités à se munir non seulement de sérieuses connaissances en matière juridique, mais également à connaitre la technique et qui plus est, l'économie. Pour certains auteurs en effet, l'usurpation d'identité est au carrefour de ces trois disciplines, et une analyse économique permettrait de mieux appréhender ce genre de pratiques[135]. Rappelons que la base de l'économie réside dans l'étude des pratiques sociales, reposant ainsi sur des faits et des analyses, qui ont des valeurs objectives. La prise en compte de ces divers domaines permettrait dès lors de lutter plus aisément contre des pratiques qui auraient vocation à atteindre les droits patrimoniaux. Cette idée pourrait également s'appliquer en matière de droits extrapatrimoniaux, car l'usurpation d'identité peut être un véritable outil technique d'atteinte à ces dits droits.

[134]HAAS (ME.), THORÉ (B.), « L'évaluation du préjudice dans les affaires de cybersquatting », *Gaz. Pal.*, 28 oct. 2000, n°302, p. 28.
[135] *Ibid*.

Paragraphe 2. L'usurpation d'identité en ligne, un outil technique d'atteinte aux droits extrapatrimoniaux

Le *phishing* peut également conduire l'usurpateur à s'attaquer aux personnes morales, et principalement aux entreprises de renom et à l'administration. Il s'agit non plus là pour l'usurpateur d'agir comme un « cyber escroc », attiré par l'appât du gain, mais plutôt par une personne qui souhaite seulement nuire à la réputation d'une personne physique ou morale. L'e-réputation est en effet, sans cesse l'objet de cyber crimes. Le vol des données personnelles de ces personnes permet généralement par la suite de créer de faux profils, blogs ou commentaires sous le nom de leur victime. Les réseaux sociaux ont favorisé ce genre de pratiques, véritables cauchemars pour les entreprises.

On se souvient tous par exemple de l'affaire de la SNCF qui avait fait l'objet d'une atteinte à sa réputation en 2013 sur le réseau social Twitter : un compte parodique de cette dernière répondait aux personnes qui se plaignaient de celle-ci. Bien qu'il s'agisse d'un compte parodique, la ressemblance avec la SNCF était telle qu'il aurait été loisible d'invoquer l'usurpation d'identité. Ce compte avait scandalisé en effet beaucoup de français qui ne s'étaient pas rendu compte qu'il s'agisse d'un compte parodique. Face aux plaintes des internautes, ce compte parodique donnait des réponses « irrévérencieuses » qui ont véritablement porté atteinte à l'e-réputation de la SNCF.

D'un point de vue plus concret en matière d'usurpation d'identité, on peut citer l'exemple d'un ex époux malheureux qui décide de créer un faux profil sur Facebook de son ex femme dans lequel il publie des photos de celle-ci en tenue désobligeante pour se venger. Ce genre d'affaires est très commun, et facile à réprimer dans la mesure où il est plausible de retrouver aisément le créateur du faux profil. Ainsi par exemple, en 2011, un homme avait été condamné pour avoir crée un faux profil sur Facebook sur lequel il avait ajouté en photo de profil son ancienne maitresse en sous-vêtements, et dans lequel il avait inséré des propos injurieux à l'égard de celle-ci. Il a été condamné à 5 mois de prison avec sursis ainsi qu'à payer 410 euros symboliques de dommages et intérêts.[136]

[136] JULIEN (L.), « Facebook : 5 mois de prison avec sursis pour un faux profil », *Numerama*, 26 juill. 2011.

Les cas d'atteinte à l'honneur ou à la réputation se multiplient de plus en plus du fait des réseaux sociaux. La multiplication des atteintes à la personne est liée au fait que la législation soit bien trop en retard par rapport à l'évolution des moyens techniques de fraudes. Certains ont critiqué la législation en la matière et souhaitent que soient instaurés des moyens d'authentification de l'internaute, au même titre que le mot de passe, qui permettrait de prouver notamment qu'il y a bien eu usurpation d'identité.

Démuni, le droit a pourtant essayé de remédier à ses lacunes en prévoyant plusieurs systèmes d'identification de l'individu, telle que la carte d'identité biométrique. Ces nouvelles solutions issues de 2012 dénotent l'obligation pour la norme de devoir prendre en compte la technique pour lutter efficacement contre ce délit. La question que l'on pourrait se poser serait celle de savoir si ces dernières solutions suffiront-elles à mettre fin à ce délit.

Chapitre Second. L'usurpation d'identité en ligne, le nécessaire recours à la technique comme solution de lutte

Malgré de nombreuses tentatives de lutte à l'initiative du Parlement, les dispositifs juridiques mis en place ne suffisent pas pour mettre fin à ces pratiques frauduleuses sur les communications électroniques. En effet, le caractère transfrontière de ces communications, cumulé à la liberté d'expression, voire de communication empêchent un contrôle accru des pratiques exercées sur ces dernières. En outre, le caractère évolutif des communications en ligne et a contrario, le caractère désuet du droit contre les nouvelles pratiques frauduleuses, toujours plus importantes et rapidement mises en place par rapport à l'adoption d'un texte, ont remis en cause l'efficacité du droit lui-même. Les lacunes du droit, aussi nombreuses que les pratiques frauduleuses 2.0 ont semé le doute chez les internautes concernant leur protection. Ces derniers ont tourné le dos au droit pour privilégier des solutions techniques (section 2.) C'est de par ce constat que le droit a tenté, de lutter contre des techniques, par la technique, en mettant en place des dispositifs non plus juridiques stricto sensu, mais qui s'apparentent davantage en véritables outils.

En 2012, la lutte contre la cybercriminalité ne se fait plus tant par l'adoption de textes à visée répressive comme le droit a pu le faire ces dernières décennies, mais par la matérialisation des textes, c'est-à-dire par la mise en place de procédés d'authentification (section 1). S'il est possible de remettre en cause cette énième étape dans le processus de lutte contre la cybercriminalité, on peut toutefois saluer la volonté du législateur d'innover par la création d'éléments techniques de protection.

Section 1 - Le droit 2.0 : la prise en compte de la technique comme solution de lutte contre l'usurpation d'identité

Le développement du commerce électronique, des objets connectés, ou encore des supports de communication ont ligne ont sans aucun doute inspiré la norme dans la prise en compte des nouvelles technologies pour lutter contre l'usurpation d'identité. En 2012, le droit compte bien mettre définitivement un terme à ce délit 2.0 en créant de toute pièce une nouvelle loi[137] dont l'objectif est de faciliter cette lutte. (Paragraphe 1.) Cette loi tend en effet à créer notamment une carte d'identité biométrique avec un système de puce électronique afin d'authentifier l'identité des individus. Or, cette initiative fera l'objet de vives controverses qui amèneront le Conseil Constitutionnel à se prononcer sur la constitutionnalité d'une telle mise en œuvre. Dès lors, il sera possible de constater que ce dispositif n'est qu'un dispositif de plus, jugé comme étant inadapté au regard des pratiques de fraude, de sorte que la seule solution fonctionnelle mise en place par la cyberjustice est la mise en place d'une certaine prévention (Paragraphe 2.)

[137] L. n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.

Paragraphe 1. La mise en place de mécanismes d'authentification comme solution juridique de lutte au regard de l'usurpation

Le 6 mars 2012, le Parlement adopte la loi relative à la protection de l'identité qui a vocation à mettre en place d'une part, une carte d'identité biométrique, d'autre part, un fichier des empreintes digitales[138]. Les pouvoirs publics, conscients de leurs erreurs passées, ont semblé innover avec de telles mesures. Ces derniers avaient en effet pris en compte les essentielles lacunes juridiques susceptibles d'être réparées, car il est vrai, qu'il est impossible de faire « du droit à coup de marteau[139] » et de remettre en question tout le système juridique. Ces lacunes réparables concernent avant toute chose, la preuve par la victime d'une usurpation d'identité. Si pour la législation autorise en matière d'identité d'état civil que la preuve de l'identité se fasse par tous moyens, c'est donc par syllogisme que cette loi instaure une nouvelle fois cette règle, au sein de son article 1er. Néanmoins, c'est l'article 2 de la loi, relatif au contenu des titres d'identité qui a fait l'objet de controverses. Cet article dispose que : « la carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :

a) le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;

b) le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;

c) son domicile ;

d) sa taille et la couleur de ses yeux ;

e) ses empreintes digitales ;

f) sa photographie.

Le présent article ne s'applique pas au passeport délivré selon une procédure d'urgence ».

[138] MATTATIA (F.), « La loi sur la protection de l'identité est-t-elle conforme à la Constitution ? », *LPA*, 24 avr. 2012, n°82, p. 6.
[139] « *Faire de la philosophie à coup de marteau* » est la citation initiale, dont l'auteur est le philosophe Nietzche.

Dans cet article, ce n'est pas tant le contenu qui a été très critiqué mais la qualité de la personne ayant été à l'initiative de cette loi. En effet, rappelons pour l'essentiel, que les données relatives à un support d'identité dépendent du règlement et non pas de la loi. La preuve en est en matière civile, où ce sont les mairies, et donc par définition, l'Administration qui assurent la gestion de l'identité. Cet article met une nouvelle fois en exergue, le conflit de compétences entre le judiciaire et l'administratif, à l'image des évènements d'actualité. Prenons l'exemple de la géolocalisation où des polémiques ont vu le jour en raison d'un conflit de légitimité entre les magistrats du Parquet et le « juge » à proprement parler[140], ou l'existence d'un filtrage opéré par une autorité privée et non judiciaire[141]ou encore le refus de donner compétence à la HADOPI de suspendre la connexion internet des utilisateurs[142] ou encore la gestion des noms de domaine sur Internet[143].

Il convient de souligner que dès lors qu' s'agit de porter atteinte à une liberté individuelle sur les supports de communication en ligne, il est souvent mis en avant le conflit de légitimité entre l'autorité compétente pour maitriser nos données personnelles, et celles qui n'ont pas *es qualite* pour le faire. C'est en partie pour cette raison que cette loi a fait l'objet d'une question prioritaire de constitutionnalité.

En outre, la loi prévoyait une puce obligatoire, aussi appelée puce « régalienne » dans laquelle il aurait été inséré les données d'identité et les données biométriques visées à l'article 1 précité. La norme prévoyait également une deuxième puce, facultative pour faciliter les usages en rapport avec les services en ligne comme la signature électronique. Compte tenu du succès du paiement en ligne, la signature électronique aurait eu pour vocation de permettre l'authentification d'une entreprise ou d'un particulier[144]. Elle aurait pu également être utilisée en matière de transactions bancaires.

Toutefois, il convient de faire quelques remarques au sujet de ces innovations techniques. En effet, bien qu'il est incontestable de noter la volonté du législateur d'innover en matière de lutte, ces outils d'authentification ne répondent pas à la protection des données personnelles, dans la mesure où elles ont vocation à divulguer davantage notre identité. On pense

[140] ALLAIN (E.), « Le magistrat du parquet n'est pas un juge pour la Cour de cassation », *Forum Pénal Dalloz*, 26 oct. 2013.
[141] MANENTI (B.), « Avec Loppsi, " la liberté d'expression est en danger " », op., cit.
[142] Cons. Const., n° 2009-580 DC, 10 juin 2009.
[143] Cons. Const., n° 2010-45 QPC, 6 octobre 2010.
[144] *A.N.*, Rapp. d'informations, « police et sécurité : protection de l'identité », disponible sur le site de l'*A.N* : http://www.assemblee-nationale.fr/13/dossiers/protection_identite.asp

notamment aux empreintes digitales, qui ne semblent pas, a fortiori nécessaires, pour démontrer son identité. Autrement dit, il semble que cette nouvelle loi va à l'encontre de tous les principes sur lesquels le droit se réfère pour lutter contre les infractions en ligne. En effet, tout au long de ce travail de recherche, il a été possible de constater que le droit faisait toujours référence au droit commun, et surtout aux droits fondamentaux (droits de la personnalité principalement) pour lutter contre l'usurpation d'identité. Or, un tel dispositif est porteur de risques sur notre identité, portant atteinte *in fine* aux droits de la personnalité. Une nouvelle fois, la législation montre une certaine incohérence, ce qui renforce d'autant plus le gouffre juridique dans lequel elle s'est immiscée.

D'ailleurs, il semblerait que le droit tente, une nouvelle fois, avant tout d'avoir le contrôle sur la gestion des données personnelles, et ce point de vue est d'ailleurs démontré par cette loi, dans la mesure où il avait été question de créer un fichier central d'empreintes biométriques[145]. Toutes ces contestations ont d'ailleurs fait l'objet de la même prise de position du Conseil Constitutionnel qui, saisit d'une question prioritaire de constitutionnalité, a déclaré non conforme à la Constitution, les articles 2 et 3 de cette loi en considérant que celles-ci portaient atteintes au droit au respect de la vie privée.[146] En outre, il déclare non conforme à la Constitution le fichier central d'empreintes biométriques qui s'apparenterait à une forme de « police administrative ou judiciaire » dans la mesure où il serait utilisé à d'autres fins « que la vérification de l'identité d'une personne[147]. » Considérée comme vidée de sa substance[148], cette loi n'a pas produit l'effet désiré ; laissant le législateur, impuissant, ainsi que les victimes d'usurpation d'une quelconque protection efficace.

La seule solution restante pour la norme est donc de faire l'inverse de ce qu'elle faisait : c'est-à-dire prévenir des risques plutôt que d'essayer de réprimer les cybers pratiques frauduleuses.

[145]SOULLIER (L.), « La loi sur l'usurpation d'identité adoptée, un fichage controversé », *L'Express*, 6 mars 2012.
[146]Cons. const., déc. n° 2012-652 DC, 22 mars 2012.
[147]LARRALDE (JM.), « Largement vidée de son contenu par le Conseil constitutionnel, la loi du 27 mars 2012 n'atteint pas les objectifs initialement poursuivis par le législateur », *L'Essentiel, Droit de la famille et des personnes*, n°5, p. 3.
[148]*Ibid*.

Paragraphe 2. La prévention comme seule solution juridique de lutte adaptée au regard de l'usurpation

Faute de dispositif efficace, on peut observer sur la toile un certain nombre de sites officiels destinés à faire de la prévention. Si pour certains il vaut mieux « prévenir que guérir », il semblerait que c'est aussi l'attitude qu'a décidé d'avoir la législation. Sur divers sites d'autorités, il est ainsi possible de constater un certain nombre de conseils visant à éviter de se faire usurper l'identité. Ainsi par exemple, la CNIL préconise le changement régulier de mot de passe afin d'éviter une usurpation plus aisée de la part du mal intentionné.[149] D'autres comme la HADOPI conseille de ne pas se connecter en wi-fi sur des sites sensibles telle que la banque, éviter de répondre à des courriers dont on ne connait pas le destinataire, ou encore d'insérer des protections anti-virus adéquates[150]. La direction générale de la concurrence, de la consommation et de la répression des fraudes incite les victimes à signaler un abus d'utilisation de données personnelles sur des plateformes de signalement spécialement conçues à cet effet[151].

D'une manière générale, il est possible de constater sur chaque page d'accueil des sites officiels la présence de liens utiles renvoyant vers d'autres sites officiels sur lesquels il existe des fiches pratiques de prévention.

Par ailleurs, force est de noter que la prévention est aujourd'hui le seul moyen de limiter les risques d'usurpation d'identité sur les réseaux sociaux, risques qui seraient liés aux droits extrapatrimoniaux. En effet, en matière de droits patrimoniaux, l'usage de la technique se veut plus aisée dans la mesure où les supports utilisés pour usurper des données identitaires font l'objet eux-mêmes de nouvelles technologies. On pense notamment au paiement en ligne, ou encore la carte de paiement sans contact. Mais, lorsqu'il s'agit de la publication d'une photo outrageante, ou plus largement d'une atteinte à l'e-réputation, la technique ne semble pas être la plus à même pour lutter contre ces infractions. La prévention reste donc la seule manière pour les autorités de mettre en garde les internautes sur les risques liés aux communications

[149] CNIL, « L'usurpation d'identité en questions », *www.cnil.fr*, 17 mars 2011, disponible sur : http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/lusurpation-didentite-en-questions/

[150] HADOPI, « Quels sont les risques d'usurpation d'identité sur Internet ? », déc. 2011, *pdf*, disponible sur : http://www.hadopi.fr/sites/default/files/page/pdf/UsurpationIdentite.pdf

[151] DGCCRF, « Phishing, (hameçonnage ou filoutage) », *economie.gouv.fr*, 2 août 2013, disponible sur : http://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage

électroniques. Cela s'explique notamment par le fait que les supports technologiques utilisés en matière de fraudes financières notamment sont matérialisés, ces supports sont eux-mêmes des outils d'usurpation alors que les atteintes aux droits de la personnalité rendent plus difficiles l'identification de l'usurpateur.

Enfin, le célèbre moteur de recherche : Google, a également fait de la prévention dans une rubrique intitulée « combattre l'usurpation d'identité[152] » en mettant en avant les techniques qu'il a mis en place pour les internautes. Ainsi par exemple, ce dernier a crée des « avertissements d'activités sur le compte » de messagerie, ou encore en précisant qu'il chiffre la connexion entre la boite de messagerie de l'internaute et Google afin de dissuader les pirates en ligne d'usurper l'adresse de messagerie. Ce dernier démontre que seuls des moyens techniques peuvent aider à combattre ce fléau numérique.

[152] GOOGLE, « Combattre l'usurpation d'identité », *google.fr*, disponible sur : http://www.google.fr/intl/tr/safetycenter/everyone/cybercrime/identity-theft-help/

Section 2. Les limites du droit 2.0 : la technique comme seule solution de lutte contre l'usurpation d'identité

Face à l'impuissance du droit en la matière, les internautes se sont naturellement orientés vers la technique, considérée comme seule solution de lutte efficace contre l'usurpation d'identité. Il est apparu depuis quelques mois des moyens pour limiter le risque de se faire usurper ses données personnelles. Ainsi par exemple dans le secteur banquier, la majorité des banques ont mis en place un système de paiement sécurisé. A ce titre, de nouvelles notions techniques ont vu le jour. Tel est le cas par exemple du chiffrement SSL favorisant la sécurité et la sécurisation des données nominatives. Ce codage permet de camoufler les données chiffrées notamment relatives aux cartes bancaires, qui se traduisent par le fait par exemple de payer avec Paypal.[153]

Par ailleurs, Visa et MasterCard de leur côté ont crée le système 3D Secure, permettant le paiement en ligne de façon sécurisée. Les banques se sont munies de ce système pour lutter contre les fraudes fiscales liées aux usurpations d'identité. Cela leur permet de mettre en œuvre des moyens d'authentification de la personne titulaire de la carte utilisée pour le paiement en ligne : en effet, au moment du paiement en ligne, il s'agit de recevoir un SMS de la banque dans lequel est renfermé un code confidentiel que le payeur doit entrer au moment de l'achat afin de prouver qu'il est bien le propriétaire de la carte. Outre ces moyens techniques utilisés par les banques, il existe aujourd'hui des adresses sécurisées, notamment sur les réseaux sociaux. Pour vérifier que l'adresse est sécurisée, il suffit de regarder l'adresse elle-même : dans le cas d'une adresse sécurisée en effet, il sera alors possible de voir indiquer la mention : « https:// ».

Toutefois, on pourrait s'intéresser à la question de savoir si ces moyens de sécurisation ne deviendront pas eux aussi, des moyens pour usurper l'identité des personnes. Par exemple Bitcoin fait beaucoup parler de lui pour sa fonction novatrice en matière de paiement.

[153] La banque postale, « Paiements sécurisés sur Internet », labanquepostale.fr, disponible sur : https://www.labanquepostale.fr/associations-gestionnaires/services/dons_cotisations/paiement_distance/paiement_securise_internet.html

Il s'agit d'un réseau de paiement libre et ouvert, « sans autorité centrale »[154], qui a l'ambition de devenir une nouvelle forme de monnaie en ligne. Ce genre d'innovation « sensible » laisse imaginer les nouvelles techniques d'usurpation qu'il sera possible de voir au sein des communications électroniques.

Du fait de la nature transfrontière des réseaux sociaux, ne serait-il pas plus judicieux de moderniser les dispositifs mis en place en matière de sécurisation, ainsi que d'harmoniser la législation des États à l'effigie de la Directive de 1995 relative aux données personnelles ?

[154] V. p. d'accueil du sitebitcoin.org.fr/

CONCLUSION

A l'ère du numérique, la question de l'usurpation d'identité, et plus généralement de la cybercriminalité n'est pas résolue. Pourtant, en raison du caractère transfrontalier des communications électroniques, cet obstacle aurait du être surmonté depuis longtemps. L'impuissance des États pour lutter face à la hausse des cybercrimes devrait laisser sa place à une coopération internationale, une coopération qui serait à même de triompher sur ces infractions.

Au niveau européen, l'idée d'une harmonisation et de modernisation des régimes en vigueur est proche de se concrétiser grâce à l'adoption d'un projet de règlement européen. Ce texte a en effet, vocation à reprendre la Directive de 1995 relative à la protection des données personnelles, considérée comme un modèle de législation pour tous les États membres de l'Union.

L'usurpation d'identité résume à elle-seule toutes les problématiques auxquelles ces derniers doivent faire face : d'une part, il serait tant de répondre à la question essentielle que nous avons pu constater tout au long de ce processus de réflexion : comment concilier les libertés individuelles avec les intérêts qui sont propres à chaque État ? Particulier, ou entreprise, chaque personne est concernée par ce phénomène de crise. L'économie numérique pour laquelle les législations ont fait d'elle un objectif prioritaire doit également être remise au goût du jour. Le phénomène de la cybercriminalité vide ces objectifs de toute leur substance.

Or, on peut constater que l'individu lato sensu reste le cœur même de ces débats : l'économie numérique ne pourrait éclore sans la présence des entreprises, la liberté d'expression ne serait pas si chère à la Cour Européenne des Droits de l'Homme si elle n'était pas à l'image même de l'individu. Si les individus (et entités) sont au carrefour de ces différents aspects, les législations devraient se mettre en conformité pour les protéger. Car les protéger, c'est également se protéger elles-mêmes.

La cybercriminalité a déjà eu bien nombre d'effets dévastateurs au sein de chaque pays, provoquant de facto la perte de confiance des internautes envers les communications

électroniques. Or, celles-ci sont aujourd'hui ancrées dans les mœurs, il serait ainsi dommage de ne pas réussir à les maitriser.

Le potentiel qu'elles gardent précieusement est prêt à être cueilli. Doter les individus d'un « haut niveau protection européen », le défi reste alors pour les Etats de s'entendre sur la législation à mettre en œuvre afin d'éviter des conflits en matière de la détermination de la loi applicable, ainsi qu'en matière d'exequatur. D'autant plus que la technique ne peut plus être mise de côté dans ce combat. Elle doit, en effet, nécessairement s'allier au droit pour lutter efficacement contre la cybercriminalité.

Malgré l'attente de l'adoption de ce projet européen, il existe aujourd'hui, un début de « révolution » numérique alliant la technique et le domaine juridique : le droit à l'oubli, ou aussi connu sous l'expression de « droit au déférencement. » Aujourd'hui les attentes sont sur le point d'être comblées par l'apparition de cette nouvelle notion. En effet, le droit à l'oubli a vocation à permettre à tout un chacun de se faire tout bonnement « oublier » pour des faits qu'il lui serait préjudiciable.

La démocratisation de ce droit est attendue de près par les internautes, mais il semblerait que les choses commencent à évoluer dans un sens propice à la consécration du droit à l'oubli. En effet, la Cour de Justice de l'Union Européenne a su donner le ton en la matière puisqu'elle a su plier Google, le géant des moteurs de recherche à se conformer à sa législation.[155]

Elle a en effet jugé que ce dernier était responsable du traitement des données à caractère personnel qui apparaissent sur des pages web publiées par des personnes autres que celles concernées par ces données. Il s'agit pour ce dernier d'utiliser des moyens techniques, à savoir le référencement, pour supprimer des liens renvoyant vers les pages contenant les données à caractère personnel. De fait, Google a mis en place un dispositif de signalement en ligne par le biais duquel les internautes peuvent déposer leur requête afin de voir cesser leur préjudice.

Ainsi, le droit à l'oubli met en exergue toutes les problématiques liées à l'usurpation d'identité : il s'agit en effet d'un début de réponse visant tout d'abord à moderniser le

[155] CJUE, 13 mai 2014, AEPD et Mario Costeja Gonzáles c/ Google.

dispositif de lutte contre la cybercriminalité, de part l'union de la technique et du droit, d'autre part à doter les internautes d'un niveau de protection inébranlable, susceptible de lutter contre ces infractions 2.0.

Toutefois, affirmer qu'il sera possible un jour de lutter contre toutes les infractions en ligne n'est que pure hérésie : une coopération internationale ne suffit pas pour mettre fin à la cybercriminalité. Non seulement il serait nécessaire de créer une coopération à l'échelon mondial, or, cela n'est pas possible dans la mesure où les Etats ne disposent pas du même régime politique. Mais également, il serait indispensable de former les professionnels du droit à la technique : ce n'est en effet, qu'en ayant acquis des connaissances spécifiques sur ce sujet qu'il sera alors possible de lutter efficacement contre la cybercriminalité.

Pour l'heure, les Etats, mais aussi les internautes attendent avec impatience l'officialisation du projet de règlement européen, considéré aujourd'hui comme étant le seul protecteur des individus.

BIBLIOGRAPHIE

I – OUVRAGES GÉNÉRAUX ET SPÉCIALISÉS

BOULOC (B.), *Droit pénal général*, Dalloz, éd. 2011, 732 p.

BRUBAKER (R.), *« Au-delà de « l'identité »*, Actes de la recherche en sciences sociales, 2001, 85 p.

CODE CIVIL 2009, Dalloz, 108e éd., 2745 p.

CODE MONÉTAIRE ET FINANCIER, *Commenté sous la direction de* MARTIN (D.), LexisNexis, 8e éd., 2014, 2621 p.

CODE PÉNAL 2014, Dalloz, 111e éd., 3458 p.

CORNU (G.), *Vocabulaire juridique*, Coll. Puf, 9e éd., 1093 p.

COURBE (P.), *Droit civil, les personnes, la famille, les incapacités*, Dalloz., 7e éd., 2009, 294 p.

DE FELCOURT (G.), *L'usurpation d'identité, ou l'art de la fraude sur les données personnelles*, Coll. Arès, CNRS Éditions, 2011, 320 p.

FÉRAL-SCHUHL (C.), *Cyberdroit : le droit à l'épreuve d'Interne*t, Dalloz, 6e éd., 2011, 1100 p.

FILLIAS (E.), VILLENEUVE (A.), *E-Réputation, Stratégies d'influence sur Internet*, Coll. Ellipses, 2e éd., 2012, 293 p.

ITEANU (O.), *L'identité numérique en question*, Coll. Eyrolles, 2008, 166 p.

LAMIZET (B.), *Politique et identité*, Coll. Pul, éd. 2002, 350 p.

MARTIN (M.), *Le pseudonyme sur Internet : une nomination située au carrefour de l'anonymat et de la sphère privée*, éd. L'Harmattan, Coll. Langue et parole, 2006, 180 p.

RAPP (L.), *Le courrier électronique : e-mail*, Coll. Puf, Que sais-je ?, 1998, 127 p.

RÉPERTOIRE DE DROIT CIVIL, Dalloz, éd., 2014, 11 vol., 297 rubriques, 9444 p.

SARTRE (J.P.), *Huis Clos* suivi de *Les mouches*, Coll. Folio, éd.2000, 245 p.

SCHERER (E.), *La révolution numérique : glossaire*, Dalloz, 1ère éd., 2009, 193 p.

E BOOK – LIVRES NUMÉRIQUES

CAPRIOLI (E.), MATTATIA (F.), et VULLIET-TAVERNIER (S.), *L'identité numérique, Cahiers de droit de l'entreprise*, mai 2011, n°3, [En ligne] : bit.ly/1ul30Vt

ERTZSCHEID (O.), *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies*, Nouvelle édition, Marseille OpenEdition Press, 2013, 73 p. [En ligne] : http://books.openedition.org/oep/332

TRUCHE (P.), FAUGÈRE (JP.) et FLICHY (P.), *Administration électronique et protection des données personnelles*, *Livre Blanc*, 129 p., [En ligne] :

http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000100/0000.pdf

II - DOCTRINE, ARTICLES, INTERVENTIONS

ARTICLES DE REVUES

ARRIGO (P.), « La cybercriminalité : vers une régulation internationale de l'Internet ? », *Gazette du Palais*, 16 octobre 2001, n°289, p. 35.

BARBRY (E.), « Internet est devenu au fil des années, un "droit spécial" », *Gazette du Palais*, 23 octobre 2010, n°296, p. 14.

BENSOUSSAN (A.) : « Vers la consécration de l'identité numérique », *Gazette du Palais*, 23 avril 2011, n°113, p. 3.

BENSOUSSAN (A.), TESSALONIKOS (A.), « Risque informatique et sécurité juridique », *Gazette du Palais*, 18 avril 2002, n°108, p. 12.

BRIAT (M.), « La cybercriminalité », *Petites Affiches*, 6 février 2004, n°27, p. 25.

CHARBONNEAU (C.), PANSIER (F.J.), « Présentation de la loi : de la LSQ à la LSI », *Gazette du Palais*, 27 mars 2003, n°86, p. 2.

COSTES (L.), « Le transfert CSA-Hadopi devrait passer sur une loi sur la culture en 2014 », *Lamy*, 20 septembre 2013.

COURBOULAY (M.), « Panorama de jurisprudence sur les litiges impliquant les noms et le droit des marques », *Gazette du Palais*, 29 décembre 2012, n°364, p.7.

DARSONVILLE (A.), « Décision n° 2011-625 DC du 10 mars 2011 : une censure sévère de la LOPPSI 2 ? », *Constitutions*, 2011 p. 223.

DUPUY-BUSSON (S.), « La liberté d'expression sur Internet : les réseaux sociaux (Facebook, Twitter...) ne sont pas des zones de non-droit », *Petites Affiches*, 15 juillet. 2010, n°140, p. 10.

FALQUE-PIERROTIN (I.), « La Constitution et l'Internet », *Nouveaux Cahiers du Conseil Constitutionnel*, 1er juin 2012, n°36, p. 31.

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

HAAS (ME.), THORÉ (B.), « L'évaluation du préjudice dans les affaires de cybersquatting », *Gazette du Palais*, 28 octobre 2000, n°302, p. 28.

HASSLER (T.), « La crise d'identité des droits de la personnalité », *Les Petites Affiches*, 7 décembre 2004, n°244, p. 3.

KLEITZ (C.) :

* « LOPPSI 2 ou l'art de la surenchère », *Gazette du Palais*, 16 septembre 2010, n°259, p. 3.

* « LOPPSI II, le retour…en arrière », *Gazette du Palais*., 17 mars 2011, n°76, p. 3.

LAROCHE-GISSEROT (F.), « Pseudonyme », *Répertoire de droit civil*, Dalloz, avril 2014.

LARRALDE (JM.), « Largement vidée de son contenu par le Conseil constitutionnel, la loi du 27 mars 2012 n'atteint pas les objectifs initialement poursuivis par le législateur », *L'Essentiel, Droit de la famille et des personnes*, n°5, p. 3.

MARICHEZ (R.), « Une analyse technique du projet de loi LOPPSI à l'usage des professionnels de la sécurité de l'information », *Gazette du Palais*, 23 juillet 2009, n°204, p. 22.

MARINO (L.), « Les nouveaux territoires des droits de la personnalité », *Gazette du Palais*, 19 mai 2007, n°139, p. 22.

MATTATIA (F.) :

* « Internet face à la loi Informatique et Libertés : l'adresse IP est-elle une donnée à caractère personnel ? » *Gazette du Palais*, 15 janvier 2008, n°15, p. 9.

* « La création d'un délit d'usurpation d'identité sur Internet », *Gazette du Palais*, 26 juillet 2008, n°208, p. 6.

* « La loi sur la protection de l'identité est-t-elle conforme à la Constitution ? », *Petites Affiches*, 24 avril 2012, n°82, p. 6.

MATTHIOS (FJ.), « La création d'un délit d'usurpation d'identité sur l'Internet », *Gazette du Palais,* 26 juillet 2008 n° 208, p. 6.

MOREL-MAROGER (J.), « La répression des fraudes à la carte bancaire », *Gazette du Palais*, 2 juin 2012, n°154, p. 12.

MOURON (P.), « L'identité virtuelle et le droit "sur" l'identité », *Lamy Droit de l'immatériel 2010*, n°64, octobre 2010.

PERRAY (R.), « Adresse IP et données personnelles : un besoin de convergence d'interprétations entre juges », *Gazette du Palais*, 30 avril 2009, n°120, p. 6.

PRUD'HOMME (M.), « L'usurpation d'identité numérique : bientôt un nouveau délit », *Gazette du Palais*, 24 avril 2010, n°114, p. 8.

RAYNOUARD (A.), « Actualité du droit des nouvelles technologies », *Defrénois*, 15 novembre 2002, n°21, p. 1407.

TÜRK (P.), « La souveraineté des États à l'épreuve d'Internet », *Droit public de la science politique en France et à l'étranger*, 1er novembre 2013, n°6, p. 1489.

VASSEUR-LAMBRY (F.), « L'identité de la personne humaine », Les *Petites affiches*, 6 mai 2004.

YAYON-DAUVET (A.), « Le devenir de la protection des données personnelles sur Internet », *Gazette du Palais*, 13 septembre 2001, n°256, p. 2.

ARTICLES SUR INTERNET

ANONYME, « LOPPSI II, acte final », *Dalloz Étudiant*, Actualité, 18 mars 2011.

ALLAIN (E.), « Le magistrat du parquet n'est pas un juge pour la Cour de cassation », *Forum Pénal Dalloz*, 26 octobre 2013.

BARBRY (E.), « Le droit du mail », *Journal du Net*, 31 octobre 2000.

BOUCHER (P.), « Safari ou la chasse aux Français », *Le Monde*, 21 mars 1974.

CNIL, « L'usurpation d'identité en questions », disponible sur le *site officiel de la CNIL*, www.cnil.fr, 17 mars 2011.

CHAMPEAU (G.), « Le gouvernement confirme la très grande largesse du délit d'usurpation d'identité », *Numerama*, 31 octobre 2011.

DARRIERE (R.), « "Phishing": que risquent les auteurs et leurs victimes ? », *Journal du Net*, 30 avril 2013.

DUPONT-CALBO (J.), PEPIN (G.), « Menacée, la Hadopi fait le dos rond », *Le Monde*, 10 octobre 2013.

JOFFRIN (L.), « 70 ans après : les 12 mystères du Débarquement », *Le Nouvel Observateur*, 6 juin 2014.

JULIEN (L.), « Facebook : 5 mois de prison avec sursis pour un faux profil », *Numerama*, 26 juillet 2011.

LACHAUSSÉE (S.), « Le régime de l'hébergeur de données, 10 ans après sa création », *Le journal du Net*, 9 juillet 2013.

MANENTI (B.), « Avec Loppsi, "la liberté d'expression est en danger" », Interview de Lucie Morillon, responsable du bureau Internet et Liberté chez RSF, *Le Nouvel Observateur*, 30 septembre 2010.

MONDOLONI (M.), « Cinq conseils pour ne pas être victime de phishing », *Franceinfo*, 3 février 2014.

PASOTTI (M.), « Défendre son e-réputation grâce au droit pénal », *Le Journal du Net*, 27 décembre 2009.

SOULLIER (L.), « La loi sur l'usurpation d'identité adoptée, un fichage controversé », *L'Express*, 6 mars 2012.

III - NOTES, OBSERVATIONS, COMMENTAIRES ET CHRONIQUES DE JURISPRUDENCE

BARBRY (E.), DUFIEF (V.), Note sous TGI de Carcassonne, 16 juin 2006, *Gazette du Palais*, 19 octobre 2006, n°292, p. 36.

MONNET (Y.), Note sous Cass., 30 mai 2007, *Gazette du Palais*, 8 mars 2008, n°68, p. 23.

CONSEIL CONSTITUTIONNEL, Commentaire de la décision n° 2004-496 DC du 10 juin 2004, *Cahiers du Conseil Constitutionnel*.

CONSEIL CONSTITUTIONNEL, Commentaire de la décision n° 2011-625 DC sur la LOPPSI 2, *Cahiers du Conseil Constitutionnel*.

IV - DISCOURS OFFICIELS, INTERVENTIONS

DISCOURS OFFICIELS

ALLIOT-MARIE (M.), Discours prononcé à l'occasion de la présentation du *plan de lutte contre la cybercriminalité*, 14 février 2008, disponible sur : www.interieur.gouv.fr/Archives/Archives-de-Michele-Alliot-Marie-2007-2009/Interventions/14.02.2008-Lutte-contre-la-cybercriminalite

COURTOIS (JP.), *Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure*, Rapport au ministre de l'Intérieur, juin 2010.

SAPIN (M.), Discours prononcé à l'occasion de la remise du rapport *Administration électronique et protection des données personnelles*, 26 février 2002, disponible sur : http://www.fonction-publique.gouv.fr/ministre/presse/discours-140

DÉLIBÉRATIONS

CNIL, Délibération n°2006-294, 21 décembre 2006.

INTERVENTIONS

GHICA-LEMARCHAND (C.), « L'interprétation de la loi pénale par le juge », Paris, Colloque organisé au Palais du Luxembourg, les 29 et 30 septembre 2006, www.senat.fr/colloques/office_du_juge/office_du_juge9.html

Groupe de travail « Article 29 » sur la protection des données, Avis 4/2007 *sur le concept de données à caractère personnel*, adopté le 20 juin 2007, pdf, http://www.cnpd.public.lu/fr/publications/groupe-art29/wp136_fr.pdf

OCDE, « Document exploratoire sur le vol d'identité en ligne », DSTI/CP(2007)3/FINAL, Réunion ministérielle de l'OCDE : *le futur de l'économie Internet*, organisée à Séoul, Corée, le 17 et 18 juin 2008, DSTI/CP(2007)3/FINAL, p.17, pdf, http://www.oecd.org/fr/sti/40699509.pdf

V - DROIT POSITIF

JURISPRUDENCE

CJUE, 13 mai 2014, AEPD et Mario Costeja Gonzáles c/ Google.

CEDH, 7 décembre 1976, *Handyside* c/ Royaume-Uni.

Cons. Const., n° 2004-496 DC du 10 juin 2004.

Cons. Const., n° 2009-580 DC du 10 juin 2009.

Cons. const., n° 2012-652 DC du 22 mars 2012.

Cons. Const., n° 2010-45 QPC, 6 octobre 2010.

Cass. Civ., 16 *mars 1841*.

Cass. Com., 12 mars 1985, n° 84-17163.

Cass. Com., 25 avril 2006, n° 04-15641.

Cass. Crim., 27 octobre 1999, n° 98-86.017.

Cass. crim., 8 avril 2009, n° 08-86.481.

Cass, n° *09-13.202, 17 février 2011, Dailymotion, Fuzz et Amen.*

Cass. Crim., 25 janvier 2012, n° 10-83.350.

Cass. Soc., 2 octobre 2001, n° 99-42942.

CA de Paris, 5 mai 2005.

CA de Paris, Pôle 5, chambre 5, 3 octobre 2013, Rentabiliweb Europe c/ Hi-Media.

CA Paris, n°09/21941, 4 février 2011, Google France c/ Aufeminin.com et autres

TGI Bobigny 14 décembre 2006, *Laurent F.* c/ Sacem et autres.

TGI Saint-Brieuc 6 septembre 2007, Ministère public, SCPP, SACEM c/ JP.

TGI de Paris, 5 mars 2009, Roland Magdane c/ Youtube.

TGI de Paris, 24 novembre 2010, Omar S. c/ Alexandre P.

LOIS

Loi du 29 juillet 1881 sur la liberté de la presse.

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

Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.

Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure.

Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.

VI - SITES ET RESSOURCES ELECTRONIQUES

http://actualitesdudroit.lamy.fr/

http://www.assemblee-nationale.fr/

http://www.cnil.fr/

http://www.conseil-constitutionnel.fr/

http://www.courdecassation.fr/

http://www.dalloz.fr/

http://www.doctrinal.fr/

http://www.eur-lex.europa.eu/

http://www.fonction-publique.gouv.fr/

http://www.hadopi.fr/

http://www.inpi.fr/

http://www.insee.fr/

http://junon.univ-cezanne.fr/u3iredic/

http://lamyline.lamy.fr/

http://www.laquadrature.net/

http://www.legalis.net/

http://www.legifrance.gouv.fr/

http://www.lemonde.fr/

http://www.lexisnexis.fr/

http://www.lextenso.fr/

http://www.oecd.org/fr/

http://www.senat.fr/

http://www.service-public.fr/

http://www.village-justice.com/

Le Monde - 21 mars 1974

Safari ou la chasse aux Français

Rue Jules-Breton, à Paris-13e, dans des locaux du ministre de l'intérieur, un ordinateur Iris-80 avec bi-processeur est en cours de mise en marche. A travers la France, les différents services de police détiennent, selon la confidence faite par un très haut magistrat, 100 millions de fiches, réparties dans 400 fichiers. Ainsi se trouvent posées — et, à terme, théoriquement résolues — les données d'un problème comprenant, d'une part, l'énormité des renseignements collectés ; de l'autre, la méthode à définir pour faire de cet ensemble une source unique, à tous égards, de renseignements.

L'histoire du très puissant appareil qu'est l'Iris-80 est exemplaire du secret qui entoure l'épanouissement de l'informatique dans les administrations, quelles que puissent être les informations qui filtrent ici et là.

Puissant, cet Iris-80, une comparaison le démontre sans contestation. L'appareil employé pour engranger les données de l'opération Safari, qui concerne l'identification individuelle de l'ensemble des 52 millions de Français, a une contenance de 2 milliards d'octets; celle de l'ordinateur du ministère de l'intérieur est de 3,2 milliards d'octets.

C'est dire que la mise en route d'Iris-80 — dont la location coûte 1 million de francs chaque mois — a été précédée d'études, de tests, pour en éprouver les possibilités. D'autant qu'à lui seul il doit remplacer les trois CII 400 et le 10070 de la C.I.I. qu'employait jusqu'alors la Place Beauvau.

De vastes ambitions

C'est sur ce dernier ordinateur qu'ont eu lieu les essais. Pour 20 % de sa capacité, il a été consacré à la gestion du personnel communal de la Ville de Paris. Mais, pour le reste (80 %), il a servi à tester les programmes devant être fournis à l'Iris-80, afin de rendre cohérentes entre elles les données contenues dans les 400 fichiers que possèdent les services de police : renseignements généraux, direction de la surveillance du territoire, police judiciaire, etc.

A titre d'anecdote, on peut rappeler que ce 10070 de la C.I.I., à l'origine, budgétairement, n'était pas du tout prévu pour la tâche qu'il a finalement assurée, mais pour « traiter » les données administratives du Fichier national des constructeurs (F.N.C.). Il s'agit donc apparemment d'un détournement manifeste de crédits d'études, ce qui n'était sans doute pas le vœu du Parlement qui les vota.

Il n'y a pas que cela. Le ministère de l'intérieur a d'encore plus vastes ambitions. Détenteurs, déjà, du fichier national du remembrement, les services de M. Jacques Chirac font de grands efforts pour, affirme-t-on, s'en adjoindre d'autres : le cadastre, le fichier de la direction nationale des impôts et, plus grave peut-être, celui du ministère du travail.

De telles visées comportent un danger qui saute aux yeux, et que M. Adolphe Touffait, procureur général de la Cour de cassation, avait parfaitement défini le 9 avril 1973 devant l'Académie des sciences morales et politiques, en disant : « *La dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques.* »

PHILIPPE BOUCHER.
(21 mars 1974.)

BOUCHER (P.), « Safari ou la chasse aux Français », *Le Monde*, 21 mars 1974, disponible sur : http://www.delis.sgdg.org/menu/nir/PresseLeMonde19740321.pdf

TABLE DES MATIÈRES