L'adaptation du droit pénal aux réseaux sociaux en ligne

Elie Stella

UNIVERSITE DE LORRAINE | Institut François Gény
École doctorale de Sciences Juridiques, Politiques, Économiques et de Gestion

L'ADAPTATION DU DROIT PÉNAL AUX RÉSEAUX SOCIAUX EN LIGNE

THÈSE

en vue de l'obtention du grade de

Docteur en droit privé et sciences criminelles

Présentée et soutenue publiquement le 12 décembre 2019 par

Élie STELLA

MEMBRES DU JURY :

Frédéric STASIAK
Professeur de droit privé et sciences criminelles à l'Université de Lorraine
Directeur de recherches

Jean-Baptiste THIERRY
Maître de conférences de droit privé et sciences criminelles à l'Université de Lorraine
Co-directeur de recherches

Emmanuel DREYER
Professeur de droit privé et sciences criminelles à l'Université Paris I Panthéon-Sorbonne
Rapporteur

Agathe LEPAGE
Professeur de droit privé et sciences criminelles à l'Université Paris II Panthéon-Assas
Rapporteur

Nathalie DROIN
Maître de conférences de droit public à l'Université de Bourgogne

Evan RASCHEL
Professeur de droit privé et sciences criminelles à l'Université de Clermont Auvergne

UNIVERSITE DE LORRAINE | Institut François Gény
École doctorale de Sciences Juridiques, Politiques, Économiques et de Gestion

L'ADAPTATION DU DROIT PÉNAL AUX RÉSEAUX SOCIAUX EN LIGNE

THÈSE

en vue de l'obtention du grade de

Docteur en droit privé et sciences criminelles

Présentée et soutenue publiquement le 12 décembre 2019 par

Élie STELLA

MEMBRES DU JURY :

Frédéric STASIAK
Professeur de droit privé et sciences criminelles à l'Université de Lorraine
Directeur de recherches

Jean-Baptiste THIERRY
Maître de conférences de droit privé et sciences criminelles à l'Université de Lorraine
Co-directeur de recherches

Emmanuel DREYER
Professeur de droit privé et sciences criminelles à l'Université Paris I Panthéon-Sorbonne
Rapporteur

Agathe LEPAGE
Professeur de droit privé et sciences criminelles à l'Université Paris II Panthéon-Assas
Rapporteur

Nathalie DROIN
Maître de conférences de droit public à l'Université de Bourgogne

Evan RASCHEL
Professeur de droit privé et sciences criminelles à l'Université de Clermont Auvergne

L'université n'entend donner ni approbation ni improbation aux opinions émises dans cette thèse, celles-ci devant être considérées comme propres à leur auteur.

À Nello, Robert et Nini

Remerciements

À mes directeurs de recherches, Monsieur le Professeur Frédéric Stasiak et Monsieur Jean-Baptiste Thierry, pour la confiance qu'ils m'ont accordée tout au long de mon travail et pour leurs conseils précieux et avisés m'ayant incité à me surpasser.

À l'ensemble du personnel, des enseignants, docteurs et doctorants de l'Institut François Gény et particulièrement à Anne, Marie-Claude, Pierre, Justine, Amélie, Constantin, Mitch, les fidèles au poste Valérie et Eugène, les enseignants plein d'avenir Mathieu, Guillaume, Julie et Catherine.

À mes fidèles amis Pierre, Olivier, Fred, Adèle, Ugo, Jean, Sarah et notamment ceux qui ont partagé mon quotidien en tant que colocataires Cyprien, Nicolas, Carlos, Chris, Maria, Clément.

Bien entendu aux Strauss et aux Straussettes.

À ma Duesenberg.

À mes parents et ma famille qui ont toujours soutenu mes choix et mes projets.

À Esther pour ton soutien indéfectible, pour ta personne, pour nos projets à venir.

Sommaire

Liste des principales abréviations

Adde	Ajouter
AJ Pénal	Revue *Actualité juridique de droit pénal*
AJDA	Revue *Actualités juridiques de droit administratif*
al.	Alinéa
AN	Assemblée Nationale
Art.	Article
Ass. plén.	Assemblée plénière
Bibl.	Bibliothèque
Bull.	Bulletin des arrêts de la Cour de cassation
c/	Contre
Cass.	Arrêt de la Cour de cassation
CDPH	Conseil de prud'hommes
CE	Conseil d'État
CEDH	Cour européenne des droits de l'Homme
Ch.	Chambre
Chron.	Chronique
Civ.	Chambre civile de la Cour de cassation
CJCE	Cour de justice des Communautés européennes
CJUE	Cour de justice de l'Union européenne
CNCDH	Commission nationale consultative des droits de l'Homme
CNRS	Centre national de la recherche scientifique
Coll.	Collection
Com.	Chambre commerciale de la Cour de cassation
Concl.	Conclusions
Cons. const.	Conseil constitutionnel
Conv. EDH	Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales
CCC	Revue *Contrats Concurrence Consommation*
CCE	Revue *Communication Commerce Electroniques*
CNIL	Commission Nationale de L'informatique et des Libertés
Comm. EDH	Commission européenne des droits de l'Homme
Cour EDH	Cour européenne des droits de l'Homme
CSA	Conseil Supérieur de l'Audiovisuel
CSI	Code de la sécurité intérieure
CPI	Code de la propriété intellectuelle
C. Pén.	Code pénal
C. Proc. pén.	Code de procédure pénale
Crim.	Chambre criminelle de la Cour de cassation
D.	Revue *Recueil Dalloz*
D. actu.	Revue *Dalloz actualité*
(dir.)	Sous la direction de
Dr. pén.	Revue *Droit pénal*
éd.	Édition
Fasc.	Fascicule
Gaz. Pal.	Revue *La Gazette du Palais*
Ibid.	Ouvrage ou article précité
infra	Ci-dessous

J.-Cl.	Encyclopédie *Jurisclasseur*
JCP	Revue *La Semaine Juridique*
***JCP* E**	Revue *La Semaine Juridique, édition Entreprise*
***JCP* G**	Revue *La Semaine Juridique, édition Générale*
JORF	Journal Officiel de la République Française.
L.	Loi
LCEN	Loi pour la Confiance dans l'Économie Numérique
LGDJ	Édition *Librairie général de droit et de jurisprudence*
LPA	Revue *Les petites affiches*
obs.	Observations
op. cit.	Œuvre citée
obs.	Observation
p.	Page
pp.	Pages
Préc.	Précité
PUF	Presses universitaires de France
PUAM	Presses universitaires d'Aix-Marseille
rapp.	Rapport
RevDH	*Revue des droits de l'homme* (en ligne)
RDLF	*Revue des droits et libertés fondamentaux*
REDC	*Revue européenne de droit de la consommation*
Rép. Pén. Dalloz	Répertoire de droit pénal et de procédure pénale Dalloz
Req.	Requête
RFDA	*Revue française de droit administratif*
RGPD	Règlement général sur la protection des données
RLDI	*Revue Lamy droit de l'immatériel*
RPDP	*Revue pénitentiaire et de droit pénal*
RSC	*Revue de science criminelle et de droit pénal comparé*
RTD Civ.	*Revue trimestrielle de droit civil*
RTDE	*Revue trimestrielle de droit européen*
RTDH	*Revue trimestrielle des droits de l'Homme*
S.	Revue *Recueil Sirey*
suiv.	Suivants
supra	Ci-dessus
somm.	Sommaire
TGI	Tribunal de grande instance
TI	Tribunal d'instance
v.	Voir
V°	*Verbo*, mot

Introduction

« *Les civilisations se transforment – elles sont mêmes mortelles, a dit Paul Valéry – et il est naturel de découvrir dans la législation pénale les traces des modifications qu'elles subissent* »[1]

1. Le « *village global* »[2] des réseaux sociaux en ligne. Depuis leur apparition au milieu des années 2000, les sites de réseaux sociaux constituent un phénomène en perpétuelle croissance dont l'importance dépasse aujourd'hui toutes les prédictions initiales. Plus encore, l'intensification de la communication permise par ces derniers semble avoir atteint un point encore inconnu dans l'histoire de l'humanité. La Terre comprend aujourd'hui environ 7,6 milliards d'habitants dont 55 % ont un accès à internet, soit environ 4,2 milliards d'internautes. Parmi ces internautes 76 % disposent d'un compte de réseau social correspondant à plus de 3,2 milliards d'utilisateurs. Ces chiffres sont en constante augmentation avec plus de 320 millions d'utilisateurs en plus recensés entre fin 2017 et fin 2018[3]. Parmi ces acteurs d'internet, le site Facebook est le réseau social le plus populaire avec plus de 2,4 milliards d'utilisateurs mensuels actifs[4], le plaçant ainsi en position dominante. Ces sites ont pour principale caractéristique de favoriser une intensification massive et diversifiée des relations interpersonnelles. Cette affirmation peut être illustrée au regard des chiffres enregistrés pour l'année 2019 du réseau social Facebook[5] selon lesquels chaque jour plus de 4,5 milliards de *like* sont distribués, 4,75 milliards de contenus sont partagés et 10 milliards de messages sont envoyés. Enfin, chaque minute, 350 gigaoctets de données sont échangées. Plus que jamais, l'expression du « *village global* » exprimée par Marshall

[1] R. MERLE, A. VITU, *Traité de droit criminel. Droit pénal spécial*, éd. Cujas, 1982, p. 14, n° 7.
[2] M. McLUHAN, *The Medium is the Message*, Bantam Books, 1967.
[3] Blog du modérateur, « Les 50 chiffres à connaître sur les médias sociaux en 2019 », chiffres publiés le 2 janvier 2019.
<https://www.blogdumoderateur.com/50-chiffres-medias-sociaux-2019> (dernière consultation le 9 octobre 2019).
[4] Blog du modérateur, « Les chiffres Facebook – 2019 », chiffres publiés le 4 juillet 2019 et mis à jour le 14 août 2019.
<https://www.blogdumoderateur.com/chiffres-facebook> (dernière consultation le 9 octobre 2019).
[5] *Ibid.*

McLuhan pour qualifier les effets engendrés par la mondialisation et les médias de masse revêt un sens particulier.

2. Les enjeux soulevés par les réseaux sociaux en ligne. Ces chiffres démontrent toute l'ampleur et le statut spécifique acquis progressivement par les réseaux sociaux en ligne au sein de notre société. Ces sites ont en moins de quinze ans changé nos usages et notre rapport au monde. Cette évolution s'est faite dans un premier temps pour le meilleur, en témoigne le rôle joué par les réseaux sociaux numériques dans les printemps arabes[6]. Plus généralement, ces sites jouent désormais un rôle démocratique majeur en donnant à tout citoyen l'aura dont seuls certains journalistes disposaient auparavant. De ce point de vue, les réseaux sociaux en ligne apparaissent donc comme une évolution souhaitable de la société humaine. Cependant, en organisant une intensification des rapports humains, les réseaux sociaux en ligne favorisent indubitablement une multiplication des comportements cyberdélinquants, voire l'émergence de nouvelles formes de délinquance à l'échelle numérique. Pire encore, la dimension hégémonique prise par ces derniers et leur capacité d'intrusion dans l'intimité de leurs utilisateurs amène la comparaison avec le spectre de la société de surveillance imaginée par George Orwell dans son roman d'anticipation *1984*[7]. Certains s'effraient même que l'opacité des traitements et des flux de communication aboutissent au conformisme anticipatif[8] dénoncé par Frantz Kafka dans le livre *Le Procès*[9]. Ce n'est pas la technologie en elle-même qui est le problème, mais l'humain par sa façon de l'utiliser ou de l'administrer. Partant, le droit, spécialement le droit pénal, a pleinement vocation à s'immiscer dans son fonctionnement afin de tenter de relever les enjeux majeurs que représentent aujourd'hui les sites de réseaux sociaux. Il convient dans ce cas de préciser l'objet et le contexte de l'étude avant de préciser le cadre de son analyse juridique. Ainsi, le nouvel ordre social initié par les réseaux sociaux en ligne (**Section 1**) révèle de nouveaux enjeux juridiques, particulièrement en droit pénal (**Section 2**).

[6] V. sur le sujet : D. M. FARIS, « La révolte en réseau : le « printemps arabe » et les médias sociaux », *Politique étrangère*, vol. printemps, nº 1, 2012, pp. 99-109.
[7] G. ORWELL, *1984*, Éd. Gallimard, 1950.
[8] Y. POULLET, *La vie privée à l'heure de la société du numérique*, Éd. Larcier, coll. CRIDS, p. 38.
[9] F. KAFKA, *Le Procès*, Éd. Gallimard, 1933.

Section 1 : Les réseaux sociaux en ligne, initiateurs d'un nouvel ordre social

3. Loin de se présenter comme un épiphénomène, les réseaux sociaux en ligne s'affirment aujourd'hui comme un acteur central et spécifique au sein d'internet suscitant des problématiques sociétales nouvelles. La notion et les contours des réseaux sociaux en ligne doivent être cernés (**§1**) avant de présenter leur impact sociétal (**§2**).

§1. Notion et contours des réseaux sociaux en ligne

4. Avant de s'attacher au contexte de l'essor des réseaux sociaux en ligne (B), il convient de revenir sur l'apparition et le développement de la notion de réseau social (A).

A. Apparition et développement de la notion de réseau social

5. Ébauche de définition du réseau social. La notion de réseau social peut se définir en s'attachant à chacun des deux mots qui la composent. Dans un premier temps, la notion de réseau renvoie à une grande variété d'objets et de phénomènes[10]. La racine du mot réseau se retrouve au XVII^{ème} siècle dans le mot *rets* désignant un filet, un ouvrage de cordes ou de fils à grosses mailles servant à la chasse ou à la pêche[11]. À partir du XVIII^{ème} siècle le mot se retrouve dans le langage médical avec les termes de réseau sanguin ou encore de réseau nerveux. Au XIX^{ème} l'usage de ce mot se généralise et sert notamment à désigner l'ensemble des routes, des voies navigables, des lignes aériennes ou des chemins de fer, qui relient différentes régions entre elles. Le terme s'est progressivement distancié des objets auxquels il était rattaché pour finalement désigner un certain nombre de propriétés générales intimement entremêlées[12]. Dans un sens général, le terme réseau renvoie aujourd'hui à un ensemble formé de lignes ou d'éléments qui communiquent ou s'entrecroisent[13]. Dans un second temps, l'adjectif social désigne pour sa part ce qui se rapporte à une société, à une collectivité humaine considérée comme une entité propre[14]. Le réseau social peut alors se définir comme l'ensemble des liens et des relations de toute nature au sein d'un groupe de personnes de plus

[10] P. MERCKLE, *La sociologie des réseaux sociaux*, La Découverte, 3ème éd., 2016, p. 7.
[11] <https://www.cnrtl.fr/definition/rets> (dernière consultation le 9 octobre 2019).
[12] P. MERCKLE, *La sociologie des réseaux sociaux, op. cit.*, p. 7.
[13] Dictionnaire Larousse en ligne, *V°* Réseau.
<https://www.larousse.fr/dictionnaires/francais/réseau> (dernière consultation le 9 octobre 2019).
[14] Dictionnaire Larousse en ligne, *V°* Social.
<https://www.larousse.fr/dictionnaires/francais/social> (dernière consultation le 9 octobre 2019).

ou moins grande importance. Cependant, le terme réseau social désigne avant tout un concept sociologique qu'il convient de mettre en évidence.

6. Apparition du concept de réseau social en sociologie. Le terme réseau social est apparu en 1954 sous la plume de l'anthropologue et sociologue John Arundel Barnes suite à une étude ethnologique de la population de l'île norvégienne de Bremnes au début des années 1950[15]. Ce dernier, identifie un *réseau social* formé par les habitants de l'île et se définissant par deux éléments : les contacts et la liaison entre les contacts. L'utilité des individus se mesure par leur capacité à transmettre des informations et croît en conséquence avec le nombre de contacts qu'ils possèdent au sein du réseau. Le sociologue observe par ailleurs que l'ensemble des individus constituant la population de l'île est relié par une chaîne qui ne compte pas plus de quatre relations d'interconnaissance. John A. Barnes conclut son étude en remarquant que ce réseau social s'étend en réalité bien au-delà de la limite géographique de l'île et que les relations d'interconnaissance se prolongent au continent, voire à la planète entière. Cette hypothèse formulée par John A. Barnes sur la non-finitude du concept de réseau social fut ensuite vérifiée empiriquement par l'expérience du « *petit monde* » réalisée par le psychologue américain Stanley Milgram en 1967[16]. Cette expérience amène à la conclusion que dans une société de masse, les individus sont reliés aux autres dans un vaste réseau dont la distance moyenne entre chaque individu est d'environ cinq intermédiaires[17]. Plus récemment, en 2011, une étude fut menée sur les 69 milliards de liens entre les 721 millions d'individus utilisant le site Facebook. Cette analyse démontre que la quasi-totalité des utilisateurs de ce site de réseau social ne constitue qu'un seul et unique vaste réseau de

[15] L'étude menée par John A. Barnes distingue au sein de la population de l'île de Bremnes trois sphères sociales : la première correspond à l'organisation politique et comprend les unités administratives et les associations présentent sur l'île ; la deuxième représente le système industriel, principalement constitué du secteur de la pêche ; enfin la troisième comprend l'ensemble des relations informelles entre les individus de l'île. John A. Barnes utilise en l'occurrence la notion de *réseau social* pour désigner cette troisième sphère sociale qui se superpose aux deux premières. V. J. A. BARNES, « Class and Committees in a Norwegian Island Parish », Human Relations, 1954.

[16] Cette expérience consistait à choisir un individu-cible, en l'occurrence un agent de change de Boston, et trois groupes d'environ cent personnes chacun d'eux constitués aléatoirement. Un premier groupe était composé des habitants de Boston choisis au hasard, le deuxième d'habitants du Nebraska choisis également au hasard, et le troisième d'habitants du Nebraska mais présentant la particularité de posséder des actions. Chacun des individus au sein de ces groupes recevait ensuite un dossier décrivant l'individu-cible, notamment son lieu de résidence et sa profession, et avait pour but de faire parvenir ce dossier par voie postale soit directement à l'individu cible, s'il le connaissait personnellement, soit à une de ses connaissances qui aurait plus de chances de le connaître personnellement. Au final, sur les 296 individus composant les trois groupes de départ, 217 ont accepté de participer à l'expérience et ont expédié le dossier à une de leurs connaissances. 64 dossiers sont parvenus jusqu'à l'individu-cible, au terme de chaîne de connaissances dont la longueur moyenne était de 5,2 intermédiaires. V. J. TRAVERS et S. MILGRAM, « Une étude expérimentale du petit monde », *in* H. MENDRAS et M. OBERTI (dir.), *Le sociologue et son terrain. Trente recherches exemplaires*, Paris, Armand Colin, 2000, trad. fr. par M. FORSE de « An experimental study of the small world problem » (1969), Sociometry, 32, 425-443, pp. 230-241.

[17] P. MERCKLE, *La sociologie des réseaux sociaux*, *op. cit.*, p. 13.

relations, la plus grosse composante connexe rassemblant 99,9 % des individus. Au sein de ce réseau, la distance moyenne entre chaque individu n'est plus que de 3,7 intermédiaires[18]. Plus généralement, le concept de réseau social en sociologie s'inscrit dans la théorie relationnelle développée par le philosophe et sociologue allemand Georg Simmel[19]. Selon ce dernier, l'objet fondamental de la sociologie s'observe à un niveau intermédiaire, c'est-à-dire, ni au niveau microsociologique de l'individu et ni au niveau macrosociologique de la société prise dans son ensemble. Georg Simmel situe son analyse à un niveau « *mésosociologique* » se plaçant à l'échelle des relations entre individus[20]. L'étude des réseaux sociaux relève alors d'une approche particulière en sociologie, n'appartenant à aucun des deux grands mouvements de pensée en la matière : l'individualisme méthodologique[21] et le holisme[22]. L'approche simmelienne développée au début du XX^{ème} siècle, reprise ensuite par John A. Barnes en 1954, appartiendrait en réalité à un individualisme méthodologique complexe, voire à un « *dualisme méthodologique* »[23].

7. Développement des réseaux sociaux à l'échelle numérique. Si le concept de réseau social n'est pas récent, la possibilité de créer son réseau, de le visualiser et d'interagir avec lui sur internet est une nouvelle pratique apparue au milieu des années 2000. Les interactions entre personnes, qui sont une caractéristique forte des réseaux sociaux, supposent sur internet la présence de deux éléments : il faut être en mesure de créer une information et par ailleurs, disposer d'une technologie suffisante permettant la communication de cette information[24]. Or,

---

[18] *Ibid.*, pp. 13-14.

[19] Georg Simmel considère que, au sein des grands centres urbains qui réunissent un nombre important d'individus, la société est faite d'interactions entre des dynamiques individuelles. Le cadre de vie moderne urbain se façonne alors autour de la qualité et de l'intensité de ces relations. G. SIMMEL, *Sociologie, études sur les formes de la socialisation*, Paris, PUF, 1999 (1908) ; Dans le même sens : J. DAMON, « La pensée de... Georg Simmel (1858-1918) », *Informations sociales*, vol. 123, n^{o} 3, 2005, p. 111 ; P. DONATI, « La relation comme objet spécifique de la sociologie », *Revue du MAUSS*, vol. n^{o} 24, n^{o} 2, 2004, p. 233.

[20] P. MERCKLE, *La sociologie des réseaux sociaux*, *op. cit.*, p. 14.

[21] L'individualisme méthodologique est un paradigme qui décrit les phénomènes collectifs à partir des propriétés et des actions individuelles et de leurs interactions mutuelles. Plus précisément, l'individualisme méthodologique est une méthode qui vise à expliquer les phénomènes sociaux en deux étapes organiquement liées : « *1/ une étape d'explication qui consiste à montrer que ces phénomènes sociaux sont la résultante d'une combinaison ou d'une agrégation d'actions individuelles ; 2/ une étape de compréhension qui consiste à saisir le sens de ces actions individuelles, et plus précisément à retrouver les bonnes raisons pour lesquelles les acteurs ont décidé de les effectuer* ». R. BOUDON, R. FILLIEULE. « Chapitre II. L'individualisme méthodologique », *in* R. BOUDON, *Les méthodes en sociologie*, PUF, 2018, p. 41.

[22] L'approche holiste étudie les pratiques sociales des individus de manière collective au sein de la société. Les faits sociaux sont alors expliqués du point de vue du groupe ou de la société et non du point de vue individuel. En conséquence, les phénomènes sociaux sont considérés comme des touts entre lesquels on cherche à faire apparaître des relations de cause à effet. R. BOUDON, R. FILLIEULE, « Introduction », *in* R. BOUDON, *Les méthodes en sociologie*, *op. cit.*, p. 3.

[23] P. MERCKLE, La sociologie des réseaux sociaux, *op. cit.*, p. 16.

[24] R. RISSOAN, *Les réseaux sociaux: Facebook, Twitter, Linkedln, Viadeo, Google +, comprendre et maîtriser ces nouveaux outils de communication*, Objectif web, Éditions ENI, 2ème éd., 2011, p. 29.

en 2004, l'apparition du web 2.0[25] fournit cette technologie nécessaire. Cette expression inventée par Monsieur Darcy Di Nucci dès 1999[26], popularisée le 30 septembre 2005 lors d'une conférence par Monsieur Tim O'Reilly[27], se réfère à une nouvelle génération de développement d'internet qui exprime le passage d'une communication verticale représentative des médias classiques à une communication horizontale appelée également « *many to many* »[28]. Le web 2.0 a pour caractéristique principale de permettre l'implication des usagers dans la création de contenus lui valant en conséquence également les appellations de web contributif[29], web participatif ou encore web interactif[30]. Il favorise le partage de contenus et leur réutilisation au gré des initiatives des internautes caractérisant le passage de l'ère des *« médias des masses* » à celle des médias *de* masse[31]. Le web 2.0 a ainsi permis l'émergence d'un web social se regroupant autour de multiples acteurs comme les sites d'édition collective à l'image de l'encyclopédie Wikipédia, les sites de partage de contenus tels que YouTube ou Dailymotion, mais aussi les sites de réseaux sociaux qui constituent un acteur particulier au sein d'internet qu'il convient de définir.

B. La notion de réseaux sociaux en ligne

8. Définitions des réseaux sociaux en ligne. Les « *réseaux sociaux en ligne* »[32] encore appelés « *sites de réseautage social* »[33] ou plus simplement sites de réseaux sociaux, peuvent se définir dans un premier temps comme des lieux de rencontres et d'échanges d'informations de toute nature entre les personnes inscrites à un même groupe ou prétendant appartenir à une même communauté[34]. Les sites de réseaux sociaux ont ainsi pour principale caractéristique

[25] En informatique, les chiffres décimaux de type 2.0 sont utilisés pour caractériser des versions successives d'un logiciel. L'expression web 2.0 symbolise donc le franchissement d'une nouvelle étape dans le développement d'internet. F. REBILLARD, *Le web 2.0 en perspective. Une analyse socio-économique de l'internet*. L'Harmattan, 2007, p. 15, nbp n° 3.
[26] D. Di NUCCI, « Fragmented futur », *Print Magazine*, avril 1999, p. 32.
<http://darcyd.com/fragmented_future.pdf> (dernière consultation le 9 octobre 2019).
[27] T. O'REILLY, « What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software », Conférence sur le Web 2.0, organisée le 30 septembre 2005 par Tim O'Reilly Media. <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html> (dernière consultation le 9 octobre 2019).
[28] L. QUONIAM, « Introduction. Du web 2.0 au concept 2.0 », *Les Cahiers du numérique*, vol. 6, n° 1, 2010, p. 9.
[29] *Ibid.*
[30] R. RISSOAN, *Les réseaux sociaux: Facebook, Twitter, Linkedln, Viadeo, Google +, comprendre et maîtriser ces nouveaux outils de communication*, *op. cit.*, p. 31.
[31] J. De ROSNAY, *La Révolte du pronétariat. Des mass médias aux médias des masses*, Fayard, coll. Transversales, Paris, 2006.
[32] E. DERIEUX, A. GRANCHET, *Les réseaux sociaux en ligne. Aspects juridiques et déontologiques*, Lamy, coll. Axe Droit, Paris, 2013.
[33] P. TRUDEL, F. ARBAN, *Gérer les enjeux et risques juridiques du web 2.0*, Centre de recherche en droit public, Université de Montréal, CEFRIO, janvier 2012, p. 30.
[34] E. DERIEUX , A. GRANCHET, *Réseaux sociaux en ligne, aspects juridiques et déontologiques*, Lamy,

d'offrir des services en ligne qui permettent la rencontre et la mise en relation de différentes personnes[35]. Aux États-Unis, Mesdames Danah Boyd[36] et Nicole Ellison[37] sont venues reconnaître en 2007 trois caractéristiques principales aux réseaux sociaux numériques venant poser les bases d'une définition communément admise en sciences de l'information[38]. Selon celles-ci, « *un site de réseau social est une plate-forme de communication en réseau dans laquelle les participants 1) disposent de profils associés à une identification unique qui sont créés par une combinaison de contenus fournis par l'utilisateur, de contenus fournis par des "amis", et de données système ; 2) peuvent exposer publiquement des relations susceptibles d'être visualisées et consultées par d'autres ; 3) peuvent accéder à des flux de contenus incluant des contenus générés par l'utilisateur - notamment des combinaisons de textes, photos, vidéos, mises à jour de lieux et/ou liens - fournis par leurs contacts sur le site* »[39]. En Europe, le groupe de l'article 29[40] propose également une définition dans son avis n°5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009 selon lequel : « *les réseaux sociaux sont des plates-formes en ligne qui permettent à tout internaute de rejoindre ou de créer des réseaux d'utilisateurs ayant des opinions similaires et/ou intérêts communs* ». Le groupement de concertation ajoute qu'ils constituent « *des outils permettant aux utilisateurs de mettre leur propre contenu en ligne (contenu généré par l'utilisateur) tel que des photos, des chroniques ou des commentaires, de la musique, des vidéos ou encore des liens vers d'autres sites* ». En France, certains auteurs ont défini leur conception de la notion de site de réseau social. Certains les décrivent comme étant une « *plate-forme de communication en ligne qui permet à*

---

coll. Axe Droit, 2013, §6.

[35] P. TRUDEL, F. ARBAN, *Gérer les enjeux et risques juridiques du web 2.0*, *op. cit*.

[36] Danah Boyd est une anthropologue américaine reconnue pour son travail sur les réseaux sociaux : v. D. BOYD, *La sociabilité des adolescents américains dans les espaces publics en réseau,* Thèse, Université de Berkeley, Californie, 2008 ; D. BOYD, « Social Network Sites: Public, Private, or What ? », *The Knowledge Tree*, n° 13, mai 2007.

[37] Nicole Ellison est professeur au *département Telecommunication, Information Studies, and Media* de la *Michigan State University*. Ses travaux portent sur les questions de représentation de soi, de développement des relations et d'identités en ligne. Plus récemment, elle s'est intéressée aux problématiques de capital social dans l'usage de *Facebook*, à la présentation de soi trompeuse sur les sites de rencontre, et à l'usage de réseaux socionumériques dans des cadres éducatifs.
<https://en.wikipedia.org/wiki/Nicole_Ellison> (dernière consultation le 9 octobre 2019).

[38] Selon les propos de Annick Thierry, s'adressant à Nicole Ellison : « *la définition des réseaux socionumériques que vous avez proposée avec Danah Boyd dans Journal of Computer-Mediated Communication (2007) est probablement celle qui est reprise le plus souvent par les universitaires* ». V. « Réseaux sociaux, numérique et capital social. Entretien réalisé par Thomas Stenger et Alexandre Coutant », *Hermès, La Revue*, vol. 59, n° 1, 2011, p. 21.

[39] D. BOYD, N. ELLISON, « Social Network Sites: Definition, History, and Scholarship » *Journal of Computer Mediated Communication*, vol. 13, Issue 1, Octobre 2007, p. 210 ; V. également pour une traduction en français, l'entretient avec Nicole Ellison réalisé par Thomas Stenger et Alexandre Coutant : « Réseaux sociaux, numérique et capital social », Hermès, vol. 59, 2011, p. 22.

[40] Groupement de concertation réunissant, en Europe, les représentants des divers organismes nationaux de régulation comme par exemple la Commission nationale de l'informatique et des libertés en France.

un internaute de rejoindre ou de créer des réseaux d'utilisateurs ayant des intérêts communs, un site Internet qui permet d'accéder à une plateforme d'échange et de dialogue »[41]. Pour d'autres, « *les réseaux sociaux peuvent être définis comme des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs. Ces derniers fonctionnant grâce à l'utilisation d'outils mettant à disposition une liste de contacts pour chaque utilisateur avec une possibilité d'interaction entre eux* »[42]. Enfin, on retrouve également la définition selon laquelle un réseau social est « *une plate-forme de communication en ligne qui permet à un internaute de rejoindre ou de créer un ou plusieurs réseaux d'utilisateurs partageant des intérêts communs. De manière plus concrète, un réseau social se présente comme un site Internet qui permet, après une inscription (…) d'accéder à une plate-forme d'échange d'informations avec d'autres internautes sur des sujets divers* »[43]. De ces diverses définitions proposées, il ressort trois caractéristiques constantes aux réseaux sociaux. Tout d'abord concernant l'interface, les réseaux sociaux en ligne constituent une « *plate-forme de communication en ligne* » ; ensuite, les utilisateurs des réseaux sociaux se réunissent autour d'« *intérêts communs* » ; enfin, chaque auteur reconnaît une forme d'interaction entre les utilisateurs de ces réseaux sociaux (« *échanges de dialogues* », « *échanges d'informations* » ou encore « *utilisation d'outils permettant une interaction entre les contacts* »). Les réseaux sociaux en ligne sont donc un moyen de conforter, de retrouver, de créer des relations avec des personnes et de pouvoir interagir avec eux à l'aide d'une interface virtuelle. Il convient dès lors de distinguer les réseaux sociaux en ligne avec d'autres acteurs similaires avec lesquels ils peuvent être confondus.

9. Réseaux sociaux en ligne et médias sociaux. Les réseaux sociaux en ligne doivent tout d'abord être différenciés des médias sociaux. Ces derniers désignent une grande variété de sites reposant sur une logique d'interaction avec les internautes issue des possibilités techniques offertes par l'apparition du web 2.0. Ils regroupent alors un champ plus vaste que les sites de réseaux sociaux qui n'en constituent qu'un élément. Ainsi, outre les réseaux sociaux en ligne, les médias sociaux sont également formés des plateformes de partages de contenus mais aussi des plateformes contributives telles que l'encyclopédie en ligne Wikipédia ou la base de donnée collaborative Discogs, mais également de l'ensemble des

[41] L. COSTES, « Réseaux sociaux: nouveaux enjeux et nouveaux défis pour les entreprises », *RLDI* 2011, n° 74, n° 2472.
[42] E. BAILLY, E. DAOUD, « Cybercriminalité et réseaux sociaux: la réponse pénale », *AJ Pénal* 2012, p. 252.
[43] N. DREYFUS, *Marques et internet. Protection, valorisation, défense,* Lamy, Coll. Axe Droit, 2011, p. 325.

blogs, forums ou autres sites sur lesquels les internautes peuvent contribuer par l'insertion de contenus (commentaires, liens hypertextes). Les sites de réseaux sociaux forment alors un ensemble particulier au sein des médias sociaux par le nombre et la diversité des interactions qu'ils proposent. Plus précisément, les réseaux sociaux se distinguent en raison de l'intensité des relations qu'ils génèrent par rapport aux simples blogs ou forums qui demeurent davantage animés par une logique contributive.

10. Réseaux sociaux en ligne et plateforme de partage de contenus. Ensuite, les réseaux sociaux en ligne se distinguent des plateformes de partage de contenus. Sur ces sites, les utilisateurs peuvent mettre en ligne des fichiers de toute nature comme des vidéos, des images, des musiques, des livres etc. Les contenus y sont ensuite diffusés en *streaming*[44]. Si les sites de réseaux sociaux peuvent être décrits comme des plateformes relationnelles liées à des activités de réseautage (par exemple les sites Facebook, Twitter ou LinkedIn), les plateformes de partage de contenus centrent davantage leur fonctionnement sur le stockage et le partage de contenus recyclés ou autoproduits (par exemple Youtube, Instagram, Dailymotion, Bandcamp, Soundcloud, etc.)[45]. La distinction entre ces deux types de site n'est toutefois pas toujours évidente. En effet, d'un côté les sites de réseaux sociaux proposent également des fonctionnalités permettant d'héberger et de partager des contenus et d'un autre côté, certains sites de partage de contenus fonctionnent sur la base de la création d'un profil d'utilisateur et ont développé la possibilité pour les internautes d'interagir avec les contenus mis en ligne notamment par le biais de commentaires. La distinction s'opère alors dans l'activité dominante qui caractérise le site, à savoir soit les interactions entre utilisateurs, soit le partage de contenus.

11. Réseaux sociaux en ligne et plateformes marchandes. Les réseaux sociaux en ligne s'opposent également aux plateformes numériques marchandes qui proposent une interface de services monétisés[46]. Ces plateformes, à l'image des sites internet Leboncoin ou encore Ebay proposent une mise en relation entre leurs utilisateurs sous forme d'échanges de biens ou de

---

[44] « *La lecture en transit (streaming) est une méthode de diffusion de fichiers audio ou vidéo qui permet leur lecture en temps réel, c'est-à-dire dès le début de la réception du fichier, sans avoir à attendre qu'il soit copié au complet sur l'ordinateur récepteur. Le transfert de données se fait sous forme de flux régulier et continu. La lecture en transit permet donc de diffuser des contenus multimédias sur Internet, à la demande ou en temps réel, et ce, sans solliciter l'espace du disque dur de l'utilisateur* ». P. TRUDEL, F. ARBAN, *Gérer les enjeux et risques juridiques du web 2.0*, *op. cit.*, p. 45.

[45] M. LAURENT et S. BOUZEFRANCE (dir.), *La gestion des identités numériques*, éd. Iste, 2015, p. 48.

[46] Pour une étude de l'impact des plateformes marchandes sur le droit, en particulier le droit du travail : v. B. GOMES, *Le droit du travail à l'épreuve des plateformes numériques*, Thèse, Université Paris-Nanterre, présentée le 3 décembre 2018.

services. Elles concernent des secteurs de l'économie classique[47], mais aussi de nouveaux secteurs d'activités relevant parfois de la vie sociale[48]. Les plateformes marchandes proposent donc un service payant à la différence des sites de réseaux sociaux qui dans leur majorité proposent une inscription et un usage gratuit[49].

12. Cartographie des réseaux sociaux en ligne. Les sites de réseaux sociaux se distinguent donc d'autres acteurs similaires du secteur numérique du fait qu'ils axent leur fonctionnement sur les relations interpersonnelles en proposant de nombreuses et diverses interactions possibles entre leurs membres indépendamment de tout rapport financier entre ces derniers. Si ces critères éliminent de nombreuses plateformes numériques utilisant les fonctionnalités du web 2.0, il n'en demeure pas moins qu'une multitude de sites peut être qualifiée de réseaux sociaux formant ainsi « *un large spectre de plateformes en ligne* »[50]. Bien que chaque site de réseau social se démarque des autres par certaines caractéristiques qui lui sont propres, il est possible de distinguer diverses catégories au sein de ces derniers sans pour autant prétendre établir une liste exhaustive.

13. Il convient d'abord de distinguer la catégorie des « *réseaux sociaux majeurs* »[51] formés par les deux principaux réseaux sociaux en ligne que sont les sites Facebook et Twitter. Cette catégorie se justifie par le caractère universel de ces plateformes disposant d'un nombre important d'utilisateurs dans la majorité des régions de la planète. Le site Facebook constitue la plateforme la plus utilisée au monde avec 2,4 milliards d'utilisateurs actifs par mois. Dans une moindre mesure, le site Twitter recense 335 millions d'utilisateurs actifs par mois[52]. Ces deux acteurs majeurs d'internet revêtent toutefois deux modes de fonctionnement très distincts. Le plus populaire, Facebook, était à l'origine le réseau social fermé des étudiants de l'université d'Harvard avant de devenir accessible aux autres universités américaines puis enfin à l'ensemble des internautes à partir de septembre 2006. De manière générale, cette plateforme permet à ses utilisateurs de renseigner des informations

[47] Par exemple louer les services d'un chauffeur *via* l'application Uber ou encore louer un logement avec la plateforme Airbnb.
[48] Par exemple, le site Blablacar proposant des services de covoiturage, ou encore le site Book a friend proposant la location de relations sociales.
[49] En réalité, sur les sites de réseaux sociaux se sont alors les utilisateurs qui deviennent le principal produit manifestant ainsi le passage d'une économie basée sur la création de valeurs à une économie fonctionnant sur le modèle de la captation de valeurs.
[50] V. NDIOR, « Le réseau social : essai d'identification et de qualification », *in Droit et réseaux sociaux*, (dir. V. NDIOR), éd. Lextenso, coll. LEJEP, octobre 2015, p. 17.
[51] Pour reprendre l'expression employée par Valère Ndior *in* : « Le réseau social : essai d'identification et de qualification », *in* V. NDIOR (dir.), *Droit et réseaux sociaux*, éd. Lextenso, coll. LEJEP, octobre 2015, p. 17.
[52] Blog du modérateur, « Les chiffres Facebook – 2019 », chiffres publiés le 4 juillet 2019 et mis à jour le 14 août 2019.

personnelles et d'interagir avec d'autres utilisateurs faisant partie de leurs « *amis* ». Tout utilisateur du site Facebook dispose d'un compte faisant apparaître un « *mur* » qui affiche les contenus publiés par le titulaire du compte ou par ses contacts. Le site Twitter a quant à lui basé sa réussite en créant un outil de microblogging aux fonctionnalités minimalistes[53]. Ce réseau social permet à ses utilisateurs de mettre en ligne de brefs messages (de 280 caractères maximum) appelés « *tweet* » sur leur fil d'actualité. Le site repose sur une logique d'abonnement où chaque utilisateur sélectionne d'autres personnes également inscrites devenant leur « *follower* ». Ces deux plateformes constituent les deux sites internet contemporains les plus représentatifs des réseaux sociaux en ligne et polarisent en outre la majorité des contentieux suscités par ces nouveaux moyens de communication, c'est pourquoi, ces derniers seront à de nombreuses reprises cités et utilisés en exemple dans la présente étude.

14. Ensuite, par opposition à ces acteurs majeurs, certains réseaux sociaux en ligne alternatifs peuvent être identifiés. En effet, une multitude d'autres sites de réseaux sociaux dont la popularité est bien moins importante que les deux géants précités visent pourtant les mêmes objectifs à savoir, créer des communautés en ligne en développant les interactions entre internautes. Certaines de ces plateformes proposent une voie alternative aux internautes par un traitement plus éthique et un niveau de protection important de leurs données personnelles. Par exemple, le réseau social Diaspora[54] offre des fonctionnalités similaires au site Facebook tout en proposant un système décentralisé et sécurisé, permettant de préserver la vie privée de ses utilisateurs. À l'inverse des sites de réseaux sociaux traditionnels, le fonctionnement de Diaspora est basé sur la décentralisation empêchant que l'ensemble des données de leurs utilisateurs soient concentrées dans d'énormes serveurs détenus par l'entreprise organisant le réseau social en ligne. L'utilisateur de Diaspora devient ainsi le seul et unique titulaire de ses données personnelles. Par ailleurs, d'autres réseaux sociaux en ligne constituent des alternatives aux sites de réseaux sociaux traditionnels en raison de leur utilisation cantonnée à un secteur géographique précis. À titre d'exemple, le réseau social japonais Mixi[55] conditionne l'inscription à ses services à la possession par l'utilisateur d'un numéro de téléphone portable local. Cependant, certains de ces réseaux sociaux régionaux ont en réalité pour but de faciliter la maîtrise des flux de contenus et la surveillance de la

[53] R. RISSOAN, *Les réseaux sociaux: Facebook, Twitter, Linkedln, Viadeo, Google +, comprendre et maîtriser ces nouveaux outils de communication*, Objectif web, Éditions ENI, 2ème éd., 2011, p. 154.
[54] <https://diasporafoundation.org>
[55] <https://mixi.jp>

population par certains régimes[56], c'est le cas notamment des sites Weibo[57] et RenRen[58] en Chine mais également VKontakte[59] en Russie.

15. Enfin, contrairement aux sites de réseaux sociaux généralistes, certaines plateformes relationnelles s'axent sur des thématiques précises. Les plus populaires sont les sites de réseaux sociaux professionnels et notamment le réseau social américain LinkedIn[60] possédant en janvier 2019 plus de 303 millions d'utilisateurs actifs par mois. Dans cette même catégorie, peuvent également être cités les réseaux sociaux français Viadeo[61] et allemand XING[62]. Ces sites proposent à leurs utilisateurs de créer un profil professionnel détaillé leur permettant, par le biais des interactions avec les autres utilisateurs, de se constituer un carnet d'adresse ou de rechercher une nouvelle profession. Par ailleurs, il existe des sites de réseaux sociaux professionnels spécifiques à certains métiers. Le corps médical dispose ainsi de plusieurs réseaux sociaux spécifiques visant notamment les médecins comme le réseau social MeltingDoc qui annonce sur sa page d'accueil : « *partagez vos cas cliniques les uns les autres* »[63], ou encore le site Décidoc qui propose pour sa part de « *partager tout le savoir médical* »[64]. Outre les sites de réseaux sociaux professionnels, certaines plateformes ont pour objectif de favoriser les rencontres entre individus possédant des affinités matrimoniales ou sexuelles. Il s'agit par exemple des sites Meetic[65], Tinder[66] ou encore Mektoube[67] concernant la communauté musulmane. D'autres sites basent encore la mise en relation des individus sur leurs affinités culturelles[68] ou artistiques[69]. Au final, si la catégorie des réseaux sociaux en ligne peut être clairement identifiée sur le réseau internet, elle n'en constitue pas moins un ensemble hétéroclite de sites recentrés chacun d'entre eux sur la mise en relation et les interactions entre personnes.

16. **Identification de l'objet de l'analyse.** Partant, la présente étude ne se réfère pas à la conception sociologique du réseau social identifié par John A. Barnes mais davantage à la

[56] V. sur le sujet : V. LINDER, « Restriction à l'utilisation des réseaux sociaux dans les systèmes juridiques étrangers », *in Droit et réseaux sociaux* (dir. V. NDIOR), éd. Lextenso, coll. LEJEP, octobre 2015, p. 63.
[57] <https://www.weibo.com>
[58] <http://www.renren.com>
[59] <https://vk.com>
[60] <https://fr.linkedin.com>
[61] <http://fr.viadeo.com>
[62] <https://www.xing.com>
[63] <https://www.meltingdoc.com>
[64] <http://www.decidoc.com>
[65] <https://www.meetic.fr>
[66] <https://tinder.com>
[67] <https://www.mektoube.fr>
[68] Il s'agit par exemple des sites Chalombook pour la communauté juive et Oummalink pour la communauté musulmane.
[69] Peuvent être cités les sites : Myspace, Ello, DeviantArt.

catégorie identifiée au sein de l'espace numérique des sites de réseaux sociaux. Ces derniers, bien que recensant une multitude d'acteurs différents, se distinguent d'autres acteurs similaires tels que les blogs, les plateformes collaboratives, les plateformes de partage de contenus ou encore les plateformes marchandes. L'exclusion de ces acteurs du champ d'analyse n'est toutefois pas d'une absolue fermeté. Leurs nombreuses similarités avec les sites de réseaux sociaux du point de vue technologique peuvent justifier des comparaisons ou exemples ponctuels au cours de l'étude. Par ailleurs, si le présent développement a pour objet central les sites de réseaux sociaux, l'étude de ces derniers se fera à travers leurs acteurs (utilisateurs et opérateurs) mais également au regard de leur composants structurels (tels que les comptes d'utilisateurs et les diverses fonctionnalités techniques permises par ces sites à l'image du partage des contenus).

§2. Impact sociétal des réseaux sociaux en ligne

17. L'utilisation des réseaux sociaux en ligne est devenue la norme dans nos rapports sociaux mais aussi économiques. Ainsi, faire le choix de ne plus utiliser le réseau social Facebook deviendrait presque un acte militant[70]. Les changements opérés entre le monde d'avant les sites de réseaux sociaux et le monde depuis leur apparition amène à constater leur forte capacité d'influence sur nos sociétés contemporaines. Ce fort pouvoir d'impact des réseaux sociaux en ligne se mesure en réalité tant à l'échelle de la société (B) qu'à l'échelle de l'individu (A).

A. L'impact des réseaux en ligne à l'échelle de l'individu

18. L'évolution des formes de sociabilité. Si les sites de réseaux sociaux confèrent aux liens sociaux une particulière mise en lumière, ces communautés virtuelles manifestent avant tout un nouveau genre d'organisation sociale. Au sein de cette dernière, « *les critères classiques de la relation sont bouleversés amenant à une sociabilité désincarnée où tout se vit à distance, virtuellement, dans l'anonymat, en amont d'un éventuel face-à-face. Bardés d'écrans et de pseudos, libérés de la matérialité du corps, chacun est délesté de marqueurs sociaux et psychologiques encombrants et affranchi des contraintes de l'identité.* […] *cette condition est le terreau d'un zapping et d'un consumérisme relationnels* »[71]. Dès lors, sur ces

[70] O. ITEANU, *Quand le digital défie l'État de droit*, Eyrolles, 2016, p. 20.
[71] I. COMPIEGNE, *La société numérique en question(s)*, Sciences Humaines Éd., 2010, p. 35.

plateformes relationnelles, c'est l'intention personnelle qui initie la mise en relation. Les réseaux sociaux obéissent à une logique d'espaces personnalisés où chacun peut s'exprimer tout en recherchant une reconnaissance. Les sites de réseaux sociaux n'entraînent cependant pas un appauvrissement du lien social mais davantage une complexification de ce dernier[72]. Ainsi, « *loin d'être en rupture, les espaces et les pratiques de sociabilité associés à l'essor des médias numériques présentent des similitudes et une continuité avec les systèmes relationnels ordinaires* »[73]. Cependant, les sites de réseaux sociaux favorisent une intensification des actes de communication qui a pour conséquence d'enrichir les pratiques relationnelles, la sociabilité se déployant alors selon une dynamique d'entrelacement[74].

19. La diversification des formes d'identité. Les réseaux sociaux ont mis en exergue une caractéristique récente de l'identité numérique : celle-ci peut d'un côté être produite par l'internaute à travers la mise en ligne d'informations au sein de son profil (nom, âge, sexe, profession, domiciliation, auto description, etc.) et d'éléments davantage expressifs sur son « *mur* » (statuts, textes, commentaires, partages, photos, vidéos, liens, etc.) ; mais elle peut également résulter de l'action d'autres utilisateurs contribuant à l'émergence d'une « *identité numérique sociale* »[75]. L'identité se construit dans un premier temps sur les réseaux sociaux à travers une mise en scène de l'individu[76]. Pour ce faire, les réseaux sociaux mettent à disposition des utilisateurs des formulaires qui visent à renseigner le site sur des éléments touchant à la fois des domaines de la vie publique de l'individu comme des domaines de sa vie privée. Ces sites proposent également à leurs utilisateurs d'adhérer à des groupes ou des communautés internes dans le but d'enrichir leur profil. La typicité des sites de réseaux sociaux oriente les informations demandées dans certains domaines particuliers. Ainsi, les sites de réseaux sociaux professionnels comme LinkedIn ou Viadeo demandent à leurs membres une description de leur parcours universitaire, formations, compétences, expériences et emplois exercés de sorte à créer un *curriculum vitae* en ligne ouvert aux autres membres du réseau. Cependant, ces éléments narratifs ne sont pas communs à tous les sites de réseaux sociaux, certains d'entre eux basant davantage leur activité sur les échanges entre les

[72] *Ibid.*, p. 38.
[73] *Ibid.*, p. 39.
[74] D. CARDON, Z. SMOREDA, V. BEAUDOIN, « Sociabilités et entrelacement des medias », *in* P. MOATI (dir.), *Nouvelles technologies et modes de vie. Aliénation ou hypermodernité ?*, Éditions de l'Aube, 2005.
[75] F. GEORGES, « L'identité numérique sous emprise culturelle. De l'expression de soi à sa standardisation », *Les Cahiers du numérique*, vol. 7, nº 1, 2011, p. 31.
[76] Selon Erving Goffman, l'individu est un acteur qui se met en scène constamment. V. *La mise en scène de la vie quotidienne. La présentation de soi*, tome 1, coll. *Le sens commun*, Les éditions de minuit, 1959.

utilisateurs que sur la construction d'un profil détaillé[77]. Le réseau social Facebook semble proposer une fiche descriptive de l'individu la plus complète car regroupant tous les aspects de leur vie. Le recoupement de l'ensemble de ces informations disponibles forme un passeport social extrêmement détaillé de l'individu. La représentation fidèle de l'identité réelle varie cependant en fonction des plateformes utilisées. Par exemple, les sites de rencontre qui ont vocation à aboutir à une relation dans la vie réelle sont plus à même de représenter l'identité réelle de l'individu pour ne pas aboutir à un décalage identitaire entre le réel et le numérique. À l'inverse, d'autres interfaces favorisent le « *mieux que moi* », le « *plus que soi* », ou même l' « *autrement que soi* »[78]. Cependant, les informations ajoutées lors de l'inscription sur le réseau social ne forment qu'une minorité des éléments formant l'identité numérique des individus. Cette dernière continue de s'étoffer au gré de l'activité de l'individu sur le réseau social. Il est ainsi indispensable de prendre en compte l'identité numérique agissante de l'individu. Dans un second temps, l'identité numérique se déploie indépendamment de soi, au travers de contenus publiés par d'autres utilisateurs[79]. Les sites de réseaux sociaux ont de ce fait contribué à développer une identité numérique sociale plus explicite que les éléments de l'identité numérique classique, mais surtout, elle devient fonction d'acteurs multiples : l'utilisateur lui-même mais également d'autres utilisateurs peuvent agir sur son identité numérique. Au final, l'identité numérique des individus est en constante évolution et surtout, à l'heure des réseaux sociaux en ligne, elle est fonction de l'action des autres utilisateurs. Autre distinction avec l'identité réelle, l'identité numérique est souvent multiple, il est alors plus à propos d'évoquer *les identités numériques de l'individu* plutôt que *l'identité numérique de l'individu*.

20. L' « *extimité* » sur les réseaux sociaux en ligne. Avec la construction d'une identité numérique sociale, les sites de réseaux sociaux favorisent indubitablement la divulgation d'éléments relevant du cercle privé. Ainsi, les sites de réseaux sociaux sont le moteur principal du phénomène de mise en visibilité de soi. Toute la philosophie de ces sites repose sur la construction d'un soi virtuel et de son exposition. Si les réseaux sociaux ne sont pas les

[77] Par exemple Snapchat permet à ses utilisateurs de s'envoyer des contenus multimédias (photos et vidéos) accompagnés éventuellement de textes. Le profil des utilisateurs de l'application n'est donc pas déterminent dans l'activité du site.
[78] C. BLANC, « Identité numérique et réseaux sociaux », *in Qui suis-je, dis-moi qui tu es. L'identification des différents aspects juridiques de l'identité*, Études réunies par V. MUTELET et F. VASSEUR-LAMBRY, *Droit et Sciences économiques*, Artois Presses-Université, 2015, p. 126.
[79] M. LAURENT et S. BOUZEFRANCE (dir.), *La gestion des identités numériques*, éd. Iste, 2015, p. 49.

seuls acteurs de cette mise en visibilité[80], ces derniers ont contribué à élargir sensiblement son champ médiatique, tout individu pouvant désormais s'adonner à cette activité. Les réseaux sociaux favorisent un étalage de l'intime, des convictions et plus généralement de toute sorte d'informations qui contribuent à étayer encore plus l'identité numérique de chaque individu. Cette activité prospère s'explique notamment par l'excès de confiance que les utilisateurs livrent dans le réseau social mais aussi par la dynamique que crée l'interaction avec autrui[81]. C'est, selon André Gunthert, « *notre propre activité sociale qui entretient notre intérêt pour le site* »[82]. Sur les sites de réseaux sociaux, c'est l'utilisateur lui-même qui créée l'information et qui de ce fait devient le moteur du site. Il est incité à dévoiler des éléments de son quotidien qui certes, indépendamment les uns des autres, ne constituent qu'un « *grain d'information* »[83] mais qui pris dans leur ensemble sont de nature à révéler des grilles d'informations détaillées des individus[84]. De nombreuses recherches soulignent que l'usage des réseaux sociaux a pleinement contribué au mouvement « *expressiviste d'Internet* »[85]. Les sites de réseaux sociaux contribuent donc à élargir sensiblement le champ médiatique de l'intimité de leurs utilisateurs qui deviennent en quelque sorte des acteurs consentants de sa divulgation. Monsieur Serge Tisseron explique ces nouvelles pratiques au moyen de la notion d' « *extimité* » : « *nous sommes de plus en plus nombreux à exposer une partie de notre intimité, au moyen de la photographie, de la vidéo ou de l'écriture, que la finalité soit ou non une création artistique. La société actuelle semble animée de ce que l'on pourrait appeler un désir d' "extimité" généralisé, dont les nouvelles technologies ont rendu l'expression aisée* »[86].

B. L'impact des réseaux sociaux en ligne à l'échelle de la société

21. L'impact des réseaux sociaux en ligne sur l'économie numérique. L'apparition des grandes plateformes numériques et la généralisation progressive de leur utilisation ont permis

[80] L'autoprésentation de soi se retrouve dans diverses pratiques : entretiens d'embauche, *speed dating*, téléréalité, autobiographies, etc.
[81] F. ROCHELANDET, *Economique des données personnelles*, coll. Repères, La découverte, 2010, p. 83.
[82] F. QUINTON, « Quelles questions Facebook nous pose-t-il ? », ina global, le 4 février 2014, <http://www.inaglobal.fr/numerique/article/quelles-questions-facebook-nous-pose-t-il> (dernière consultation le 9 octobre 2019).
[83] D. KAPLAN, *Informatique, libertés, identités*, FYP, 2010, p. 27.
[84] L'autrichien et étudiant en droit Maximilian Schrems a pu constater cela après avoir demandé à Facebook l'accès à ses informations personnelles. Le réseau social lui a retourné en réponse un DVD de plus de 1200 pages en PDF d'informations le concernant, trois ans d'activité sur le réseau social scindé en 57 catégories.
[85] L. ALLARD, F. VANDENBERGHE., « Express Yourself ! Les pages perso. Entre légitimation technopolitique de l'individualisme expressif et authenticité réflexive peer to peer », *Réseaux*, vol. 21, n° 117, 2003, p. 191-220.
[86] S. TISSERON, *L'intimité surexposée*, Hachette littérature, 2001, p. 52.

l'abondance et l'explosion des données personnelles. Les traces numériques générées par l'activité des individus interconnectés ont été captées, croisées et interprétées par les géants d'internet favorisant l'émergence du phénomène du *Big Data*[87]. Sur ce point, les sites de réseaux sociaux et particulièrement le site Facebook s'érige en acteur clé en la matière en raison de la masse et de la variété des données qu'il génère du fait de l'activité de ses utilisateurs. L'expression *Big Data*, que l'on peut traduire littéralement par « *grosses données* » ou « *mégadonnées* »[88], est apparue en 2008 sous la plume des analystes du cabinet américain Gartner. La définition de cette notion répond à la règle des 3V[89]. Le *Big Data* fait d'abord référence à un grand *volume* de données stockées[90]. Ensuite, le *Big Data* représente une grande *variété* de données provenant du web (*web mining*), qui se matérialisent en format texte[91] ou encore en format image[92]. Enfin, le *Big Data* renvoie à une grande *vélocité* quant à la fréquence à laquelle les données sont générées, capturées et partagées. Plus généralement, le groupe de l'article 29 conçoit le *Big Data* comme un ensemble de données numériques gigantesque détenues par des sociétés privées, des gouvernements ou n'importe quelle autre grande organisation. Contrairement aux bases de données classiques qui regroupent des ensembles de données très structurées, le *Big Data* constitue un ensemble d'informations hétérogènes peu structurées et analysées en temps réel. Désormais, le comportement de l'internaute est analysé de façon dynamique, ce qui cause de véritables bouleversements technologiques et organisationnels par rapport aux anciennes méthodes d'analyse de données. Cela s'observe par un changement quantitatif qui correspond à la démultiplication du volume de données à traiter, mais aussi par un changement qualitatif en raison du fait que le *Big Data* ne porte plus sur des données préalablement échantillonnées[93].

22. Au-delà de ces aspects techniques, le *Big Data* renferme de véritables enjeux économiques. L'ensemble des traces numériques laissées par l'internaute servent de base pour profiler des tendances de consommation détaillées, permettant aux agents économiques non seulement d'anticiper les comportements de consommation mais également de les influencer. Ainsi, les données personnelles générées par l'action des internautes constituent une véritable

[87] S. SOLTANI, « "Big data" et le principe de finalité », *RLDI*, 2013, n° 97.
[88] Terme recommandé en France par la DGLFLF, JO du 22 août 2014.
[89] Cette règle se retrouve dans le *Gartner IT Glossary*.
<http://www.gartner.com/it-glossary/big-data> (dernière consultation le 9 octobre 2019).
[90] À titre d'exemple, Twitter générait en janvier 2013 7 teraoctets de données chaque jour et Facebook 10 teraoctets.
[91] Comme par exemple les cookies qui sont de petits fichiers textes stockés sur le terminal de l'internaute et qui renseignent sur les sites fréquentés par l'internaute.
[92] Facebook traite plus de 50 milliards de photos ce qui fait de lui la plus grande bibliothèque d'images du monde.
[93] S. SOLTANI, « "Big data" et le principe de finalité », *RLDI*, 2013, n° 97.

valeur et notion économique[94]. Plus encore, elles seraient devenues le nouvel « or noir » de l'économie mondiale. Dès lors, la détention des données personnelles et la maîtrise des outils technologiques qui permettent de les valoriser représentent un avantage certain sur le plan concurrentiel, faisant du réseau social Facebook l'un des acteurs dominants de ce secteur économique. Ainsi, dans son site *Facebook business*[95], le réseau social propose aux entreprises un profilage précis des internautes leur permettant ensuite d'effectuer des publicités ciblées sur un type de population en particulier[96]. En conséquence, en 2019, plus de 2,234 milliards d'utilisateurs se voient proposer sur le réseau social Facebook une publicité personnalisée. L'économie n'est plus uniquement représentée par le système classique de création de valeur basé sur le travail fourni par chaque individu, mais dorénavant également par un système de captation de valeur résumé dans l'expression : « *si c'est gratuit c'est que vous êtes le produit* ». Loin de s'en cacher, les grands acteurs du web affirment ce modèle économique à l'image du site Facebook qui précise à ses utilisateurs dans ses conditions générales d'utilisation : « *Au lieu de payer pour l'utilisation de Facebook et des autres produits et services que nous offrons, en utilisant les Produits Facebook inclus dans les présentes Conditions, vous acceptez que nous vous montrions les publicités payées par les entreprises et organisations pour que nous les promouvions sur les Produits des entités Facebook et en dehors. Nous utilisons vos données personnelles, telles que les informations concernant votre activité et vos intérêts, afin de vous montrer des publicités plus pertinentes pour vous* »[97]. De plus, le rôle des sites de réseaux sociaux au sein de l'économie est de nature à se diversifier, en témoigne le projet de cryptomonnaie appelée la Libra[98] dévoilé par le réseau social Facebook le 18 juin 2019. Ce projet vise à permettre aux utilisateurs du réseau social d'effectuer entre eux des transferts de fonds *via* les services de messagerie du site. Par ailleurs, la cryptomonnaie pourrait également servir à régler des achats directement sur les filiales ou partenaires du site tels que les sociétés Uber, Lyft, Spotify, Paypal ou encore Mastercard. À terme, ses concepteurs souhaiteraient en faire une monnaie stable permettant à leurs utilisateurs de payer des achats du quotidien[99].

[94] V. sur le sujet : F. ROCHANDELET, *Économie des données personnelles et de la vie privée*, *op. cit.*
[95] <https://www.facebook.com/business>
[96] Par exemple pour la catégorie personnes aisées correspondant aux 13% des français les plus riches, Facebook quantifie leurs probabilités d'achats sur différents types de produits. Ainsi cette catégorie dispose de + 30% de chance d'acheter des cosmétiques de plus de 75 € ou + 33% de chance d'acheter des robes à plus de 1000 euros.
[97] <https://www.facebook.com/terms>
[98] <https://libra.org/fr-FR>
[99] J. LAUSSON, « Libra : tout ce qu'il faut savoir sur la future cryptomonnaie propulsée par Facebook, Iliad, PayPal, Uber… », numerama, 18 juin 2019.

23. Les enjeux démocratiques suscités par les sites de réseaux sociaux. Au-delà du simple secteur économique, l'usage des sites de réseaux sociaux impacte la société en général révélant certains enjeux démocratiques fondamentaux. En effet, l'utilisation des données personnelles peut également revêtir un intérêt particulier sur le plan politique. Certains scandales ont permis de mettre en lumière l'étendue et les finalités de la captation des données personnelles des usagers des sites de réseaux sociaux. C'est le cas notamment du lanceur d'alerte Edward Snowden qui révéla en juin 2013 la collecte massive par l'administration américaine des données issues notamment du réseau social Facebook[100]. Les documents mis en ligne établirent l'existence au sein de la *National Security Agency* (NSA) du programme de surveillance *PRISM* s'attachant à cibler les données des personnes vivant hors des États-Unis et venant compléter le programme *XKeyscore*[101]. Leurs finalités dépassaient en l'occurrence la seule lutte contre le terrorisme et aboutissaient à une surveillance généralisée des communications sur internet par l'administration américaine[102]. Plus récemment, une affaire est venue dénoncer le recueil massif des données personnelles de plus de 87 millions d'utilisateurs du réseau social Facebook par la société britannique *Cambridge Analytica*. Le recueil de ces informations a ainsi servi à influencer les intentions de votes en faveur d'hommes politiques ayant fait appel aux services de cette société[103]. Les sites de réseaux

<https://www.numerama.com/business/523272-la-cryptomonnaie-de-facebook-ce-que-lon-sait.html> (dernière consultation le 9 octobre 2019).

[100] Le 7 juin 2013 le quotidien britannique *The Guardian* ainsi que le *Washington post* publièrent les documents transmis par l'ex-consultant de la *National Security Agency* (NSA) et attestant que l'administration américaine exploite un vaste programme d'interception des communications Internet à l'échelle mondiale avec la coopération des principaux fournisseurs américains de services en ligne tels que Microsoft, Yahoo !, Skype, Google et Facebook. La NSA dispose pour ce faire d'un accès direct aux données hébergées par les géants américains du Web, sites de réseaux sociaux compris. V. sur le sujet le film-documentaire « *Citizenfour* », retraçant le scandale d'espionnage mondial de la NSA au travers des révélations d'Edward Snowden, réalisé par Laura Poitras et sorti en 2014 ; V. également les travaux des auditeurs de l'Institut National des Hautes Études de la Sécurité et de la Justice : « L'affaire PRISM. Quelles conséquences pour la sûreté et le développement des entreprises ? », Travaux de la 18ème session nationale spécialisée 2014-2015 « Protection des entreprises et intelligence économique », Novembre 2015.

[101] XKeyscore est un programme de surveillance de masse créé par la NSA et opéré conjointement avec les services de renseignements britanniques, canadiens, australiens et néo-zélandais1, services dont la coopération historique en matière de partage de l'information a entraîné le surnom des « Five Eyes ». Il permettrait une « collecte quasi systématique des activités de tout utilisateur sur Internet »1, grâce à plus de 700 serveurs localisés dans plusieurs dizaines de pays.

[102] PRISM aurait également été utilisé comme arme économique en permettant « *d'accompagner les entreprises américaines sur les marchés ouverts à la concurrence internationale, afin de leur donner une longueur d'avance* ». Institut National des Hautes Études de la Sécurité et de la Justice, « L'affaire PRISM. Quelles conséquences pour la sûreté et le développement des entreprises ? », Travaux de la 18ème session nationale spécialisée 2014-2015 « Protection des entreprises et intelligence économique », Novembre 2015, p. 13.

[103] Par exemple, en 2015, la société *Cambridge Analytica* s'est engagée pour Ted Cruz dans sa campagne pour les élections primaires présidentielles américaines. Après l'échec du candidat, la société a travaillé à partir de 2016 pour la campagne présidentielle de Donald Trump. La société *Cambridge Analytica* aurait au final eu un rôle certain dans de nombreuses campagnes électorales aux États-Unis, en Europe, en Asie et en Afrique. Son ancien directeur de recherche, Christopher Wylie, a sur ce point affirmé qu'elle aurait joué un « *rôle crucial* » dans le vote en faveur du BrexitV. l'entretien accordé par Christopher Wylie au journal Libération : « Sans

sociaux constituent dès lors une arme de campagne redoutable pour les candidats. Donald Trump a d'ailleurs déclaré après sa victoire à l'élection présidentielle américaine de 2016 : « *Sans Twitter, je ne serais probablement pas là. J'ai près de cent millions d'abonnés sur Facebook, Twitter et Instagram. J'ai mon propre média. Je n'ai pas besoin de m'en remettre aux faux médias* »[104]. De nombreuses études se sont dès lors attachées aux effets produits par ces nouvelles plateformes relationnelles sur le système démocratique en particulier sur le pouvoir d'impact des « *fake news* » sur les processus électoraux[105]. En réalité, bien qu'il soit incontestable qu'un nombre important d'informations trompeuses ait été diffusé sur les sites de réseaux sociaux au moment de l'élection américaine de 2016 et du vote en faveur du Brexit, le sociologue Dominique Cardon nuance toutefois leur réel pouvoir d'impact. Ce dernier rappelle qu'il demeure extrêmement difficile de mesurer l'effet direct d'un message vu, lu ou entendu sur un comportement d'autant plus que l'exposition à une fausse information ne suscite pas nécessairement la croyance dans cette information[106]. Monsieur le Professeur Idris Fassassi rappelle ainsi que si les sites de réseaux sociaux ancrent, voire amplifient les travers de nos sociétés, ils ne les créent pas eux-mêmes[107]. Leur force réside dans leur pouvoir d'accentuer les tensions au sein de nos sociétés notamment lors de moment démocratiques clés. Il convient dès lors de mettre en évidence les nouveaux enjeux juridiques suscités par ces derniers.

Section 2 : Les réseaux sociaux en ligne, nouveaux enjeux juridiques

24. Le fort impact des sites de réseaux sociaux à l'échelle individuelle et sociétale révèle des enjeux fondamentaux dans de nombreuses matières : en sociologie, en économie, en sciences politiques. De son côté, le droit n'échappe pas aux nombreuses problématiques

---

Cambridge Analityca, il n'y aurait pas eu de Brexit », propos recueillis par Sonia Delesalle-Stolper, le 26 mars 2018.

[104] Propos de Donald Trump, interview à Fox News, 15 mars 2017. *In* : I. FASSASSI, « Les effets des réseaux sociaux dans les campagnes électorales américaines », *Les Nouveaux Cahiers du Conseil constitutionnel*, vol. 57, nº 4, 2017, p. 69.

[105] V. par exemple : D. CARDON, *Culture numérique*, Presses de Science Po, 2019, préc. chap. « Fake news panic : les nouveaux circuits de l'information », p. 261 ; D. CARDON, *La Démocratie Internet. Promesses et limites*, Seuil, Paris, 2010 ; I. FASSASSI, « Les effets des réseaux sociaux dans les campagnes électorales américaines », *Les Nouveaux Cahiers du Conseil constitutionnel*, vol. 57, nº 4, 2017, p. 69 ; P. SEGUR, S. PIERE-FREY, *L'internet et la démocratie numérique*, Presses Universitaires de Perpignan, 2016.

[106] D. CARDON, *Culture numérique*, Presses de Science Po, 2019, préc. chap. « Fake news panic : les nouveaux circuits de l'information », p. 261.

[107] I. FASSASSI, « Les effets des réseaux sociaux dans les campagnes électorales américaines », *Les Nouveaux Cahiers du Conseil constitutionnel*, vol. 57, nº 4, 2017, p. 86.

propres à ces nouveaux acteurs de l'internet. Loin d'être une zone de non droit, les sites de réseaux sociaux se révèlent en réalité être un nouvel espace où une multitude de droits sont applicables (**§1**), la présente étude se recentrant précisément sur les problématiques juridiques propres au droit pénal (**§2**).

§1. Une multitude de droits applicables

25. Les réseaux sociaux ne sont pas une zone de non droit. Dans l'imagerie fantasmée d'un espace internet affranchi de toute règle certains s'amusent à comparer le Grand Ouest américain auquel se substitue désormais les étendues de la Silicon Valley[108] ou encore la *lex mercatoria* s'appliquant à un espace maritime sans frontières se mutant aujourd'hui en une *lex electronica* régulant un espace numérique mondialisé[109]. Cette théorie d'un internet zone de non-droit n'a cependant jamais existé et n'a en aucun cas vocation à s'appliquer à la catégorie particulière que forment les réseaux sociaux en ligne au sein du web. Bien loin d'un non-droit, internet constitue en réalité une zone d'enchevêtrement des droits. D'une part, ceci s'explique par le caractère général des lois préexistantes à ce nouveau format de communication. L'exemple le plus frappant est celui de la loi du 29 juillet 1881 sur la liberté de la presse qui trouve aujourd'hui une application particulièrement étendue sur les sites de réseaux sociaux. D'autre part, dès l'émergence du réseau internet le législateur a pris la mesure de ce tournant en adoptant des lois rendues nécessaires par l'évolution technologique. Ainsi, en France, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite « *loi informatique et libertés* »[110] proposait déjà un encadrement des données personnelles ; ensuite, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[111] a notamment défini les différents régimes de responsabilité civile et pénale applicables aux différents acteurs d'internet ; plus récemment encore, la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique[112] aborde quant à elle des thèmes nouveaux tels que la portabilité des données ou la mort en ligne. En réalité, comme le souligne Francis Donnat, la difficulté est ailleurs : « *Elle tient en premier lieu au décalage*

[108] V. par exemple : F. DONNAT, *Droit européen de l'internet, Réseaux, données, services*, LGDJ, Systèmes, 2018, p. 11, n° 1 ; V. FAUCHOUX, P. DEPREZ, *Droit de l'internet*, Litec, Paris, 2009, p. 1.
[109] O. CACHARD, *La régulation du marché électronique*, LGDJ, 2002, pp. 18 et suiv ; F. DONNAT, *Droit européen de l'internet, Réseaux, données, services*, *op. cit.*, p. 11, n° 1.
[110] L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, 7 janvier 1978 p. 227.
[111] L. n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *JORF* n° 0143, 22 juin 2004, p. 11168.
[112] L. n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n° 0235, 8 octobre 2016.

entre le droit et le fait, entre la norme et la réalité technologique. Le problème n'est pas tant qu'internet ne serait soumis à aucun droit, mais plutôt que ce droit court en permanence après l'innovation à tel point qu'il peut apparaître rapidement inadapté, obsolète, voire inapplicable. Problématique différente qui n'est pas l'absence de normes mais leur capacité à résister à l'assaut du temps »[113].

26. Des problématiques juridiques de différente nature. Les sites de réseaux sociaux suscitent une myriade de problématiques juridiques liées à leurs spécificités intrinsèques ou à l'usage qui en est fait. Dans ce sens il est affirmé que : « *la nouveauté et la spécificité des* [sites de réseaux sociaux] *par rapport aux autres médias sociaux amènent le juriste à constater l'existence d'un "concentré de problèmes juridiques autour de frontières nouvelles"* »[114]. Sans prétendre à l'exhaustivité, certaines problématiques juridiques peuvent être mises en évidence afin de démontrer l'implication de l'ensemble des branches du droit en la matière. Par exemple, les particularités des principaux sites de réseaux sociaux, notamment quant à l'étendue de leur utilisation, impliquent des réflexions en droit de la concurrence en raison de la situation monopolistique occupée par certaines plateformes à l'image du réseau social Facebook, mais également en droit international public ou privé en raison leur dimension transnationale. De plus, leur modèle de fonctionnement basé sur la collecte de données personnelles est source de convoitises pour les États, ce qui amène à un développement du droit du renseignement et plus particulièrement à l'extension des techniques intrusives au bénéfice des autorités publiques, permettant la captation des données des utilisateurs. En conséquence, la dimension particulière prise par les sites de réseaux sociaux dans nos sociétés est source d'enjeux majeurs concernant la sauvegarde des libertés fondamentales telles que le droit au respect de la vie privée ou encore le droit à la liberté d'expression.

27. D'autres problématiques juridiques se révèlent également par l'usage des réseaux sociaux en ligne. Au moment de son inscription sur un site de réseau social l'utilisateur passe un contrat avec son opérateur. Le droit des contrats constitue la première relation juridique qui lie l'utilisateur au réseau social. Outre le droit des contrats, l'inscription sur un réseau social appelle également l'application du droit de la consommation en raison du statut de consommateur accordé à leurs utilisateurs. Le droit du travail trouve à s'appliquer lorsque les

[113] F. DONNAT, *Droit européen de l'internet, Réseaux, données, services, op. cit.*, pp. 11-12, n° 1-2-3.
[114] L. PAILLER, *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, larcier, 2012, p. 20, citant : J.-E. RAY, « Little brothers are watching you », obs. sous CPH Boulogne-Billancourt, 19 novembre 2010, Semaine sociale Lamy, 6 décembre 2010, n° 1470, p. 10.

travailleurs utilisent ce moyen de communication sur leur lieu de travail ou pour s'exprimer à propos de leur entreprise. Par ailleurs, la mise en avant et le partage de certains contenus appelle également des nouvelles problématiques concernant le droit des marques et le droit de la propriété intellectuelle. Par exemple, certaines pratiques favorisées par les sites de réseaux sociaux, telles que les *mash-ups*[115], amènent à redéfinir les contours de la protection offerte par le droit d'auteur. Enfin, les réseaux sociaux représentent la transposition et l'amplification des rapports humains dans l'espace numérique, il est donc logique d'y retrouver certains comportements délictueux. Les sites de réseaux sociaux forment alors un espace d'étude pour le droit pénal. Les réseaux sociaux en ligne seront en l'occurrence spécifiquement analysés sous l'angle de ce dernier.

§2. Les problématiques juridiques propres au droit pénal

28. Justification de l'approche pénaliste. Si les problématiques juridiques soulevées par l'usage ou la simple présence des sites de réseaux sociaux ne peuvent à l'évidence se résumer à la seule matière pénale, l'approche pénaliste s'avère révélatrice de forts enjeux juridiques justifiant une étude particulière. Selon André Vitu, le droit pénal constitue en effet le « *miroir de la civilisation* » en ce qu'il permet d'appréhender d'une façon vivante et concrète « *le développement, les conditions de vie, la morale, la situation économique, les principes d'une civilisation déterminée* »[116]. Le droit pénal est de ce fait particulièrement sensible à l'évolution des modes de vie et des courants d'idées, ainsi lorsque la société évolue il est logique que la législation pénale en fasse de même[117]. Pour illustrer ses propos, André Vitu donnait l'exemple suivant : « *des pratiques telles que la conduite d'une automobile ou la consommation de l'opium, tant qu'elles ne concernaient qu'une poignée de riches excentriques, pouvaient ne faire l'objet d'aucune réglementation spécifique* »[118]. Cet exemple met en exergue la fonction axiologique du droit pénal par laquelle ce dernier exprime les valeurs essentielles d'une société humaine. Le droit pénal élabore ainsi l'ordre public en identifiant les comportements pouvant faire l'objet d'incriminations, et veille par ailleurs à son respect au moyen de son pouvoir sanctionnateur. Or, les sites de réseaux sociaux

[115] « *Collage hétérogène d'œuvres différentes ou, inversement, forme de fusion de deux œuvres dans une troisième* ». P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *CCE* n° 4, Avril 2016, étude 8.
[116] R. MERLE, A. VITU, *Traité de droit criminel. Droit pénal spécial*, éd. Cujas, 1982, p. 13, n° 6.
[117] *Ibid.*, p. 14, n° 7.
[118] P.-X. BOYER, « La judiciarisation de l'Internet », *in* F. ROUVILLOIS (dir.), *La société au risque de la judiciarisation*, Litec, 2008, Colloques & débats, 2008, p. 55.

représentent un tournant sociétal suffisamment important et ancré de nature à faire évoluer le droit pénal. À titre d'exemples, ils ont permis la démultiplication de certains comportements délinquants particulièrement les infractions de presse prévues par la loi du 29 juillet 1881[119] au point d'amener certains à observer que « *la liberté d'expression sera, dans vingt ou trente ans, ce que les réseaux sociaux auront fait d'elle* »[120]. Ils ont par ailleurs généré de nouvelles formes de délinquance propres à l'environnement numérique, en témoigne le développement fulgurant des usurpations d'identité numérique qui a accompagné l'émergence de ces moyens de communication. Une étude des réseaux sociaux en ligne sous le prisme du droit pénal s'avère dès lors justifiée.

29. Les enjeux au regard des principes fondamentaux du droit pénal. Les pénalistes, tout comme les travaillistes[121], accueillent le développement des grandes plateformes numériques avec mesure au regard de la difficile conciliation des principes fondamentaux du droit pénal et des caractéristiques de ces nouveaux moyens de communication. Monsieur Marc Dalloz relève ainsi ces ambiguïtés entre le droit pénal et la nouvelle économie collaborative générée par ces grandes plateformes numériques :

« *L'économie collaborative est en effet un phénomène mondialisé quand le droit pénal est très national, un secteur d'innovation perpétuelle quand le droit pénal a une propension conservatrice, une activité dématérialisée quand le droit pénal est très attaché à la matérialité infractionnelle, une action collective et diffuse alors que nul n'est pénalement responsable que de son propre fait, une activité parfois algorithmique alors qu'il n'y a point de crime ou de délit sans intention de le commettre. Appréhender pénalement ce qui mérite d'être qualifié d'illégal dans cette nouvelle économie est donc un véritable défi* »[122].

Les changements sociétaux induits par l'usage massif des sites de réseaux sociaux entrent en conflit avec les systèmes juridiques traditionnels et mettent à l'épreuve les principes fondamentaux sur lesquels ils reposent. Sur ce point, le droit pénal dispose de la capacité d'absorber de nouveaux concepts pouvant donner lieu à certaines adaptations législatives à condition que celles-ci restent conformes à la philosophie profonde de la

[119] L. sur la liberté de la presse du 29 juillet 1881, *JORF* 30 juillet 1881, p. 4201.
[120] R. LE GUNEHEC, « Twitter et la vie d'avant : les réseaux sociaux changent-ils tout ? », *Légipresse* n° 355, décembre 2017, p. 597.
[121] Pour une approche travailliste des défis juridiques soulevés par les plateformes numériques v. : B. GOMES, *Le droit du travail à l'épreuve des plateformes numériques*, Thèse, Université Paris 10 (Nanterre), 3 décembre 2018.
[122] M. DALLOZ, « Quel droit pénal pour réguler l'économie collaborative ? », *in Quelles régulations pour l'économie collaborative ?,* Dalloz, 1ère éd., 2018, p. 159.

matière[123]. Le droit pénal contemporain dispose d'une fonction protectrice se justifiant par le caractère profondément attentatoire aux libertés individuelles de la répression pénale. Pour ce faire, le droit pénal consacre de nombreux principes à valeur supralégislative qui encadrent la loi pénale et assurent ainsi le respect et la garantie des droits et libertés. À ce titre, le principe de légalité des délits et des peines[124] constitue le principe fondamental du droit pénal selon lequel il ne peut y avoir d'infraction ou de peine sans un texte légal : « *nullum crimen, nulla poena sine lege* ». En plus d'exister, la norme doit également être claire et précise de manière à ce que « *chaque comportement incriminé sous la menace d'une peine soit immédiatement identifiable* », autrement dit, « *les textes publiés ne doivent laisser aucune place au doute* »[125]. Le principe de légalité criminelle se justifie du point de vue juridique par des considérations d'intérêt public et privé : d'un côté il donne à la sanction pénale une certitude qui renforce son pouvoir d'intimidation qui ne peut qu'être profitable à la société ; d'un autre côté il constitue l'une des garanties essentielles de la liberté individuelle permettant au citoyen, du fait de connaître à l'avance ce qui est défendu et la peine à laquelle il s'expose en le faisant, d'être protégé contre l'arbitraire du juge[126]. Le principe de légalité criminelle induit en réalité une série de corolaires possédant chacun d'eux tout autant une valeur fondamentale. Il s'agit notamment des principes d'interprétation stricte de la loi pénale, de non-rétroactivité de la loi pénale, de nécessité et de proportionnalité des peines qui viennent également encadrer le législateur dans son travail d'élaboration du droit pénal et le juge dans l'application de celui-ci. Dans cette hypothèse, si l'environnement des réseaux sociaux en ligne incite le droit pénal à quelques évolutions, ces dernières doivent toutefois intervenir dans le respect de ces principes fondamentaux, « *dès lors le droit pénal ne doit pas trop promettre et, s'il devra sans doute faire quelques compromis, il ne devra pas se compromettre* »[127].

---

[123] C. COURTAIGNE, *L'adéquation du droit pénal à la protection de l'environnement*, Thèse, Université de Paris II (Panthéon-Assas), soutenue le 15 septembre 2010, p. 28, n° 38.

[124] Ce principe se retrouve pour la première fois dans la Déclaration des droits de l'homme et du citoyen de 1789 (art. 5 : « *Tout ce qui n'est pas défendu par la loi ne peut être empêché, et nul ne peut être contraint de faire ce qu'elle n'ordonne pas* » et art. 8 : « *Nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit et légalement appliquée* »). Le Code pénal de 1810 vient le réaffirmer à son article 4 qui disposait : « *Nulle contravention, nul délit, nul crime ne peuvent être punis de peines qui n'étaient pas prononcées par la loi avant qu'ils fussent commis* ». Ce principe se retrouve dans le droit pénal contemporain à l'article 111-3 du Code pénal selon lequel : « *Nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi ou pour une contravention dont les éléments ne sont pas définis par le règlement* ». Le deuxième alinéa précise : « *Nul ne peut être puni d'une peine qui n'est pas prévue par la loi, si l'infraction est un crime ou un délit, ou par le règlement, si l'infraction est une contravention* ».

[125] E. DREYER, *Droit pénal général*, LexisNexis, 5ème éd., 2019, p. 242, n° 278.

[126] B. BOULOC, *Droit pénal général*, Dalloz, coll. Précis, 26ème éd., 2019, p. 104, n° 106.

[127] M. DALLOZ, « Quel droit pénal pour réguler l'économie collaborative ? », *in Quelles régulations pour l'économie collaborative ?,* Dalloz, 1ère éd., 2018, p. 159.

30. Le droit pénal face à l'internationalité des réseaux sociaux en ligne. Par ailleurs, le cadre d'expression mondialisé mis en œuvre par les principaux sites de réseaux sociaux constitue un autre défi à relever pour le droit pénal au regard du principe de souveraineté territoriale de la loi pénale. Ce principe est affirmé à l'article 113-2 du Code pénal qui dispose : « *la loi pénale française est applicable aux infractions commises sur le territoire de la République* ». En conséquence, l'action publique peut être exercée même si les faits ont été dénoncés à une autorité étrangère et ont donné lieu à une condamnation définitive dans son pays[128]. Plus généralement, un tel principe affirme le pouvoir régalien des États qui leur permet de disposer au sein de leurs espaces territoriaux de leur propre législation. Partant, « *l'objectif à atteindre est de parvenir à concilier le caractère spatiotemporel - délimité et stable - de la norme de droit pénal avec le caractère global de l'espace virtuel* »[129]. Cette finalité semble difficilement réalisable tant le droit pénal se trouve d'une part confronté à l'universalité d'internet et aux multiples facettes de la cybercriminalité et d'autre part, se heurte à l'ubiquité et à l'immédiateté qui caractérisent les flux d'informations sur les sites de réseaux sociaux[130]. Aussi, dans une logique d'adaptation aux formes modernes de communication, le droit pénal français s'est alors doté d'un nouvel instrument juridique. L'article 113-2-1 du Code pénal a introduit par la loi n° 2016-731 du 3 juin 2016[131] une règle spécifique en matière d'infractions commises au moyen d'un réseau de communication électronique. Cette nouvelle disposition reconnait l'application la compétence territoriale de la loi pénale française dès lors que tout crime ou tout délit commis ou tenté au moyen d'un réseau de communication électronique porte préjudice à une personne physique qui réside sur le territoire national ou à une personne morale dont le siège se situe sur le territoire de la République. Aussi, en matière de communication au public en ligne, ce nouveau critère se substitue à celui de la focalisation du contenu vers le public français utilisé par la jurisprudence[132]. Par ailleurs, si les critères de compétence territoriale de la loi pénale

[128] B. BOULOC, *Droit pénal général*, Dalloz, coll. Précis, éd. n° 26, août 2019, p. 176, n° 178.
[129] J. FRANCILLON, « La compétence pénale territoriale française à l'épreuve de la cybercriminalité », *in* Mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, p. 208.
[130] *Ibid.*
[131] L. n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, *JORF* n° 0129, 4 juin 2016.
[132] Selon la jurisprudence, en matière d'internet, la simple accessibilité d'un contenu sur le territoire français ne suffit pas à reconnaître l'application de la loi pénale française, le contenu doit être en outre orienté vers le public français justifiant ainsi son rattachement au territoire de la république. V. par exemple : Crim., 14 décembre 2010, n° 10-80.088 : inédit ; *D.* 2011 p. 1055, note E. DREYER ; *RSC* 2011 p. 651, note J. FRANCILLON ; *RTD Com.* 2011 p. 356, note F. POLLAUD-DULIAN – Crim. 12 juillet 2016, n° 15-86.645 : Publié au Bulletin ; *Dalloz IP/IT* 2016 p. 618, note B. AUROY ; *CCE* n° 10, Octobre 2016, comm. 83, A. LEPAGE ; *D.* 2016 p. 1848, note E. DREYER – Crim. 23 janv. 2018, n° 17-80.323 : inédit ; *Légipresse* 2018, p. 154, note

française s'avèrent extensifs pour les infractions commises sur internet, cela n'élude pas pour autant le problème d'effectivité du droit pénal concernant la répression des infractions présentant un caractère d'extranéité particulièrement lorsque l'auteur se trouve en dehors de l'Union européenne. Les difficultés liées à la coopération policière ou à l'entraide juridictionnelle qui impliquent notamment une extradition de l'auteur de l'infraction[133] ou à l'impossible exequatur d'une décision de condamnation dans un ordre juridique étranger[134] ne sont cependant pas spécifiques aux sites de réseaux sociaux mais concernent en réalité l'architecture du cyberespace prise dans son ensemble. Cette problématique se rattache au sujet plus général de la justice pénale face à la cybercriminalité ayant déjà fait l'objet d'études spécifiques[135].

31. Sans être évincé du présent raisonnement, l'aspect international se retrouvera à travers des problématiques propres aux sites de réseaux sociaux faisant l'originalité du sujet. La dimension internationale de ces derniers sera envisagée par le biais de la coopération des opérateurs des réseaux sociaux avec l'autorité judiciaire nationale dans l'identification des auteurs d'infractions, cette problématique étant prégnante sur ces espaces d'échanges du fait qu'ils favorisent, ou du moins autorisent, l'usage d'un pseudonyme et par là même l'anonymat de leurs utilisateurs. De plus, la coopération avec l'autorité judiciaire relève d'un enjeu certain tant les sites de réseaux sociaux disposent d'informations nombreuses et détaillées de leurs utilisateurs. Par ailleurs, l'émergence d'une réponse alternative à la commission des infractions sur les réseaux sociaux favorisée par le développement et l'encadrement d'un pouvoir de régulation de leurs opérateurs témoigne dans une certaine mesure d'une internationalisation, voire plus encore d'une dématérialisation de la réponse aux

---

E. DREYER ; *Gaz. Pal.* 30 avril 2018, n° 16, p. 52, obs. S. DETRAZ – Crim. 6 mars 2018, n° 16-87.533 : inédit ; *Dr. pén.* 2018, n° 6, comm. 105, note P. CONTE ; *Gaz. Pal.* 22 mai 2018, n° 18, p. 38, obs. F. FOURMENT – Crim. 19 juin 2018, n° 17-86.604 : inédit ; *RSC* 2019 p. 109, note E. DREYER.

[133] L'extradition est la demande d'un État (l'État requérant) à un autre État (l'État requis) de lui remettre afin de poursuites ou jugement ou afin d'exécution d'une peine un délinquant ou criminel. L'État requérant mène une extradition active alors que l'Etat requis mène une extradition passive. Il s'agit d'un acte participant des relations internationales (relations d'État à État). L'art 696-2 du Code de procédure pénale précise que « *le gouvernement français peut remettre, sur leur demande, aux gouvernements étrangers, toute personne n'ayant pas la nationalité française* ». L'extradition relève alors de l'opportunité politique, il s'agit d'un acte de souveraineté étatique.

[134] L'exequatur consiste à exécuter une décision étrangère après l'application d'une procédure permettant d'en contrôler la conformité. Cependant, la territorialité des jugements répressifs s'oppose à l'exécution des condamnations pénales étrangères et donc à leur exequatur. L'exequatur n'est donc possible qu'en matière civile ou concernant les dispositions civiles des condamnations pénales. D. REBUT, *Droit pénal international*, Dalloz, coll. précis, 2ème éd., nov. 2014, p. 448, n° 746. Notons toutefois l'existence du principe de reconnaissance mutuelle des condamnations pénales au sein de l'Union européenne reconnu à l'article 707-1 du Code de procédure pénale.

[135] Pour une récente étude sur le sujet v. : F. SKAF, *La justice pénale face à la cybercriminalité*, Éditions universitaires européennes, 2018.

infractions. Ainsi, sur les sites de réseaux sociaux, la problématique de l'effectivité de la réponse pénale trouve aujourd'hui des éléments de réponse dans la mise en place d'un système de régulation des contenus ne se souciant pas du lieu de leur émission mais, au contraire, du lieu de leur réception. Au final, « *loin d'être une zone sans frontière, internet est un réseau à la fois mondial et régional, qui obéit tout autant à des règles universelles qui sous-tendent son fonctionnement qu'aux législations nationales applicables sur le territoire dans lequel les activités ont lieu* »[136]. Au sein de ces espaces virtuels mondialisés les États, par l'intermédiaire du droit pénal, ont encore un rôle à jouer, plus encore, ils se révèlent être un gardien essentiel des valeurs fondamentales de nos sociétés. Le cadre spatial délimité de la loi pénale ne doit pas être perçu comme une limite mais, au contraire, comme un contrepouvoir essentiel à l'hégémonisme de ces acteurs dominants du cyberespace.

32. Droit pénal et régimes spéciaux. Outre le droit pénal commun, les sites de réseaux sociaux, en tant que moyens de communication au public en ligne, exigent l'intégration de différents régimes spéciaux dans le cadre du développement. C'est le cas de la loi sur la liberté de la presse du 29 juillet 1881[137] qui vient régir les limites admissibles de l'expression publique dans nos sociétés mais également de la loi pour la confiance en l'économie numérique (LCEN)[138] qui détermine quant à elle les régimes de responsabilité applicables aux acteurs d'internet. Cependant, dans un souci de clarté et d'homogénéité, tous les pans du droit pénal ayant vocation à s'appliquer au sein de l'espace numérique créé par les sites de réseaux sociaux ne pourront être abordés. Ainsi, les atteintes à la propriété intellectuelle sur les plateformes numériques ne feront pas l'objet de développements spécifiques mais serviront tout au plus d'appuis ponctuels dans la démonstration. Ce choix se justifie par le fait que cette thématique, d'une particulière richesse, devrait requérir une étude à part en entière. Mais surtout, l'analyse des problématiques liées à la propriété intellectuelle à l'échelle numérique nécessiterait une modification du présent champ d'analyse pour y inclure également les plateformes de partage de contenus qui sont le principal vecteur des atteintes à la propriété intellectuelle. Le cantonnement du sujet aux seuls sites de réseaux sociaux s'explique alors par la volonté d'étudier spécifiquement l'évolution de la dimension sociale de l'espace numérique et d'analyser sous l'angle du droit pénal les formes variées d'interactions entre les personnes permises par ces sites et les abus qui en découlent. C'est pourquoi la présente étude

[136] F. DONNAT, *Droit européen de l'internet, Réseaux, données, services*, LGDJ, Systèmes, 2018, pp. 11-12, n° 1-2-3.
[137] L. sur la liberté de la presse du 29 juillet 1881, *JORF* 30 juillet 1881, p. 4201.
[138] L. n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *JORF* n° 0143, 22 juin 2004, p. 11168.

s'attachera principalement aux atteintes aux personnes et de manière que subsidiaire aux atteintes aux biens révélées par les sites de réseaux sociaux.

33. Droit pénal et droit administratif. Enfin, si le droit pénal, entendu comme « *l'ensemble des règles juridiques qui organisent la réaction de l'État vis-à-vis des infractions et des délinquants* »[139], constitue l'angle d'attaque principal de l'étude, il ne saurait en constituer l'unique. Le présent développement amène en effet à dépasser les clivages juridiques traditionnels et à incorporer à l'analyse les outils proposés par le droit administratif. Madame Coralie Courtaigne-Deslandes observe à ce propos que « *le droit pénal au sens strict n'est en effet pas le seul droit sanctionnateur à avoir une dimension d'intérêt général : le droit administratif dispose lui aussi d'un volet répressif exprimant le pouvoir de contrainte de l'État. Fondamentalement, le droit administratif et le droit pénal se rattachent à la même branche du droit, le droit public* »[140]. Œuvrant dans une même direction, le droit pénal et le droit administratif veillent par des moyens distincts à la préservation de l'ordre public. Ces deux droits sont appelés à coexister dans les nouveaux mécanismes de réponse aux infractions constatées sur les réseaux sociaux en ligne et plus particulièrement dans les régimes de responsabilité applicables aux acteurs de ces sites. La répression pénale s'envisagera alors conjointement avec la régulation administrative au travers de l'analyse de la pertinence des régimes de responsabilité applicables aux acteurs des réseaux sociaux en ligne.

34. Approche juridique. Plus généralement, l'étude sous l'angle juridique des sites de réseaux sociaux peut être amorcée selon différentes approches. Ainsi, la doctrine juridique anglo-saxonne appréhende les réseaux sociaux en ligne sous l'angle d'une problématique juridique spécifique qui implique la reconnaissance d'un « *Droit des réseaux sociaux en ligne* »[141] et amène, au-delà de ces derniers, à s'interroger sur l'existence d'un droit global[142]. Cette approche consiste à envisager l'état du droit à partir d'une situation concrète plutôt que

---

[139] R. MERLE et A. VITU, *Traité de droit criminel. Problèmes généraux de la science criminelle, droit pénal général*, éd. Cujas, 4ème éd. 1981, Tome 1, p. 201, n° 140.

[140] Observations partagées et développées par Madame Coralie Courtaigne-Deslandes *in* : *L'adéquation du droit pénal à la protection de l'environnement*, *op. cit.*, p. 28, n° 40.

[141] V. par exemple : D. STEWART, *Social media and the law*, Routledge, Abingdon, 2013.

[142] V. les nombreux ouvrages sur cette thématique, en particulier ceux du Professeur Benoît Frydman : B. FRYDMAN, *Petit manuel pratique de droit global*, Bruxelles, Académie royale de Bruxelles, 2014 ; B. FRYDMAN et J.-Y. CHEROT (dir.), La science du droit dans la globalisation, Bruxelles, Bruylant, 2012 ; B. FRYDMAN, et G. LEWKOWICZ, *Le droit global selon l'Ecole de Bruxelles, Bruxelles, Académie royale de Belgique, à paraître en 2017* ; B. FRYDMAN, et G. LEWKOWICZ (dir.), *Les théories du droit global*, Paris, Presses de Sciences Po, 2017 ; B. FRYDMAN et C. BRICTEUX (dir.), *Les défis du droit global*, bruylant, 2017 ; B. FRYDMAN, « A Pragmatic Approach to Global Law », in H. MUIR WATT and D. ARROYO, *Global Governance Implication of Private International Law*, Oxford University Press, 2015, p. 181 ; K. BENYEKHLEF (dir.), Vers un droit global ?, Montréal, Éditions Thémis, 2016.

d'un système de règles allant non pas de la règle aux faits, mais des circonstances d'une situation problématique vers les solutions juridiques envisageables. Si une telle méthode peut apparaître avantageuse quant à la flexibilité d'analyse qu'elle suggère, elle peut également être critiquée par le caractère extrêmement hétéroclite des problématiques juridiques qu'elle mobilise mais surtout par sa remise en cause des catégories juridiques préexistantes. En effet, si les réseaux sociaux ne forment pas un nouveau droit spécifique, ils constituent cependant assurément un nouvel espace juridique soumis au droit préexistant[143]. Dans ce cas, la présente étude ne consiste pas à mettre en évidence une problématique juridique spécifique aux sites de réseaux sociaux justifiant la construction d'un « *Droit des réseaux sociaux en ligne* » mais davantage à s'interroger sur l'adaptation du droit existant à cette nouvelle catégorie d'acteurs spécifique d'internet. Plus précisément, il sera question d'analyser l'adaptation du droit pénal à l'environnement des réseaux sociaux en ligne qui comprend à la fois l'activité de leurs utilisateurs et de leurs opérateurs, mais également les spécificités techniques et structurelles propres à ces nouveaux moyens de communication. La notion d'adaptation comprend en l'espèce différents niveaux de lecture. L'adaptation peut se comprendre en premier lieu comme le constat selon lequel le droit pénal se trouve parfaitement adapté aux sites de réseaux sociaux. Le droit pénal se montre alors adéquat au nouvel environnement numérique. L'adaptation peut se comprendre ensuite comme un mouvement, celui du droit pénal qui s'est adapté à ces nouveaux outils numériques. Enfin, le mot adaptation peut s'entendre comme un besoin d'évolution de la législation pénale actuelle. Ainsi, les règles de droit ne peuvent être posées et dégagées qu'en tenant compte des faits, des comportements sociaux, des possibilités techniques et des conséquences de leur utilisation, « *le droit est une science dont le fondement est puisé dans la réalité* »[144]. En revanche, l'adaptation du droit à des nouveaux phénomènes sociaux ne doit pas être pour autant automatique. Christian Atias observait ainsi que « *ce n'est pas parce qu'une nouvelle possibilité technique est mise au point que le recours cette possibilité doit être entériné, voire favorisé par le droit* »[145]. Le fait ne dicte pas le droit, bien au contraire, le droit doit guider le fait vers des fins choisies et conformément aux principes qui le gouvernent. Les nouveaux comportements permis par les sites de réseaux sociaux doivent dans ce cas être passés au crible des instruments du droit pénal et plus précisément de

[143] V. NDIOR, « Le réseau social : essai d'identification et de qualification », *in Droit et réseaux sociaux*, (dir. V. NDIOR), éd. Lextenso, coll. LEJEP, oct. 2015, p. 11.
[144] A.-J. ARNAUD, *Les juristes face à la société du XIXème siècle à nos jours*, PUF, 1975, p. 64-65.
[145] C. ATIAS, *Devenir juriste. Le sens du droit.* LexisNexis, Carré Droit, 2011, pp. 93-94. *Adde* : C. ATTIAS, D. LINOTTE, « Le mythe de l'adaptation du droit au fait », *D.*, 1977, p. 251.

ses principes fondamentaux et des valeurs qu'il protège. Le droit pénal dispose alors d'un pouvoir d'influence sur l'environnement numérique.

35. Plan. L'adaptation du droit pénal aux réseaux sociaux en ligne implique dans un premier temps l'étude de l'adaptation des incriminations aux comportements rencontrés sur ces sites. Il s'agit dans cette hypothèse de déterminer la capacité des incriminations à saisir les comportements cyberdélinquants, parfois d'un nouveau genre, rencontrés sur les sites de réseaux sociaux amenant le législateur à proposer, dans une logique de modernisation ou d'adaptation, des améliorations législatives. Ce constat polarisant d'un côté la technologie soumise à une évolution constante et rapide et d'un autre un droit suiveur empreint de rigidité et de lenteur doit être cependant relativisé dans le sens où la réforme n'est pas gage de qualité[146]. Partant du principe que seule l'identification de véritables carences structurelles du droit pénal spécial[147] justifie l'adoption de nouvelles incriminations, il convient alors de rechercher si les incriminations préexistantes, interprétées strictement, peuvent suffire à encadrer et réprimer les comportements cyberdélinquants et si l'adoption de nouvelles incriminations s'avère justifiée au regard des principes fondamentaux du droit pénal. Sur ce point, l'adaptation des incriminations traduit dans certaines hypothèses l'évolution de valeurs sociales protégées (**Partie 1**).

36. L'adaptation du droit pénal aux réseaux sociaux en ligne nécessite dans un second temps de s'attacher à l'adaptation de la répression aux réseaux sociaux en ligne. Pour ce faire, il revient d'identifier les différents régimes de responsabilité pénale applicables aux acteurs des réseaux sociaux en ligne à savoir, les utilisateurs et les opérateurs, et de s'interroger sur leur capacité à sanctionner justement et efficacement les comportements de ces derniers. Toutefois, l'environnement des réseaux sociaux en ligne est de nature à remettre en cause l'efficacité des régimes de responsabilité applicables en la matière et plus encore, la mécanique répressive dans son entier. Le droit pénal se doit alors d'évoluer en admettant notamment un système de régulation des contenus faisant intervenir l'autorité administrative, gardienne elle aussi de l'ordre public. L'équilibre de ce nouveau cadre doit alors être trouvé,

---

[146] T. AZZI, « La responsabilité des nouvelles plates-formes : éditeurs, hébergeurs ou autre voie ? », *in* Contrefaçon sur Internet. Les enjeux du droit d'auteur sur le WEB 2.0, LexisNexis, coll. IRPI, 2009, n° 33, p. 75.

[147] La définition du droit pénal spécial peut s'envisager ainsi selon le professeur André Vitu : « *Le droit pénal spécial envisage les infractions séparément. Pour chacune, il énumère et précise ses éléments constitutifs, c'est-à-dire les pièces dont l'agencement, plus ou moins complexe, traduit le comportement délictueux ; il indique les pénalités applicables aux auteurs de chacune de ces infractions et mentionne, s'il y a lieu, les particularités procédurales qu'elle comporte. D'une façon plus brève, on dira que le droit pénal spécial consiste en l'étude analytique des diverses infractions, envisagées une à une dans leurs éléments particuliers et dans les modalités de leur répression* ». A. VITU, *Traité de droit criminel, droit pénal spécial* (Tome 3), Éd. CUJAS, 1982, p. 9.

ce dernier ne pouvant s'exercer au détriment de certains droits et principes fondamentaux et sans une collaboration avec l'autorité judiciaire (**Partie 2**).

Partie I – L'adaptation des incriminations aux réseaux sociaux en ligne

Partie II – L'adaptation de la répression aux réseaux sociaux en ligne

Partie 1 – L’adaptation des incriminations aux réseaux sociaux en ligne

37. Avec le développement des interractions numériques permises par les réseaux sociaux en ligne, beaucoup de comportements délictueux ont trouvé la possibilité de s’étendre au domaine numérique. Ainsi, nombre d’infractions renvoyant à une délinquance traditionnelle se retrouvent désormais dans le contexte des réseaux sociaux en ligne. Cependant, dans la majorité des cas l’utilisation d’un réseau social comme moyen de commettre une infraction ne pose aucune difficulté concernant l’appréhension pénale de ce comportement. Les incriminations du droit pénal commun démontrent, en de nombreux points, une réelle adaptation aux sites de réseaux sociaux nécessitant tout au plus certains ajouts ponctuels. Ceci étant, les pratiques engendrées par ces nouveaux moyens de communication créent également des situations non encore envisagées par la loi et qui ne peuvent entrer sous des qualifications préexistantes en raison du principe d’interprétation stricte de la loi pénale. Les comportements générés par les sites de réseaux sociaux révèlent alors, dans certains cas, de véritables carences des incriminations classiques se manifestant par leur incapacité à appréhender des nouvelles formes de comportements portant pourtant atteinte à des valeurs sociales protégées.

Si les incriminations préexistantes démontrent globalement leur adéquation aux comportements rencontrés sur les réseaux sociaux (**Titre 1**), certains comportements favorisés par ces sites ont justifié un mouvement d’adaptation du droit pénal se manifestant par l’adoption de nouvelles incriminations (**Titre 2**).

Titre 1 – L’adéquation des incriminations préexistantes

38. Les réseaux sociaux en ligne manifestent une transposition dans l’environnement numérique des rapports sociaux et nécessairement, de certains actes délinquants. Cependant, dans la majorité des hypothèses, les incriminations préexistantes à l’apparition et au développement des sites de réseaux sociaux se montrent d’ores et déjà adaptées aux comportements spécifiques pouvant s’y rencontrer. Plus encore, la communication massive sur les sites de réseaux sociaux en ligne a favorisé un accroissement de certains comportements infractionnels en particulier les infractions de presse qui démontrent un réel pouvoir d’adaptation de la loi sur la liberté de la presse du 29 juillet 1881. Certaines réformes entreprises en matière pénale se sont révélées alors injustifiées, pire encore, dangereuses au regard de certains principes fondamentaux du droit pénal.

Il sera ainsi confronté dans un premier temps les incriminations de presse à la communication massive permise par les sites de réseaux sociaux (**Chapitre 1**), puis dans un second temps, les incriminations du droit pénal commun au regard des formes particulières de délinquance rencontrées sur les sites de réseaux sociaux (**Chapitre 2**).

Chapitre 1 – Les incriminations de presse confrontées aux réseaux sociaux

39. Une loi centenaire face à un changement de paradigme. L'apparition d'internet a engagé un changement de paradigme dans l'expression publique en offrant un nouveau potentiel technique de diffusion des pensées qui n'avait jusque-là trouvé aucune mesure. Les sites de réseaux sociaux ont su exploiter ce potentiel technique pour offrir à l'ensemble de la communauté des internautes des outils de communication encore inégalés. Désormais tout un chacun peut s'exprimer sans le filtrage ou la sélection qui sont de rigueur dans l'accès aux modes traditionnels d'expression publique, comme l'édition, la télévision, la radio. Les réseaux sociaux en ligne donnent ainsi toute son ampleur au principe de la liberté d'expression puisqu'ils rendent ce principe directement applicable à tout citoyen disposant d'un accès à internet[148]. La liberté d'expression, affirmée par des instruments constitutionnels, européens et internationaux[149], est régie en droit interne par la loi du 29 juillet 1881 sur la liberté de la presse[150] venant poser les limites admises dans notre société à la liberté d'expression. Or, le droit de la presse démontre une large adaptation aux changements des modes de communication issus des réseaux sociaux en ligne.

Cette adaptation se retrouve à deux niveaux, d'une part en raison du caractère majoritairement public des propos diffusés sur ces nouveaux moyens de communication (**Section 1**), d'autre part par la capacité de ses incriminations à appréhender les nouvelles formes d'expression issues des sites de réseaux sociaux (**Section 2**).

[148] A. LEPAGE, « Internet au regard de la loi du 29 juillet 1881 sur la presse : un mode de communication comme un autre ? », *in*, *L'opinion numérique : Internet un nouvel esprit public*, Dalloz, 2006, pp. 141 et 142.
[149] L'ensemble des instruments de protection des droits de l'homme prévoient une protection de la liberté d'expression des individus, tel est le cas de la Déclaration des Droits de l'Homme et du Citoyen de 1789 (art. 11), de la Déclaration Universelle des Droits de l'Homme de 1948 (art. 19), de la Convention EDH (art. 10).
[150] L. sur la liberté de la presse du 29 juillet 1881, *JORF* 30 juillet 1881, p. 4201.

Section 1 : Le caractère majoritairement public des propos diffusés sur les sites de réseaux sociaux

40. La publicité, condition préalable à l'ensemble des infractions de presse. L'adaptation des incriminations issues de la loi sur la liberté de la presse aux réseaux sociaux dépend en premier lieu de la publicité des propos tenus sur ces plateformes. Le critère de publicité des propos prévu à l'article 23 de cette loi constitue une condition préalable devant être démontrée pour chaque infraction commise par voie de presse[151]. En l'absence de ce critère, certains délits de presse deviennent de simples contraventions[152], d'autres ne sont simplement pas constitués et ne peuvent en conséquence faire l'objet de poursuites[153]. En l'occurrence la majorité des propos tenus sur les réseaux sociaux en ligne revêtent un caractère public induisant une très large application de la loi sur la liberté de la presse aux réseaux sociaux.

L'application étendue de la loi sur la liberté de la presse aux réseaux sociaux implique en premier lieu de démontrer, au regard de son article 23, que ces derniers constituent un support de publication par voie de presse (**§1**) puis en second lieu, que les propos qui y sont diffusés disposent d'une large audience permettant d'en déduire dans leur majorité un caractère public (**§2**).

§1. Les réseaux sociaux, un support de publication par voie de presse

41. Le support de presse originel : la presse écrite. Dans sa conception originelle le droit de la presse est l'instrument de l'imprimerie[154]. L'application du régime de la loi sur la liberté de la presse présupposait un objet imprimé en tant que destinataire ou accessoire de la réglementation[155]. Ainsi, le droit de la presse est étroitement lié au support papier à l'exemple

---

[151] C. BIGOT, *Pratique du droit de la presse*, Éd. Victoires, PUF, 2013, p. 83.
[152] Par exemple, les injures ou diffamations privées sanctionnées aux articles R. 621-1 et 621-2 du Code pénal.
[153] Par exemple, le délit de négationnisme prévu à l'article 24 bis, les délits de provocation aux infractions prévus aux articles 23 et 24 de la loi sur la liberté de la presse.
[154] « *On entend par le mot presse la machine au moyen de laquelle on imprime sur des feuilles de papier ou de quelque autre matière, soit les divers caractères qui forment les mots, soit les desseins qui forment les gravures et les lithographies. La presse tient donc essentiellement à l'art de l'imprimerie ; elle en constitue le principal moyen d'exécution* ». G.-J. FAVARD De LANGLADE, *Répertoire de la nouvelle législation civile, commerciale et administrative*, Paris, 1824, t. IV, p. 461, *V° Presse*.
[155] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 51, n° 71.

des livres, journaux, périodiques et affiches[156]. L'objet de l'impression n'est cependant pas nécessairement un écrit, l'opinion pouvant se manifester également par l'image. « *Les dessins, les médailles, les emblèmes, frappent l'intelligence d'une manière plus vive et souvent plus impressive que les écrits* »[157]. Dès son origine, le support de publication par voie de presse dépassait le simple cadre des publications périodiques et des journaux. Le support était cependant nécessairement imprimé, autrement dit, matériel. Une première modification de l'article 23 de la loi sur la liberté de la presse est intervenue par la loi du 1er juillet 1972[158] qui est venue ajouter aux prévisions initiales de l'article 23 des « *dessins, gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués* ». Tout en venant ajouter certains supports de publication possibles[159], la loi du 1er juillet 1972 élargit considérablement le champ d'application de l'article 23 par une formulation générale : « *tout autre support de l'écrit, de la parole ou de l'image* ». Dès lors, les supports de publications ne sont plus définis de façon limitative mais de manière ouverte, de façon à y inclure n'importe quel support qui n'aurait pas été prévu par le législateur. Le support de publication matériel a toutefois rapidement trouvé ses limites avec le développement des nouveaux moyens de communication : la radio, la télévision et enfin internet.

42. L'extension du support de publication à l'audiovisuel. L'extension de l'article 23 de la loi sur la liberté de la presse à l'audiovisuel est d'abord issue de l'interprétation extensive de ce texte par le juge dans le but constant d'appliquer le droit de la presse aux nouveaux supports de communication alors même que ceux-ci n'auraient pas été encore prévus par la loi du 29 juillet 1881. Furent ainsi incriminés comme constituant des actes de publication les photographies[160], les films cinématographiques[161], la radiophonie[162], les disques phonographiques[163], la télévision[164]. Par la suite, la loi du 29 juillet 1982[165] est venue définir pour la première fois la communication audiovisuelle comme : « *la mise à la disposition du public, par voie hertzienne ou par câble, de sons, d'images, de documents, de*

---

[156] Selon André VITU, la presse désigne « *l'ensemble des dispositions juridiques qui intéressent l'impression et la diffusion des livres, des journaux et périodiques, ainsi que des affiches* ». R. MERLE et A. VITU, *Traité de droit criminel, Droit pénal spécial*, Cujas, 1982, p. 1204, n° 1527.
[157] Dalloz, *Répertoire*, Paris, 1856, t. XXXVI, p. 490, n° 408.
[158] L. n° 72-546 du 1er juillet 1972 relative à la lutte contre le racisme, *JORF* n° 0154, 2 juillet 1972, p. 6803.
[159] En l'occurrence : « *dessins, gravures, peintures, emblèmes, images* ».
[160] TC de la Seine, 26 décembre 1895, *D.* 1896, II, 230.
[161] Dijon, 8 janvier 1936, *RSC* 1936, 222, note MAGNOL.
[162] Paris, 6 mars 1933 ; Tr. corr. de Bourges, 19 juillet 1934, *D.* 34, II, 121.
[163] Crim., 17 janvier 1971 : *Bull. crim.* 1971, n° 14.
[164] TC de Bourges, 19 juillet 1934, *D.* 1934, p. 121.
[165] L. n° 82-652, 29 juillet 1982 sur la communication audiovisuelle, *JORF* 30 juillet 1982 p. 2431.

données ou de messages de toute nature »[166]. La loi n° 86-1067 du 30 septembre 1986 dite loi Léotard[167] est cependant venue abroger ces dispositions pour proposer une nouvelle définition de la communication audiovisuelle selon laquelle : « *On entend par communication audiovisuelle toute mise à disposition du public ou de catégories de public, par un procédé de télécommunication, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée* »[168]. La loi n° 85-1317 du 13 décembre 1985[169] parachève cette évolution en ajoutant comme support de publication à l'article 23 de la loi sur la liberté de la presse : « *tout moyen de communication audiovisuelle* ». Ces nouveaux moyens d'expression à distance représentés principalement par la télévision et la radio se trouvent ainsi soumis au régime de la loi du 29 juillet 1881 et peuvent devenir vecteur d'infractions de presse.

Cette évolution législative a cependant trouvé ses limites avec l'apparition du support internet comme moyen de communication. Le champ d'application de l'article 23 s'est alors rapidement étendu à la communication au public en ligne (A) permettant l'application du droit de la presse aux propos émis sur les sites de réseaux sociaux (B).

A. L'extension des supports de publication à la communication au public en ligne

43. Anticipation de l'évolution législative par la jurisprudence. À l'instar du support de communication audiovisuelle, la jurisprudence est venue anticiper l'extension du champ d'application de la loi sur la liberté de la presse au support internet. La méthode utilisée par la jurisprudence est toutefois différente. La communication en ligne a été assimilée à d'autres supports préexistants dans la loi sur la liberté presse et notamment à celui de la communication audiovisuelle. Selon ce raisonnement, « *l'Internet est un procédé de télécommunication* »[170] et partant, une publication sur un site internet peut parfaitement entrer dans les prévisions de l'article 23 de la loi sur la liberté de la presse. Un site web au contenu évolutif fut par exemple assimilé à la presse périodique en raison de sa « *mise à jour régulière* »[171] remplissant ainsi le critère posé par la loi du 1er aout 1986[172]. Les critères alors

[166] Art. 1, loi n° 82-652 du 29 juillet 1982.
[167] L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, *JORF* 1er octobre 1986 p. 11755.
[168] Art. 2, loi n° 86-1067 du 30 septembre 1986, version initiale.
[169] L. n° 85-1317, 13 décembre 1985 modifiant la loi 82-652 du 29 juillet 1982 et portant dispositions diverses relatives à la communication audiovisuelle, *JORF* n° 0290, 14 décembre 1985 p. 14535.
[170] TI de Puteaux, 28 septembre 1999, AXA Conseil IARD et AXA Conseil Vie c/ MM. C. M. et C. Sapet, Société Infonie, *Légipresse* n° 168, janvier-février 2000, p. 19.
[171] TI de Paris (11ème arrondissement) 36 août 1999. Société Group Tests c/ Groupe Worldnet, *Légipresse* n° 168, janvier-février 2000 p. 22.

retenus pour déterminer une publication par voie de presse sont : « *la diffusion par écrit, la mise à disposition du public et la périodicité de cette diffusion* »[173]. En conséquence, antérieurement à la LCEN du 21 juin 2004 la jurisprudence avait déjà tendance à assimiler l'internet au régime de la communication audiovisuelle et à justifier l'application du régime de « *la presse écrite* » en raison des mises à jour régulières des sites. Cette solution a pour mérite de ne pas laisser dépourvu d'encadrement juridique les propos émis sur internet. De cette façon le juge maintient un standard unique d'appréciation des limites de la liberté d'expression et ne laisse pas internet soumis à une jurisprudence instable de tribunaux de première instance[174]. Ainsi, nombreuses sont les décisions ayant appliqué la loi sur la liberté de la presse au support internet avant la réforme du 21 juin 2004[175]. Cette interprétation extensive de la communication audiovisuelle fut validée par deux arrêts de la chambre criminelle du 6 mai 2003[176] et du 10 mai 2005[177].

44. Assimilation légale de l'internet au régime de l'audiovisuel. Suivant cette dynamique jurisprudentielle, le législateur est intervenu par la loi n° 2000-719 du 1er août 2000[178] en assimilant le réseau internet à un moyen de communication audiovisuelle au sens de l'article 2 de la loi du 30 septembre 1986 relative à la liberté de communication. Cette loi entérine l'appartenance d'internet aux supports de publication prévus à l'article 23 de la loi sur la liberté de la presse. Cette assimilation n'offre toutefois pas de régime particulier à la communication en ligne malgré les spécificités techniques qui la distinguent de la communication audiovisuelle.

45. Spécificité de la communication au public en ligne. Il est nécessaire de distinguer le public passif de la communication audiovisuelle soumis à une programmation, du public actif de la communication en ligne. Cette dernière se manifeste essentiellement par la multitude de ses intervenants et également par le rôle actif du public. De ce fait, les consommateurs de

---

[172] L'article 1 de la Loi n° 86-897 du 1 août 1986 portant réforme du régime juridique de la presse précise qu'il faut entendre par publication de presse : « *tout service utilisant un mode écrit de diffusion de la pensée mis à la disposition du public en général ou de catégorie de public et paraissant à intervalles réguliers* ».

[173] TI de Paris (11e arrondissement) 36 août 1999. Société Group Tests c/ Groupe Worldnet, Legipresse n° 168, janvier-février 2000 p. 22.

[174] En ce sens : C. BIGOT, « Application de la loi de 1881 à l'internet », *Légipresse* n° 168, janvier-février 2000, p. 23, n° 3.

[175] Par exemple : Paris, ch. corr. 11 section B, 14 février 2002, n° 2002-181380 – TGI Paris, réf., 16 avril 1996 : *D.* 1997, somm. p. 72, obs. J.-Y. DUPEUX – TGI Paris, 1ère ch., 1ère sect., 10 juillet 1997 : *Gaz. Pal.* 18 janvier 1998, p. 42, note A. COUSIN.

[176] Crim., 6 mai 2003, n° 02-80.284 : *Bull. crim.* n° 94 ; *CCE* n° 9, Septembre 2003, comm. 89, A. LEPAGE ; *JCP* G n° 26, 25 juin 2003, 2175 ; *D.* 2003, p. 2192, note E. DREYER.

[177] Crim., 10 mai 2005, n° 04-84.705 : *JCP* G n° 25, 22 juin 2005, IV 243 ; *D.* 2005 p. 2986, pan. G. ROUJOU De BOUBÉE, T. GARE, C. MASCALA.

[178] L. n° 2000-719 du 1er août 2000 modifiant la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication, *JORF* n° 177, 2 août 2000, p. 11903.

contenus sur internet sont bien plus impliqués que les consommateurs de la presse et des médias traditionnels. « *La communication en ligne est spécifique en raison de l'interactivité du récepteur du message. L'internaute est invité à collaborer, à communiquer à son tour. La technique du Web 2.0 ouvre l'ère d'une communication nouvelle. (…) Finalement, la spécificité des communications en ligne réside dans la multiplication des intervenants et dans le brouillage des rôles entre l'émetteur et le récepteur* »[179]. Plus encore, au-delà d'être un récepteur actif, l'internaute devient un potentiel émetteur d'informations contribuant encore davantage à obscurcir la distinction opérée dans le régime de la communication audiovisuelle.

46. Notion de communication au public par voie électronique. Cette absence de régime spécifique est corrigée par la loi n° 2004-575 pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004[180] qui remplace dans l'article 23 de la loi sur la liberté de la presse la mention « *tout moyen de communication audiovisuelle* » par celle de « *tout moyen de communication au public par voie électronique* ». Cette nouvelle notion regroupe en fait deux sous-ensembles bien distincts. D'une part la communication audiovisuelle (principalement radio et télévision) qui se manifeste par « *l'existence d'un public simultané en direction duquel les programmes sont émis* »[181]. D'autre part, la communication au public en ligne (ou la communication par internet) qui vise quant à elle « *un échange réciproque d'informations entre l'émetteur et le récepteur* »[182].

47. Adoption d'un régime spécifique pour la communication au public en ligne. La rédaction actuelle de l'article 23 de la loi sur la liberté de la presse inclut ainsi dans les supports de publication la communication audiovisuelle et la communication au public en ligne, de manière à envisager l'ensemble des moyens d'expression. Ces deux supports possèdent toutefois deux régimes distincts et spécifiques à chacun d'eux issus de la loi du 30 septembre 1986[183], modifiée à plusieurs reprises[184] et de la LCEN du 21 juin 2004[185] largement modifiée depuis également[186].

---

[179] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 1124, § 1901.
[180] L. n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), *JORF* n° 0143, 22 juin 2004, p. 11168.
[181] M. MORITZ, « Entre idéal de neutralité technologique et réalité d'une mutation sémantique : analyse des catégories juridiques du droit français de la communication », *Revue internationale de droit des données et du numérique*, mars 2017, v. 1, p. 31.
<http://ojs.imodev.org/index.php/RIDDN/article/view/148/212> (dernière consultation le 9 octobre 2019).
[182] *Ibid.*
[183] L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, *JORF*, 1er octobre 1986, p. 11755.
[184] L. n° 94-88 du 1 février 1994 *JORF* 2 février 1994 ; L. n° 89-25 du 17 janvier 1989 *JORF* 18 janvier 1989 ; L. n° 90-1170 du 29 décembre 1990 *JORF* 30 décembre 1990 ; L. n° 92-1336 du 16 décembre 1992 *JORF* 23

B. L'application du droit de la presse aux propos émis sur les sites de réseaux sociaux

48. Les sites de réseaux sociaux, un support de publication par voie de presse. Depuis l'entrée en vigueur de la LCEN, la communication au public en ligne est entrée officiellement dans les prévisions de l'article 23 de la loi sur la liberté de la presse. Cette dernière constitue alors un support de publication par voie de presse. Or, internet a ouvert un potentiel technique sans commune mesure en matière de communication devenant le principal moyen d'exercice par les individus de leur droit à la liberté d'expression et d'information[187]. Les sites de réseaux sociaux ont su exploiter ce potentiel en l'ouvrant à l'ensemble de la communauté des internautes. Leurs moyens de communication permettent à l'internaute d'émettre et de partager quotidiennement de l'information et de devenir le cas échéant, lui-même écrivain, journaliste, artiste ou éditeur[188]. Ce faisant, l'expression au public ne relève plus uniquement des supports de presse traditionnels à savoir l'écrit et l'audiovisuel réservé majoritairement aux professionnels de la communication[189]. Désormais, tout individu dispose de la capacité technique de s'exprimer à une large audience.

49. Les réseaux sociaux, un support d'infractions commises par voie de presse. En conséquence, les réseaux sociaux en ligne sont devenus un support de publication par voie de presse qui soumet leurs utilisateurs aux incriminations issues de la loi du 29 juillet 1881. Au-delà de constituer un support d'expression entrant dans les prévisions de la loi sur la liberté de la presse, les réseaux sociaux en ligne en raison de leur utilisation massive, sont source d'un important contentieux en la matière. Certaines affaires ont ainsi mis en avant l'utilisation d'un site de réseau social comme support de commission d'infractions par voie de presse. Par exemple, l'humoriste Dieudonné fut condamné à deux ans d'emprisonnement avec

décembre 1992 en vigueur le 1er mars 1994 ; L. n° 2000-719 du 1 août 2000 *JORF* 2 août 2000 ; L. n° 2004-669 du 9 juillet 2004, *JORF* 10 juillet 2004 en vigueur le 1er août 2004 ; L. n° 2006-64 du 23 janvier 2006 *JORF* 24 janvier 2006 ; L. n° 2007-309 du 5 mars 2007 *JORF* 7 mars 2007 ; L. n° 2008-776 du 4 août 2008 *JORF* n° 0181 du 5 août 2008 ; L. n° 2009-258 du 5 mars 2009 ; L. n° 2009-526 du 12 mai 2009 ; L. n° 2009-879 du 21 juillet 2009 ; L. n° 2010-121 du 8 février 2010 ; L. n° 2011-525 du 17 mai 2011 ; L. n° 2011-901 du 28 juillet 2011 ; L. n° 2012-158 du 1er février 2012 ; L. n° 2013-1028 du 15 novembre 2013 ; L. n° 2015-1267 du 14 octobre 2015 ; L. n° 2016-987 du 21 juillet 2016 ; L. L. n° 2016-1321 du 7 octobre 2016 ; L. n° 2016-1524 du 14 novembre 2016 ; L. n° 2016-1888 du 28 décembre 2016 ; L. n°2017-55 du 20 janvier 2017 ; L. n° 2017-86 du 27 janvier 2017 ; L. n° 2017-256 du 28 février 2017.

[185] L. n° 2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique (LCEN), *JORF* n° 0143, 22 juin 2004, p. 11168.

[186] L. n° 2007-297 du 5 mars 2007, *JORF* 7 mars 2007 ; L. n° 2008-3 du 3 janvier 2008 ; L. n° 2014-344 du 17 mars 2014 ; L. n° 2015-990 du 6 août 2015 ; Ordonnance n° 2016-301 du 14 mars 2016 ; L. n° 2016-1888 du 28 décembre 2016.

[187] Cons. const., 10 juin 2009, DC n° 2009-580 – CEDH, *Ahmet Yildirim c. Turquie*, 18 décembre 2012, n° 3111/10, §54.

[188] P. ACHILLEAS, « Internet et libertés », *J.-Cl.* Libertés, 5 décembre 2007, fasc. n° 820, n° 27.

[189] À l'exception notamment de l'affichage qui est au sens de l'article 23 un moyen de communication par voie de presse.

sursis et à 1000 euros d'amende, pour apologie du terrorisme commis au moyen d'un service de communication au public en ligne pour avoir publié sur sa page officielle Facebook le message « *Sachez que ce soir, je me sens Charlie Coulibaly* » le lendemain des attentats de Charlie-hebdo[190]. Dans une autre affaire, un élu du front national s'est vu condamner pour provocation à la haine ou à la violence, à l'égard de personnes à raison d'une religion déterminée[191] pour avoir publié sur son mur Facebook des propos virulents à l'égard de la communauté musulmane de la ville de Nîmes[192]. Il est ainsi considéré de jurisprudence constante que « *l'appréhension des contenus illicites ne pose pas de difficulté particulière concernant les réseaux sociaux* »[193]. Le régime spécial du droit de la presse trouve parfaitement vocation à s'appliquer au support de publication des réseaux sociaux étendant l'application du régime de la loi sur la liberté de la presse à une multitude d'acteurs dont la plupart sont largement profanes en la matière. Le contentieux de la presse se trouve en conséquence en nette augmentation en raison de l'accroissement du nombre de communications potentiellement soumises au droit de la presse[194]. Cet élargissement du champ d'application de la loi sur la liberté de la presse est renforcé en outre par le caractère majoritairement public des propos émis sur les réseaux sociaux en ligne.

§2. La large audience des propos diffusés sur les sites de réseaux sociaux

50. Le droit de la presse ou droit de la publication. La notion de presse utilisée dans le langage courant[195] est en réalité bien éloignée de celle que recouvre le droit de la presse. Selon Monsieur Basile Ader, **«** *la loi du 29 juillet 1881 qui s'intitule elle-même loi sur la liberté de la presse, réglemente plus que la presse elle-même. Elle a, en fait, vocation à encadrer "le droit de la publication"* »[196]. Le Professeur Emmanuel Dérieux partage ce point de vue en considérant que « *plus que jamais s'impose […] la nécessité de recentrer [le droit*

[190] TGI Paris, 16ème ch. corr., 18 mars 2015, n° 2015-005323.
[191] L. sur la liberté de la presse du 29 juillet 1881, art. 24, al. 6.
[192] Crim., 17 mars 2015, n° 13-87.922 : *Bull. crim.* 2015, n° 57.
[193] F. PERBOST, A. EUVRETE, « Régulation des réseaux sociaux : où en est-on ? », *Revue de jurisprudence commerciale*, juillet/août 2016, n° 4, p. 418.
[194] V. *infra* n° 438.
[195] Dans le sens commun le mot presse est défini comme : « *une machine à imprimer* » ou « *l'ensemble des journaux et revues périodiques* ». Le mot presse dans le sens courant est ainsi directement lié à l'idée d'un support papier. Dictionnaire Larousse en ligne, *V°* Presse.
<www.larousse.fr/dictionnaires/francais/presse> (dernière consultation le 9 octobre 2019).
[196] B. ADER, « Évolution de la notion de publication : de la presse écrite à Internet », *Légipresse*, octobre 1999, n° 165, p. 123 et suiv.

de la communication] sur la notion fondamentale de "publication" »[197]. Le droit de la presse revêt donc un aspect bien plus large que ce qui pourrait être entendu dans le sens commun. Il est néanmoins indispensable de définir avec précision la notion de publicité d'un propos en tant que condition préalable à l'ensemble des délits définis dans la loi sur la liberté de la presse. Cette dernière est en l'occurrence principalement déterminée au regard du critère de la communauté d'intérêts qui se montre cependant insuffisant pour le support internet nécessitant également l'intervention du critère quantitatif du nombre de personnes visées par le propos. La publicité d'un propos est alors dépendante d'un critère à la fois qualitatif et quantitatif (A). Les spécificités techniques des sites de réseaux sociaux amènent toutefois à constater la difficile réunion de ces critères à leur échelle (B).

A. La publicité d'un propos dépendante d'un critère qualitatif et quantitatif

51. Construction jurisprudentielle et doctrinale. La notion de publicité des propos qui revêt une importance majeure au sein de la loi du 29 juillet 1881 n'est cependant pas suffisamment définie par la loi (1). La précision de cette notion est alors intervenue par le biais d'une construction jurisprudentielle et doctrinale de critères à la fois qualitatifs et quantitatifs démontrant l'insuffisance du seul critère de communauté d'intérêt sur le support internet (2).

1) L'absence de définition légale du critère de publicité d'un propos

52. Le flou législatif. La définition du critère de publicité apparaît dans un premier temps dans la loi du 30 septembre 1986 qui définit les communications au public par voie électronique comme « *toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée* »[198]. Par la suite, la loi pour la confiance en l'économie numérique (LCEN) est venue ajouter qu' *« on entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur* »[199]. Dans les deux cas, la notion de correspondance publique se

[197] E. DERIEUX, *Droit de la communication*, L.G.D.J., 4ème éd., 2003, avant-propos, XVII.
[198] L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), *JORF*, 1er octobre 1986 p. 11755, art 2, al. 2.
[199] LCEN, art. 1.

définit par opposition à la notion de correspondance privée, il faut donc recourir à une lecture *a contrario* de la notion de correspondance privée pour en déduire celle de correspondance publique. Ce raisonnement peut être éclairé par l'interprétation donnée par la circulaire du 17 février 1988[200] définissant la correspondance privée comme une communication « *destinée exclusivement à une ou plusieurs personnes physiques ou morales, déterminées et individualisées* ». En conséquence, toute communication destinée à une personne indéterminée ou non individualisée serait une communication publique. Cette solution qui a le mérite de poser un critère de distinction entre ce qui est public et ce qui est privé manque toutefois, en raison de son caractère trop général, de précision. C'est pourquoi la jurisprudence et la doctrine ont développé la notion de communauté d'intérêts pour pallier ce flou législatif.

2) La définition prétorienne et doctrinale des critères de publicité d'un propos

53. Le développement du critère de la communauté d'intérêts par la jurisprudence. L'article 23 de la loi sur la liberté de la presse pose l'exigence de la publicité du propos comme condition préalable nécessaire à toute infraction de presse mais sans la définir. Le critère de la publicité des propos s'est alors construit autour de la notion de communauté d'intérêts développée par la jurisprudence et appuyée par la doctrine. Depuis la fin des années 1980 le critère de la communauté d'intérêts est retenu de manière systématique par les juridictions pour déterminer si l'infraction commise a un caractère public[201]. Pour ce faire, la Cour de cassation pose des éléments d'interprétation sur la base de l'article 23 de la loi du 29 juillet 1881 en précisant qu'est « *public* » un message auquel peut accéder « *un public anonyme et imprévisible* »[202]. Le juge a par la suite affiné sa position en identifiant le critère de la communauté d'intérêts. Il est dans ce cas de principe qu'une imputation diffamatoire ou injurieuse ne revêt pas un caractère public lorsqu'elle concerne un cercle restreint de personnes liées entre elles par une communauté d'intérêts[203]. Les adhérents d'une association[204], les membres d'un syndicat[205], et les actionnaires d'une société[206] ont été jugés comme formant une communauté d'intérêts. À l'inverse, les conseillers municipaux ne

[200] Circulaire du 17 février 1988 prise en application de l'article 43 de la loi du 30 septembre 1986.
[201] C. BIGOT, *Pratique du droit de la presse*, Éd. Victoires, PUF, 2013, p. 83.
[202] Crim. 3 juillet 1980 : *Bull. Crim.* n° 560.
[203] Crim., 3 juin 1997 : *Bull. Crim.*, n° 218.
[204] Crim., 15 juillet 1981 : *Bull, crim.*, n° 232.
[205] Crim., 18 mai 1954 : *Bull, crim.*, n° 187 ; *D.* 1956.366, note LEMERCIER ; *JCP* 1954.II.8292, note CHAVANNE.
[206] Crim., 27 novembre 1920 : *Bull, crim.*, n° 461.

forment pas un groupement de personnes liées par une communauté d'intérêts[207], de même, les parents d'élèves d'une classe de l'école publique ne constituent pas une communauté d'intérêts[208]. Plus largement, une simple convergence de pensée politique ou idéologique ne peut caractériser un tel critère[209]. De manière générale, la communauté d'intérêts regroupe « *toutes les hypothèses où les propos tenus ou les écrits diffusés ne sortent pas du cadre étroit de la communauté à laquelle ils appartiennent, à la fois ceux qui en sont les auteurs et ceux auxquels ils sont destinés* »[210] de sorte que « *la distribution d'un écrit non confidentiel à divers destinataires qui ne constituent pas entre eux un groupement de personnes liées par une communauté d'intérêts caractérise la publicité prévue à l'article 23 de la loi du 29 juillet 1881* »[211].

54. La précision du critère de la communauté d'intérêts par la doctrine. Bien que largement utilisée par la jurisprudence la notion de communauté d'intérêts « *présente l'inconvénient d'être un peu fuyante* »[212]. Cela s'explique par le fait que ce critère est indubitablement lié à des éléments de pure espèce et qu'à chaque cas correspond une solution spécifique. La doctrine a cependant travaillé à théoriser cette notion. Selon le Professeur Yves Mayaud, la communauté d'intérêts s'observe lorsque « *des personnes forment une entité suffisamment fermée pour ne pas être perçues comme regroupant des tiers par rapport à l'auteur des propos* »[213]. Il s'agit d'un critère qualitatif qui s'entend par l'existence d'un lien unissant les différentes personnes visées par le propos. Ces liens doivent être « *réels, par référence à des intérêts véritablement partagés, situant chacun de ses membres dans une situation de proximité par rapport aux autres* »[214]. Plus encore, une communauté d'intérêts supposerait « *la démonstration d'un ciment juridique ou contractuel, soit que les membres sont liés contractuellement entre eux, soit qu'ils sont membres d'un groupement institué par un texte légal ou réglementaire, ou par un instrument juridique s'apparentant à un contrat.*

[207] Crim. , 16 mars 2010, n° 09-84.160 – Crim. 29 mars 1994, n° 92-80.728 – Crim., 3 juin 1997, n° 96-81.706.
[208] Crim., 3 juillet 2003, n° 00-15.468.
[209] Crim., 28 avril 2009, n° 08-85.249 : *CCE* 2009 comm. 102, obs. A. LEPAGE ; *Dr. pén.* n° 9, Septembre 2009, comm. 105, M. VERON.
[210] Y. MAYAUD, « De la mise en cause diffamatoire d'une gestion municipale : l'enjeu de publicité », *RSC* 1998, p. 104 ; Crim., 3 juin 1997, *Bull. Crim.*, n° 218.
[211] Civ. 2ème, 23 septembre 1999, n° 97-18.784 : *Bull. II* n° 140 – Crim. 29 janvier 1998, n° 95-82.09.
[212] A. LEPAGE, « Précisions sur la communauté d'intérêts », Obs. sous Crim. 28 avril 2009, *CCE* 2009, comm. 102.
[213] Y. MAYAUD, « De la mise en cause diffamatoire d'une gestion municipale : l'enjeu de la publicité », *op. cit.*
[214] *Ibid.*

[…] *Ainsi, distinction subtile, le groupement de personnes liées par une communauté d'intérêts, n'est pas une communauté de personnes partageant des intérêts communs* »[215].

55. Le nombre de personnes visées par les propos, critère quantitatif. Outre la qualité du lien unissant les personnes destinataires d'un propos, certains auteurs ont également conclu que la publicité est fonction du nombre de personnes visées par ce dernier[216]. De manière logique, le critère qualitatif de la communauté d'intérêts décroît proportionnellement à l'augmentation du nombre de personnes atteintes par le propos. Autrement dit, la subjectivité du critère qualitatif est indubitablement liée à l'objectivité du critère quantitatif. La détermination du caractère public des propos résulte alors de la combinaison de ces différents éléments. Il est en conséquence nécessaire de s'attacher non seulement à la qualité du lien unissant les différentes personnes mais également au nombre de destinataires du message et aux conditions d'accès au propos litigieux. Si le faible nombre d'individus visés par les propos, constitue l'indice certain d'un lien objectif les unissant, il peut néanmoins exister une communauté d'intérêts entre un nombre important de personnes[217]. À l'inverse, un écrit transmis à une seule personne peut revêtir un caractère public si aucune communauté d'intérêts ne lie ces deux personnes. L'exemple le plus parlant est celui de la transmission à un inspecteur du travail d'un écrit diffamatoire interne à une entreprise qui caractérise la publicité[218], le constat est le même lorsque l'écrit est transmis à un journaliste[219]. L'analyse du caractère public d'un propos ne peut résulter de la seule détermination d'une communauté d'intérêts unissant les différents destinataires d'un propos en particulier lorsque ce dernier est émis sur le support internet. La détermination de la publicité d'un propos se construit de façon empirique entre le critère qualitatif de la communauté d'intérêts et le critère quantitatif du nombre de personnes auxquelles le propos est rendu accessible. Dès lors, l'application de ces critères doit nécessairement s'analyser à la lumière des spécificités techniques de la communication sur les réseaux sociaux en ligne.

---

[215] C. BIGOT, *Pratique du droit de la presse*, Éd. Victoires, PUF, 2013, p. 85. Cette analyse est confortée par un arrêt ayant reconnu l'existence d'une communauté d'intérêts entre les différents locataires d'un office HLM, sans chercher si les intéressés « *s'étaient réunis en groupement ou en association de défense de leurs intérêts communs* » : Crim. 5 octobre 1999 : *Bull. Crim.* n° 203.

[216] En ce sens E. DERIEUX, *Droit des médias*, LGDJ, 7ème éd., 2015, p. 37, n° 11.

[217] Tel est le cas pour l'ensemble du personnel d'une usine dès lors que les placards ne sont pas accessibles aux personnes extérieures à l'usine, Crim., 8 octobre 1974, *Bull. Crim.* n° 280 ; Civ. 2ème , 8 novembre 1993, *Bull. Civ.* n° 318.

[218] Civ. 2ème, 14 novembre 2002, n° 00-15.549.

[219] Crim., 26 février 2008, n° 07-84.846 : *CCE* 2008 comm. 71, obs. A. LEPAGE.

B. La difficile réunion des critères qualitatifs et quantitatifs sur les réseaux sociaux en ligne

56. Les sites de réseaux sociaux ne sont pas des espaces publics par défaut. Si les réseaux sociaux en ligne forment le plus souvent des espaces de communication ouverts au public permettant de démontrer la publicité des propos y étant diffusés, il ne peut être conclu pour autant que ces derniers revêtent automatiquement un tel caractère. Ainsi, la détermination du caractère public d'un propos diffusé sur un réseau social doit résulter d'une démonstration positive attestant l'absence d'une communauté d'intérêts entre les personnes visées par le propos[220]. Il convient alors de déterminer quel critère peut servir de base à l'analyse du caractère public des propos diffusés sur les sites de réseaux sociaux. La difficulté de l'appréciation d'une communauté d'intérêts n'est pas propre à ces espaces d'échanges mais cette dernière se trouve dans leur contexte, particulièrement mise en relief dès lors que leurs utilisateurs disposent des instruments techniques permettant d'ouvrir de manière plus ou moins large leur auditoire.

57. L'impertinence du critère du lien virtuel. Cela amène à exclure dans un premier temps une analyse basée sur les liens virtuels unissant les utilisateurs d'un réseau social. Il s'agit en réalité de s'interroger sur la qualité du lien des différents « *amis* », « *followers* » ou plus généralement « *contacts* » au sein d'un même compte de réseau social. Sous le terme « *amis* » se cache une multitude de relations sociales différentes pouvant aller des liens familiaux, amicaux, des relations de travail, jusqu'aux simples connaissances voire, des contacts exclusivement virtuels. Les liens entre les différents contacts d'un compte de réseau social se trouvent souvent disparates, décousus. Il a par exemple été rappelé que « *le terme d' "ami" employé pour désigner les personnes qui acceptent d'entrer en contact par les réseaux sociaux ne renvoie pas à des relations d'amitié au sens traditionnel du terme et que l'existence de contacts entre ces différentes personnes par l'intermédiaire de ces réseaux ne suffit pas à caractériser une partialité particulière, le réseau social étant simplement un moyen de communication spécifique entre des personnes qui partagent les mêmes centres*

[220] Les juges du fond sont venus affirmer ce principe à propos du réseau social Facebook : « *aucun élément ne permettait de dire que le compte Facebook tel que paramétré par la salariée, ou par les autres personnes ayant participé aux échanges, autorisait le partage avec les "amis de ses amis" ou toute autre forme de partage avec des personnes indéterminées, de nature à faire perdre aux échanges litigieux leur caractère de correspondance privée* ». Rouen, ch. soc., 15 novembre 2011, n° 11/01827 : J.-E. RAY, « Little brothers are watching you », Semaine sociale Lamy, n° 1477, p. 78.

d'intérêt »[221]. Autrement dit, si de véritables liens forts peuvent se retrouver au sein d'un réseau social, les relations entre les différents contacts d'un compte ne permettent pas de déduire de manière générale l'existence de véritables liens de proximité et donc d'une communauté d'intérêts entre eux. L'analyse du caractère public des propos sur les sites de réseaux sociaux, doit alors s'effectuer au regard d'éléments davantage objectifs.

58. La pertinence du critère du paramétrage de confidentialité. Le critère du paramétrage de confidentialité se révèle mieux adapté pour déterminer le caractère public des propos diffusés sur les réseaux sociaux en ligne. Ce critère basé sur un aspect davantage quantitatif permet de déterminer l'ensemble des individus ayant accès aux propos diffusés au sein d'un compte de réseau social. En fonction de son paramétrage de confidentialité, l'utilisateur aura une maîtrise plus ou moins affirmée de son cercle de contacts et en conséquence de l'audience de ses propos. L'analyse de la quantité des personnes atteintes par les propos doit alors précéder l'analyse de la qualité du lien les unissant. En l'occurrence, la majorité du contentieux concernant le caractère public des espaces d'échanges sur les réseaux sociaux s'est principalement focalisée sur le réseau social Facebook. Les jurisprudences qui en émanent permettent d'émettre de premières hypothèses sur l'analyse du caractère public ou privé des propos diffusés sur des sites fonctionnant sur un modèle similaire.

En l'occurrence, le paramétrage de confidentialité permettant de définir l'audience potentielle du compte d'un réseau social (1) servira de référence pour démontrer que les réseaux sociaux forment un espace majoritairement public (2).

1) Le paramétrage de confidentialité, élément déterminant de la publicité des propos

59. Le paramétrage de confidentialité, élément d'interprétation pour le juge. L'ensemble des réseaux sociaux en ligne permettent peu ou prou à leurs utilisateurs d'effectuer un paramétrage de confidentialité. Il faut alors distinguer en fonction de ce critère les propos qui revêtent *de facto* un caractère public (a) des propos pouvant revêtir un tel caractère (b).

[221] Civ. 2ème, 5 janvier 2017, n° 16-12.394 : *D.* 2017, n° 62 ; *Dalloz IP/IT*, juin 2017, n° 6, p. 350-351; *RLDI*, 2017, n° 135, p. 33; *Légipresse*, janvier 2017, n° 345, p. 7 ; *D.*, 26 janvier 2017, n° 4, p. 208 ; *CCE* février 2017, n° 2, p. 1.

a- Les propos revêtant *de facto* un caractère public

60. Paramétrage au « *public* » ou aux « *amis des amis* ». Selon que le réseau social soit « *ouvert* » ou « *fermé* » à la communauté des internautes, les propos diffusés acquièrent ou non un caractère public. Aussi, lorsque l'utilisateur d'un réseau social programme son paramétrage de confidentialité comme ouvert au « *public* » ce dernier ouvre en réalité son compte à l'ensemble des utilisateurs du réseau social voire, à l'ensemble des internautes. Un tel paramétrage permet de déduire automatiquement le caractère public des propos y étant diffusés en raison de la largesse intrinsèque de l'auditoire y ayant accès. Cette réflexion vaut également pour les comptes paramétrés « *aux amis des amis* », dans cette hypothèse l'utilisateur ne maîtrise pas davantage le champ de diffusion de son propos[222] qui revêt alors *de facto* un caractère public. En somme, dès lors que le paramétrage de confidentialité du compte permet d'observer que l'audience du propos y étant diffusé dépasse les seuls contacts ou relations de l'individu sur le réseau social, il peut en être déduit le caractère public de celui-ci.

61. Ouverture par défaut du réseau social au public. Dans la majorité des cas les comptes de réseaux sociaux sont paramétrés par défaut au « *public* », l'utilisateur doit en conséquence réaliser une action positive sur son paramétrage de confidentialité pour restreindre l'audience de son compte. Par ailleurs, certains modèles de réseaux sociaux[223] fonctionnent sur des systèmes d'abonnements ou de « *followers* » ne permettant pas à l'utilisateur d'agréer les personnes avec qui il est en relation sauf si ce dernier privatise son compte. Le profil de l'utilisateur est de ce fait accessible à l'ensemble des adhérents du réseau social qui peuvent s' « *abonner* » ou « *suivre* » son profil sans le consentement de ce dernier. Dès lors les publications des utilisateurs sont ouvertes aux utilisateurs du réseau social mais également à tout internaute. Il est évident qu'en pareille hypothèse les critères qualitatif et quantitatif ne peuvent être réunis assurant le caractère public des propos publiés sur le profil de l'utilisateur.

[222] Partant du principe qu'en moyenne, le nombre d' « *amis* » sur un compte Facebook étant de 177 personnes (Blog du modérateur, « Les chiffres Facebook – 2019 », chiffres publiés le 4 juillet 2019 et mis à jour le 14 août 2019), l'audience potentielle d'un compte ouvert aux « *amis des amis* » est de 31 329 personnes (Ce calcul ne prend toutefois pas en compte l'éventualité que des mêmes contacts se retrouvent liés à plusieurs comptes).
[223] On peut citer ici les exemples de Twitter ou Instagram.

b- Les propos pouvant revêtir un caractère public

62. Paramétrage restreint aux seuls contacts. L'analyse devient plus complexe lorsque l'utilisateur d'un réseau social restreint l'audience de son compte à ses seuls contacts[224]. La Cour de cassation est venue apporter son interprétation à cette situation particulière dans un arrêt du 13 avril 2013[225]. En l'espèce, une personne avait proféré une injure sur son profil Facebook dont l'audience était paramétrée aux seuls « *amis* ». Selon les juges, les propos « *n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressée, en nombre très restreint* », de sorte que la Cour d'appel en a conclu que ces personnes « *formaient une communauté d'intérêts* » et en a déduit que les « *propos, n'étant pas destinés à un public inconnu et imprévisible, ne constituaient pas des injures publiques* »[226]. Il ne faut pas pour autant voir dans cette jurisprudence une portée générale, le juge s'étant livré à une analyse empirique de la situation. Le titulaire du compte avait d'une part, restreint l'audience de son compte à ses « *amis* » et d'autre part, leur nombre était particulièrement limité, à savoir 14, ce qui est significativement au-dessous de la moyenne du nombre de contacts observée sur le réseau social Facebook[227]. Les « *amis* » Facebook peuvent dans ce cas former une entité au sein de laquelle s'observe une communauté d'intérêts, du moment que leurs nombre est connu ou prévisible et qu'ils soient tous identifiés[228]. Cette solution privilégie cependant le critère quantitatif au critère qualitatif, selon cet arrêt, un faible nombre de personnes agréées par le titulaire du compte suffirait à exclure la publicité des propos tenus sur le profil de l'intéressé. Autrement dit, donner à quelqu'un l'accès à sa page Facebook en l'acceptant dans ses contacts suffirait à déterminer avec lui et les autres contacts du profil un lien objectif, une

[224] Facebook en tant que service interactif, permet à ses utilisateurs de publier des contenus sur leur propres « *pages* » mais également sur les « *pages* » d'autres utilisateurs. En l'occurrence, le caractère public ou non des contenus publiés par un utilisateur sur la page d'un autre utilisateur épouse le paramétrage de confidentialité du compte sur lequel le contenu est publié. La personne à l'origine de la publication, partant du principe qu'elle ne peut connaître le paramétrage de confidentialité du compte récepteur, ne peut donc prévoir l'audience potentielle de son post. Or, les infractions de presse sont intentionnelles impliquant pour leur auteur d'avoir eu la conscience et la volonté d'accomplir l'ensemble des éléments constitutifs de l'infraction, y compris de donner à son propos une dimension publique. L'élément moral devient alors l'imprudence de publier un propos dans une interface dont l'audience est inconnue ou plutôt non maîtrisée.

[225] Civ. 1ère, 10 avril 2013, n° 11-19530 : *Bull. civ.* I, n° 70 ; *JCP* G 2013, 816, spéc. n° 17, obs. L. MARINO ; *JCP* E 2013, spéc. n° 47, note B. BOSSU ; *Légipresse* 2013, p. 312, n° 305, note B. ADER ; *CCE* 2013, comm. n° 81, obs. A. LEPAGE ; « Des injures proférées sur des réseaux sociaux ne sont pas forcément publiques », *D. actu.*, 24 avril 2013 ; M. HUYETTE, « À propos des injures sur Facebook » : blog Paroles de juges, 25 avril 2013.

[226] L. MARINO, « Qualification de l'injure sur Facebook », *JCP* G n° 17, 22 Avril 2013, n° 466.

[227] Le nombre d'amis moyen en France est de 177. Blog du modérateur, « Les chiffres Facebook – 2019 », chiffres publiés le 4 juillet 2019 et mis à jour le 14 août 2019.
<https://www.blogdumoderateur.com/chiffres-facebook> (dernière consultation le 9 octobre 2019).

[228] B. ADER, « les "amis" sur Facebook forment une communauté d'intérêts », *Légipresse* n°35, Mai 2013, p. 312-313.

appartenance commune. Un faible nombre d' « *amis* » Facebook n'est cependant pas gage d'une réelle communauté d'intérêts entre eux, la Cour de cassation ayant postérieurement rappelé la faiblesse de ce prétendu lien d'amitié[229]. Il apparaît alors déterminant, au-delà de l'analyse portant sur le nombre de personnes atteintes, d'examiner la qualité du lien les unissant afin d'en déduire une réelle existence d'une communauté d'intérêts.

63. Les groupes thématiques sur les sites de réseaux sociaux. Le profil de l'utilisateur n'est pas le seul espace d'échanges sur les réseaux sociaux, certains groupes de discussion thématiques formant également des espaces d'expression. À l'instar des comptes des utilisateurs, l'expression au sein des groupes ou communautés formés sur les réseaux sociaux est fonction dans un premier temps du paramétrage de confidentialité attribué à ces espaces. Les groupes ouverts doivent être assimilés à des espaces de discussion publics dans la mesure où tout utilisateur du réseau social y a accès. À l'inverse, les groupes fermés induisent l'application des critères quantitatif et qualitatif afin de déterminer la nature publique ou privée des échanges. Certains de ces groupes de discussion thématiques pourraient alors matérialiser une communauté d'intérêts entre leurs différents membres et garantir en conséquence le caractère privé des propos y circulant. Le raisonnement doit cependant prendre en compte non seulement l'intérêt commun unissant les différents membres mais également leur nombre. Or, certains groupes dénombrent plusieurs milliers d'adhérents[230], dans cette hypothèse il apparaît difficile au vu du critère quantitatif d'admettre le caractère privé des propos diffusés sur ces espaces de discussion quand bien même ces derniers seraient fermés. Dans un second temps, pour que le critère qualitatif de la communauté d'intérêts fonctionne, la teneur des propos échangés au sein du groupe doit correspondre à la thématique de discussion réunissant ses différents membres. Par exemple, le titulaire d'un compte Facebook peut classer ses contacts dans différents groupes comme par exemple les groupes « *famille* », « *amis* », « *collègues* », « *connaissances* ». Ces entités qui regroupent nécessairement un nombre restreint d'individus, matérialisent au mieux la conception de la communauté d'intérêts telle que rencontrée sur un site de réseau social[231].

[229] V. *supra* n° 57.
[230] Par exemple, le groupe fermé « Guitarsites » qui dénombre environ 30 000 membres.
[231] M. HUYETTE, « À propos des injures sur Facebook », blog Paroles de juges, 25 avril 2013, <www.huyette.net> ; E. PIERROUX, « Facebook, Twitter et autres réseaux sociaux : petites injures entre "amis" », *Gaz. Pal.* 3 décembre 2015, n° 337, p. 4.

2) Les réseaux sociaux en ligne, un espace majoritairement public

64. **Analyse empirique.** La grille d'analyse vue ci-dessus est applicable à l'ensemble des sites de réseaux sociaux. Il est nécessaire de privilégier une analyse empirique basée sur le paramétrage de confidentialité opéré par chaque utilisateur ou chaque administrateur d'un espace de discussion. Le caractère public d'un propos émis sur un réseau social devient alors fonction du nombre de personnes ayant accès à celui-ci et de la qualité du lien les unissant. Partant du constat du nombre élevé d'utilisateurs faisant l'une des spécificités des sites de réseaux sociaux, il est déduit d'une part qu'un paramétrage au « *public* » ou aux « *amis des amis* » forme nécessairement un espace de discussion public. D'autre part, un paramétrage restreint aux seuls contacts de l'utilisateur ne permet pas de conclure pour autant à un espace de discussion privé. Cela se justifie au regard du nombre moyen élevé de contacts par utilisateur qui ne permet le plus souvent pas d'établir une réelle communauté d'intérêts entre ces derniers. En réalité, lorsque le compte est paramétré aux seuls « *amis* » ce dernier ne recouvrira un caractère privé que dans des cas bien particuliers où le nombre de contacts du titulaire du compte est extrêmement faible, de sorte qu'une réelle communauté d'intérêts entre les contacts puisse être identifiée. La détermination du caractère public d'un propos émis sur un réseau social dépend alors d'une analyse empirique de l'auditoire ayant accès au propos.

65. **Analyse selon l'audience potentielle.** La précision majeure réside dans la façon de prendre en compte l'audience du propos diffusé et donc la manière de déterminer si ce dernier revêt un caractère public. À ce titre, le caractère public d'un compte ne se mesure pas en termes d'audience effective mais par son audience potentielle ce qui justifie pourquoi un compte paramétré au « *public* » se voit *de facto* attribuer le caractère d'espace public. Il est insinué que même si le titulaire du compte ouvert au public possède un nombre extrêmement restreint de contacts pouvant matérialiser une réelle communauté d'intérêts, l'audience potentielle du compte dépasse de loin le cercle privé. Autrement dit, il ne faut pas s'attacher au faible nombre de contacts de l'utilisateur ayant eu connaissance effective du propos litigieux, mais à l'ensemble des internautes pouvant à tout moment y accéder. Un parallèle peut être réalisé avec l'acte d'affichage dont le caractère public est déduit de la seule présence d'une feuille imprimée ou dactylographiée apposée sur un mur dans un lieu public[232]. De même, ce raisonnement peut être rapproché de la jurisprudence de la chambre criminelle de la Cour de cassation selon laquelle un propos proféré à la terrasse d'un restaurant est nécessairement public alors même qu'aucune personne ne se trouvait sur les lieux à ce

[232] Crim. 18 juin 1958 : *Bull. crim.* 1958, n° 465.

moment[233]. Au final, l'expression à caractère public est « *celle qui, délibérément mise à la disposition des tiers par son auteur, l'est également en considération de l'indétermination des personnes qui sont appelées à en prendre connaissance* »[234].

66. Conclusion de la Section 1. La détermination du caractère public d'un propos émis sur un réseau social s'effectue en l'occurrence par une analyse *in concreto* basée sur le paramétrage de confidentialité opéré par l'utilisateur ou l'administrateur de l'espace de discussion incriminé au regard du critère qualitatif de la communauté d'intérêts et du critère quantitatif du nombre de personnes ayant eu accès à ce dernier. Le caractère privé d'une allégation émise sur un réseau social se déduit de situations particulières où l'espace de discussion est fermé à un nombre restreint d'individus formant une réelle communauté d'intérêts autour du sujet animant le débat. En réalité, tant au regard du critère qualitatif que du critère quantitatif, les propos diffusés sur les réseaux sociaux en ligne revêtent dans leur large majorité un caractère public amenant à un regain d'application de la loi sur la liberté de la presse du 29 juillet 1881. Cette capacité de diffusion inégalée associée au nombre croissant des utilisateurs de ces plateformes d'échanges[235] favorise une augmentation automatique du nombre de délits commis par voie de presse. L'enjeu consiste alors à s'assurer de l'adaptation des incriminations prévues par la loi sur la liberté de la presse à cette nouvelle expression massive permise par les réseaux sociaux en ligne[236].

[233] V. en ce sens : Crim. 27 mai 1943 : DA 1943. 52 – Crim. 15 mars 1983 : *Bull. crim.* n° 82 : « *Est un lieu public par nature la terrasse d'un restaurant* ».
[234] T. BESSE, *La pénalisation de l'expression publique*, Thèse, Université de Limoges, soutenue le 22 juin 2018, p. 46, n° 47.
[235] À titre d'exemple : chaque minute 2,46 millions de contenus sont échangés sur Facebook, 277 000 tweets sont envoyés, 216 000 photos sont partagées sur Instagram. Source : Novius ; Rapport d'information de MM. F. PILLET et T. M. SOILIHI, « L'équilibre de la loi du 29 juillet 1881 à l'épreuve d'Internet », fait au nom de la commission des lois n° 767 (2015-2016), 6 juillet 2016.
[236] Le Professeur Robert Badinter avait su souligner cet enjeu lors des débats au Sénat relatifs à la loi « Perben II » : « *La technique a fondamentalement modifié les données du problème. (…) Nous ne sommes plus au temps de la presse imprimée ! Nous sommes tous ici les défenseurs de la liberté de la presse et j'ai, pour ma part, beaucoup plaidé pour elle au cours de ma vie. Mais nous sommes là devant un outil qui est sans commune mesure avec la presse écrite que nous avons connue, et qui était en fait celle de 1881. L'internet pose des problèmes considérables et il faut prendre des dispositions adaptées* ». Sénat, séance du 20 janvier 2004.

Section 2 : Les nouvelles formes d'expression appréhendées par les incriminations de presse

67. Une loi adaptée aux nouvelles formes de communication. Cette extension du champ d'application de la loi sur la liberté de la presse qui n'avait pas été prévue à l'origine, implique nécessairement des conséquences sur le contenu de cette loi plus que centenaire. Sur ce point, deux visions s'opposent. D'un côté internet aurait sonné le glas de la loi sur la liberté de la presse imaginée à l'origine pour la société du XIXème siècle. En effet, cette évolution dans les techniques de communication engage des conséquences trop importantes pour que cette loi puisse les absorber. Certains observateurs préconisent alors un basculement de nombreuses infractions de presse dans le droit commun à l'image du délit de provocation et d'apologie au terrorisme, ce qui contribue à un mouvement de déspécialisation de la loi sur la liberté de la presse[237]. D'un autre côté, la loi du 29 juillet 1881 doit être défendue en ce qu'elle définit « *de manière subtile et évolutive, l'équilibre à maintenir entre la liberté d'expression, qu'elle protège et ses limites. C'est pourquoi, les infractions incriminant les discours de haine, abus de la liberté d'expression, présentent une spécificité telle, qu'il n'est pas permis de les intégrer dans le Code pénal* »[238]. Bien entendu, il ne s'agit pas d'affirmer que la loi sur la liberté de la presse ne nécessite aucune intervention ou rajeunissement. L'ensemble du corps des infractions de presse doit être utilisé ou réutilisé ce qui peut engager quelques retouches ponctuelles[239].

Les incriminations de presse démontrent leur adaptation aux nouvelles formes d'expressions permises par les sites de réseaux sociaux (**§1**). L'expression massive suscitée par les réseaux sociaux en ligne entraîne de surcroît un certain regain d'intérêt pour certaines incriminations de presse tombées en désuétude, particulièrement le délit de fausse nouvelle (**§2**).

---

[237] V. en ce sens : Rapport d'information de MM. F. PILLET et T. M. SOILIHI, « L'équilibre de la loi du 29 juillet 1881 à l'épreuve d'Internet », fait au nom de la commission des lois n° 767 (2015-2016), 6 juillet 2016 ; E. DREYER, « L'opportunité d'une sortie des infractions de presse de la loi du 29 juillet 1881 au regard d'un exemple précis : le cas du délit d'apologie du terrorisme et de provocation aux actes de terrorisme », *in* N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, Coll. Grands Colloques, 2017, p. 37 et suiv.

[238] Avis sur la lutte contre les discours de haine sur internet, Commission Nationale Consultative Des Droits De l'Homme (CNCDH), assemblée plénière, 12 février 2015.

[239] V. sur le sujet : N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, Coll. Grands Colloques, 2017.

§1. L'adaptation des incriminations de presse aux nouvelles formes d'expression

68. L'adaptation des incriminations aux contenus publiés sur les sites de réseaux sociaux. Les modes d'expression rencontrés sur les réseaux sociaux sont plus riches que dans la presse traditionnelle. Le terme *propos* semble en l'espèce trop réducteur au regard des possibilités de communication offertes par les sites de réseaux sociaux, il convient alors d'utiliser la notion de *contenu* qui appréhende plus largement le potentiel d'expression permis par ce sites. En effet, les contenus échangés sur internet comprennent les propos qui peuvent être diffusés de manière textuelle ou sonore mais aussi des images ou vidéos accompagnées ou non de textes ou encore des liens hypertextes. L'expression rencontrée sur les réseaux sociaux se retrouve sous des formes plus diverses mais qui demeurent tout autant soumises à la loi sur la liberté de la presse. L'article 23 de la loi du 29 juillet 1881 rappelle que le droit de la presse sanctionne tout individu qui aurait proféré de manière publique et ce par tout support de la parole, de l'écrit ou de l'image y compris tout moyen de communication au public en ligne, un propos constituant une infraction de presse. Tout contenu diffusé sur un site de réseau social, quelle que soit sa forme, se trouve potentiellement soumis à l'application du droit de la presse. Cette affirmation se vérifie particulièrement à l'égard de l'expression sous forme de hashtags (A) mais également concernant l'expression sous forme de partage de contenus (B).

A. L'adaptation de l'incrimination de presse aux hashtags

69. Le hashtag, un moyen d'expression publique. Le réseau social Twitter a mis en place un système de mots clés, plus connu sous le terme anglais de *hashtag* ou sous le symbole # (dièse), permettant de regrouper tous les messages portant sur un thème similaire favorisant un accès rapide et ciblé aux contenus[240]. En d'autres termes, « *il s'agit d'un mot-clé cliquable précédé du signe # qui sert d'agrégateur de contenus permettant de classer les tweets relayés par la plateforme* »[241]. Le système du hashtag est d'abord apparu sur Twitter et s'est ensuite propagé à d'autres réseaux sociaux tels Facebook, Instagram ou encore Pinterest. Techniquement, les hashtags permettent de donner un contexte supplémentaire aux messages pour contourner le nombre de caractères restreints imposés par le site (par exemple, 280 signes pour Twitter). Ainsi, « *le hashtag permet de suivre une thématique donnée ou un*

[240] Vocabulaire des télécommunications et de l'informatique, *JORF* n° 0019, 23 janvier, p. 1515.
[241] D. LABOURDIQUE-BOUZIDI, « Les hashtags: quelle protection pour quelle action ? », *JCP* E, 13 octobre 2016, pp. 5-6.

évènement auquel on ne peut assister. Il devient un véritable slogan interactif pour créer un espace communautaire autour d'un sujet de conversation »[242]. Le hashtag, qui effectue une catégorisation des contenus, est accessible à l'ensemble de la communauté des internautes. Celui-ci doit alors être assimilé à un espace de discussion thématique public par nature car n'étant pas soumis à l'action d'un paramétrage de confidentialité.

70. Le hashtag, moyen de commission d'infractions. Ces modes d'expression aussi brefs soient-ils, peuvent constituer une infraction de presse de manière autonome dès lors qu'ils recouvrent l'ensemble de ses éléments constitutifs. Par exemple, les hashtags « *#UnJuifMort* » ou encore « *#SiJétaisNazi* »[243] ont été jugés comme constitutifs de propos d'apologie de crimes contre l'humanité et d'incitation à la haine raciale prévus à l'article 24 alinéas 3 et 5 de la Loi du 29 juillet 1881[244]. De la même manière, les auteurs des hashtags « *#BrûlonsTousLesGaysSurDuLégion88* », « *#LaChasseAuxPD* », ainsi que « *#LesGayDoiventDisparaitreCar* » ont été condamnés sur le fondement de l'article 24 alinéa 6 de la loi sur la liberté de la presse pour provocation à la haine ou à la violence, à l'égard d'une personne ou d'un groupe de personnes à raison notamment, de leur orientation ou de leur identité sexuelle[245].

71. Il faut toutefois distinguer les hashtags qui sont en eux-mêmes constitutifs de l'infraction à l'image du hashtag « *#LaChasseAuxPD* », des hashtags qui, pris isolément, ne peuvent constituer l'infraction mais qui deviennent répréhensibles en raison de leur contexte et notamment du contenu du tweet qui leur est associé comme par exemple « *#SiMonFilsEstGay* » ou encore « *#UnBonJuif* ». De même le caractère apologétique du hashtag « *#JeSuisKouachi* » faisant référence à l'un des terroristes ayant participé aux attentats de Charlie Hebdo doit être examiné à la lumière du contenu du tweet l'accompagnant[246]. Ce hashtag a en effet été utilisé également par des personnes voulant dénoncer les actes de terrorisme et non en faire l'apologie.

---

[242] N. DREYFUS, « Quel encadrement juridique pour le hashtag ? », *Expertises des systèmes d'information*, mars 2015, n° 400, p. 107.

[243] Des milliers de tweets ont été publiés sur Twitter sous ces hashtags et se sont retrouvés placés en première position de la rubrique « tendances » de la plateforme, V. F. PERBOST, « La lutte contre les propos antisémites sur internet », Chronique du droit des nouvelles technologies, *Revue de jurisprudence commerciale*, juillet/août 2014, n° 4.

[244] TGI Paris, 24 janvier 2013, n° 13/50276, UEJF/ Twitter Inc. Et Sté Twitter France : *Légipresse* n° 304, p. 235, com. N. MALLET-POUJOL.

[245] TGI Paris, 20 janvier 2015, association Comité IDAHO c/ M. X. et a. : *Légipresse*, n° 326, avril 2015, p. 212.

[246] N. DREYFUS, « Quel encadrement juridique pour le hashtag ? », *op. cit*., p. 107. Précisons que le hashtag « *#JeSuisKouachi* » a pu être également utilisé par des personnes voulant dénoncer les actes de terrorisme et non en faire l'apologie. Dans ce cas précis, le caractère apologétique du hashtag doit être examiné à la lumière du contenu du tweet l'accompagnant.

Au final, l'expression par le biais du hashtag n'échappe pas aux prévisions de la loi sur la liberté de la presse qui ne trouve aucun mal à s'appliquer à ces petits modes d'expression qui, se voulant percutants, poussent souvent leurs auteurs à franchir les limites admissibles de la liberté d'expression.

B. L'adaptation de l'incrimination de presse aux partages de contenus

72. Partage ou approbation d'un contenu. Les usages rencontrés sur les sites de réseaux sociaux ont démultiplié les hypothèses de diffamations par reproduction. Il s'agit de déterminer si le partage de contenus, spécifique aux sites de réseaux sociaux, peut être assimilé à une reproduction au sens de l'article 29 de la loi sur la liberté de la presse. Le partage de contenus sur les réseaux sociaux peut se faire de différentes manières. Premièrement, ces sites proposent certaines fonctionnalités ayant pour objet direct le partage d'informations[247]. Mais plus encore, la reproduction d'une information publiée sur un réseau social s'observe également par d'autres moyens que la simple fonction de partage proposée par ces sites. En réalité, la reproduction d'un contenu s'entend de manière bien plus large que son simple partage. Ainsi, le simple fait de marquer son approbation à une publication ou plus généralement d'agir sur un contenu[248] a pour effet de rendre visible celui-ci à un nouveau cercle d'utilisateurs qui n'y avait pas nécessairement accès à l'origine[249]. Le caractère public du contenu relayé sera alors fonction du paramétrage de confidentialité opéré par le titulaire du compte ayant reproduit le contenu[250]. En somme, les effets de l'approbation ou plus largement de la réaction[251] à un contenu sont quasi-identiques à ceux du partage d'un contenu sur un réseau social. Par exemple, « *liker* » un contenu sur le réseau social Facebook agira dans un premier temps sur le contenu lui-même en augmentant sa notoriété mais contribuera également à propager ce dernier au sein du réseau et à le rendre visible à de nouveaux cercles

[247] Sur Facebook on retrouve ainsi le bouton "partager" (ou "*Share*" en anglais), sur Twitter la fonction de partage s'observe avec le retweet.
[248] Sur les réseaux sociaux de multiples actions sont possibles telles que : aimer le contenu, désapprouver le contenu, identifier quelqu'un, commenter le contenu etc.
[249] Le 29 mai 2017, un tribunal d'arrondissement de Zurich a condamné au paiement d'une amende équivalent à 3 700 € un ressortissant suisse du chef de diffamation pour avoir « liké » des propos sur Facebook reprochant au président d'une association de lutte contre les élevages et abattoirs d'animaux d'être « raciste », « fasciste » et « antisémite ». D'après le tribunal, le prévenu, « *en cliquant sur le célèbre pouce levé, a propagé un jugement de valeur et des accusations qu'il n'a pas pu prouver* ». E. DREYER, « "Liker" un contenu injurieux revient-il à injurier autrui ? », *D.* 2017, p. 1464.
[250] V. *supra.* n° 59 et suiv.
[251] Il faudrait en réalité non pas parler d' « approbation » d'un contenu mais plutôt de « réaction à un contenu ». Facebook permet de réagir de différentes façons à une publication : « j'aime », « triste », « en colère », « j'adore », « wouah », « haha ». Par ailleurs, le fait de commenter une publication s'analyse également comme une réaction à ce contenu.

d'utilisateurs qui n'en n'avaient jusque-là pas encore connaissance. En ce sens, la réaction à un contenu, au même titre que son partage, contribue techniquement à la reproduction de ce dernier au sein du réseau concerné. Toutefois, si l'action de partager démontre l'intention de rendre accessible le contenu à un nouveau cercle d'individus, la simple approbation d'un contenu ne démontre quant à elle pas nécessairement cette intention même si les effets sont similaires. Cette position est partagée par le Professeur Emmanuel Dreyer qui distingue le relais d'un contenu de sa simple approbation qui, selon ce dernier, ne peut constituer une infraction de presse à part entière[252]. Se pose alors la question de la qualification pénale d'une telle reproduction constitutive d'une infraction de presse.

73. L'impossible complicité du relayeur. Malgré la présence de règles spécifiques en matière de complicité[253], la loi sur la liberté de la presse ne renonce pas pour autant à envisager la possibilité de voir prononcer des condamnations au titre d'une complicité de droit commun prévue aux articles 121-6 et 121-7 du Code pénal[254]. Est considérée comme complice, la personne qui « *sciemment, par aide ou assistance* », a « *facilité la préparation ou la consommation* » d'une infraction, ou « *par don, promesse, menace, ordre, abus d'autorité ou de pouvoir aura provoqué à une infraction ou donné des instructions pour la commettre* ». Partant, le relayeur d'un contenu diffamatoire ou injurieux ne peut, selon les règles de droit commun, être déclaré complice de l'infraction dans la mesure où le relais de l'infraction est nécessairement réalisé après sa réalisation. Le complice doit avoir intentionnellement et matériellement participé à la publication litigieuse par fourniture de moyens[255], une intervention *a posteriori* ne peut donc fonder un acte de complicité au sens de l'article 121-7 du Code pénal[256]. Si le relais d'une infraction de presse ne peut constituer une complicité de droit commun, la question qu'il reste à résoudre est la suivante : le fait de relayer un contenu délictueux sur un réseau social peut-il caractériser en soi également un délit de presse ? Dans cette hypothèse, le relayeur serait l'auteur d'une nouvelle infraction. Le droit de la presse vient expressément régir ce type de situation à l'incrimination de diffamation qui prévoit la reproduction d'un contenu diffamatoire au même titre que la publication originelle (1). Cette hypothèse pourrait être étendue à l'ensemble des incriminations de presse (2).

---

[252] « *La loi du 29 juillet 1881 permet seulement de sanctionner le fait de rendre public un propos injurieux. L'approbation publique de ce même propos ne semble pas équivaloir au fait de le publier* », E. DREYER, « "Liker" un contenu injurieux revient-il à injurier autrui ? », *op. cit.*, p. 1464.
[253] V. *infra* n° 428.
[254] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 647, n° 1122.
[255] *Ibid.*
[256] En ce sens : E. DREYER, « "Liker" un contenu injurieux revient-il à injurier autrui ? », *D.* 2017, p. 1464.

1) L'hypothèse de reproduction prévue par l'incrimination de diffamation

74. La reproduction d'un propos diffamatoire. L'article 29 alinéa 1 de la loi de 1881 précise que « *la publication directe ou par voie de reproduction* » d'une allégation diffamatoire est punissable. En conséquence, dès l'instant où un individu reproduit une accusation diffamatoire, ce dernier commet lui-même l'infraction quand bien même le propos d'origine n'aurait pas été poursuivi ou serait prescrit. Ces précisions de la loi sur la liberté de la presse ont été jugées inutiles par Pierre Mimin selon lequel « *la circonstance qu'un fait diffamatoire est déjà rendu public n'a jamais été considéré comme justifiant celui qui le publiait à nouveau* »[257].

75. Relais d'un propos diffamatoire sous forme dubitative. Par ailleurs, le partage d'un propos diffamatoire revêt un caractère infractionnel, même lorsque la personne a pris le soin de nuancer celui-ci dans un commentaire annexe. Selon la loi sur la liberté de la presse, la prudence dans le ton ne retire pas à la reproduction son caractère illicite. L'article 29 de de cette loi dispose dans ce sens que « *la publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative* ». Cette affirmation a largement été reprise par la jurisprudence qui souligne que la diffamation peut être présentée « *sous une forme déguisée, ou dubitative ou par voie d'insinuation* »[258]. En conséquence, à partir du moment où le propos revêt un caractère diffamatoire, le fait de l'exposer au public même sur un ton modérateur caractérise le délit de diffamation publique. Cette position est notamment défendue par Monsieur Emmanuel Netter selon lequel : « *le fait d'assortir l'acte de partage d'un commentaire personnel exprimant une incertitude sur la réalité de l'information ne suffit même pas à éviter les foudres de la loi !* »[259].

76. La prise en compte des faits justificatifs en matière de diffamation. Cette position vaut cependant dans la limite des faits justificatifs spéciaux applicables au délit de diffamation

---

[257] P. MIMIN, *D.* 1946, législ. p. 3. En l'espèce, le contentieux concerne souvent la reprise d'informations d'origine policière ou judiciaire. V. notamment : Crim., 4 décembre 2007 : *D.* 2008, act. Jurispr. p. 298.

[258] Crim. 2 janvier 1980 : *Bull. crim.* 1980, n° 3 – Crim., 29 mars 1978 : *Bull. crim.* 1978, n° 118 – Crim., 21 avril 1980 : *Bull. crim.* 1980, n° 115 – Crim., 23 octobre 1980 : *Bull. crim.* 1980, n° 270 – Crim., 17 juillet 1985 : *Bull. crim.* 1985, n° 267 – Crim., 30 mai 1996 : *Bull. crim.* 1996, n° 228 – Civ. 2ème, 10 juin 1999 : *Bull. civ.* II, n° 46 – Crim., 11 février 2003, n° 01-86.041 – Civ. 1ère, 27 septembre 2005 : *Bull. civ.* I, n° 346 ; *D.* 2006, 637, note S. VIGAND ; Pror. intel. janvier 2006, n° 18, p. 81, note J. PASSA.

[259] E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, p. 171, n° 141. L'auteur défend ce point de vue en soulignant que : « *cette solution, qui semble bien sévère au premier abord, se comprend par la préoccupation qui animait certainement le législateur : empêcher la propagation de rumeurs nauséabondes. Partager l'accusation dégradante, c'est lui donner corps et substance, la porter à l'attention d'autrui, quand bien même le véhicule serait habillé d'incertitude. Le combat contre la rumeur, légitime déjà au XIXe siècle, n'est que plus nécessaire à présent qu'un ragot peut faire le tour du monde en moins d'une heure* ».

à savoir l'exception de vérité prévue à l'article 35 de la loi du 29 juillet 1881 et la bonne foi du diffamateur[260]. La Cour de cassation rappelle que le fait justificatif de bonne foi, qui se distingue de l'exception de vérité des faits diffamatoires, « *se caractérise par la légitimité du but poursuivi, l'absence d'animosité personnelle, la prudence et la mesure dans l'expression ainsi que la fiabilité de l'enquête* »[261]. Le diffamateur qui poursuit un but légitime en portant à la connaissance du public une information utile se verra donc reconnaître le fait justificatif de bonne foi d'autant plus lorsque le sujet abordé relève de « *l'intérêt général* »[262]. En l'occurrence, la jurisprudence réalise une interprétation large des sujets revêtant un intérêt légitime et bénéficiant ainsi d'une liberté de parole accrue[263]. C'est le cas des débats d'ordre historique[264], sportif[265], judiciaire[266] et particulièrement politique[267]. Cependant, la reconnaissance de la bonne foi du diffamateur dépend également de la démonstration d'une absence d'animosité personnelle envers le diffamé ou du moins d'une prudence dans l'expression. Ce dernier critère est cependant nuancé dans le domaine de la polémique politique où « *le fait justificatif de la bonne foi n'est pas nécessairement subordonné à la prudence dans l'expression de la pensée* »[268]. En définitive le retweet d'un contenu diffamatoire peut être sanctionné sur ce même fondement si l'ensemble des propos rattachés au retweet emportent la qualification du délit de diffamation et qu'aucun fait justificatif, notamment la bonne foi de l'internaute, de ne peut être démontré.

2) Généralisation de l'hypothèse de reproduction aux incriminations de presse

77. Assimilation de la solution existante en matière de diffamation à l'injure. L'article 29 alinéa 2 de la loi sur la liberté de la presse définit l'injure comme « *toute expression*

[260] Une diffamation peut devenir licite par l'application de faits justificatifs ordinaires mais elle connaît également des causes de justification qui lui sont propres : l'*exceptio veritatis* et la bonne foi. V. P. CONTE, *Droit pénal spécial*, Litec, 3ème éd. 2007, n° 412.
[261] Civ. 2ème, 14 mars 2002 : *Bull. civ.* II, n° 41.
[262] Crim. 3 novembre 2015, n° 14-83.420 – Civ. 1ère, 3 février 2011, n° 09-10.301 : *Bull. civ.* I, n° 21 ; *CCE* 2011. Comm. 46, obs. A. LEPAGE ; *D.* 2012. Pan. 765, obs. E. DREYER.
[263] V. par exemple : Civ. 1ère, 11 juillet 2018, n° 17-22.381 : Hebdo édition privée Edition n° 753, 13 septembre 2018, note N. DROIN – Crim., 8 janvier 2019, n° 17-81.396 : Lexbase Pénal Edition n° 13 du, 21 février 2019, note N. DROIN.
[264] Crim. 16 mai 1995, n° 93-83.690 : *Bull. crim.* n° 175.
[265] Crim. 11 juillet 2017, n° 16-84.859 : Jurisport 2017, n° 179, p. 9, J. MONDOU ; *AJ Pénal* 2017, p. 497 ; *D. actu.*, 6 sept. 2017, obs. S. LAVRIC.
[266] Crim. 27 juin 2000, n° 99-85.258.
[267] La Cour de cassation se montre ouvertement bienveillante à l'égard des propos relevant de la polémique politique. V. par exemple : Crim. 23 mars 1978, n° 77-90.339 : *Bull. crim.* n° 115 ; *LPA* 24 janvier 1997, n° 11, p. 13. V. également sur le sujet : N. , « [Actes de colloques] 2ème Congrès des jeunes pénalistes (28 septembre 2018) : la politique et le droit pénal - L'expression des politiques : une marge de manœuvre confortable, des bornes étroites... », Lexbase Pénal Edition n° 11, 20 décembre 2018.
[268] Crim. 23 mars 1978, n° 77-90.339 : *Bull. crim.* n° 115.

outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait ». L'injure se définit en conséquence par opposition à la diffamation en ce qu'elle ne renferme l'imputation d'aucun fait précis[269]. L'injure se distingue également de la diffamation en ce que l'article 29 alinéa 2 ne vient pas préciser l'hypothèse de la reproduction de celle-ci. Deux solutions sont alors envisageables : la première reviendrait à effectuer une lecture stricte de l'article 29 alinéa 2 de la loi sur la liberté de la presse et à conclure que seul l'auteur du propos injurieux peut être poursuivi pour injure ; la seconde serait d'assimiler la répression de l'injure à la solution existante en matière de diffamation. Dans ce cas, l'auteur mais également celui qui reproduit un propos injurieux seraient susceptibles de poursuites. Cette dernière interprétation est celle préconisée par Monsieur Emmanuel Netter qui affirme que « *ceux qui la [l'injure] reprennent pour poursuivre et amplifier l'agression ou l'humiliation de la personne visée se rendent évidement coupables d'injures* »[270]. Cette interprétation semble convaincante tant la loi du 29 juillet 1881 vient sanctionner la publication d'un propos injurieux et non uniquement sa rédaction. En revanche, si le partage d'une injure est constitutif lui-même du délit d'injure, *quid* si le propos est accompagné d'une modération ?

78. Le relais d'un propos injurieux accompagné d'une modération. Le délit d'injure publique obéit à une logique différente lorsque la reproduction est accompagnée d'une modération. Les personnes qui reprennent une injure dans le but de la dénoncer ne participent pas à la propagation d'une rumeur (qui est du domaine de la diffamation) et ne tiennent pas de propos outrageant, partant l'infraction d'injure ne saurait être constituée[271]. En somme, la modération accompagnant l'invective contribue à retirer à l'ensemble du propos son caractère outrageant, condition nécessaire de l'infraction. Les éléments constitutifs du délit d'injure ne sont dès lors plus réunis, retirant à la reproduction son caractère délictueux.

79. Généralisation de la sanction de la reproduction d'un contenu à l'ensemble des incriminations de presse. Au vu de ces éléments il est proposé de généraliser à l'ensemble des infractions de presse la répression de la reproduction au public d'un contenu constitutif

---

[269] Selon les juges de Cour de cassation : « *pour être diffamatoire, une imputation doit se présenter sous la forme d'une articulation précise de faits de nature à être, sans difficulté, l'objet d'une preuve et d'un débat contradictoire, et que lorsqu'une telle articulation fait défaut il ne peut s'agir que d'une injure* », Crim., 17 février 1981, *Bull. crim.* 1981, n° 64. Le terme « *canaille* » a été jugé constitutif d'une injure, distincte d'un éventuel délit de diffamation, dans la mesure où il a été « *employé sans aucune imputation de faits précis et sans rapport avec le contexte de l'article* », Crim., 22 juin 1994, n° 92-21060.

[270] E. NETTER, « La responsabilité juridique de l'utilisateur de Twitter », *JCP* G, 2013, n° 3, p. 102-103.

[271] Selon E. NETTER : « *pour la dénoncer, pour exprimer le dégoût qu'elle leur inspire, ne peuvent sans doute rien se voir reprocher : ils ne participent à la propagation d'aucune rumeur (c'est le domaine de la diffamation et non de l'injure), et ils ne tiennent aucun propos outrageant, bien au contraire* », *in* « La responsabilité juridique de l'utilisateur de Twitter », *JCP* G, 2013, n° 3, p. 102-103.

d'une infraction de presse au même titre que la publication d'origine. Cette solution est justifiée par le fait qu'en matière de presse, la publication est l'élément par lequel les infractions sont consommées. Dans ce sens, la Cour de cassation affirme que : « *toute reproduction dans un écrit rendu public d'un texte déjà publié, est elle-même constitutive d'infraction* »[272]. L'infraction réalisée par l'acte de publication originel et sa reproduction postérieure sur un support de communication par voie de presse au public, constituent en conséquence des infractions successives. Il est toutefois nécessaire que le caractère délictueux de la reproduction se déduise de l'ensemble du contenu reproduit, le propos d'origine pouvant être accompagné d'une modération démontrant la bonne fois du relayeur.

Les infractions définies par la loi sur la liberté de la presse s'accordent ainsi aux nouvelles formes d'expression rencontrées sur les réseaux sociaux. Leurs éléments constitutifs sont parfaitement transposables à la communication rencontrée sur ces nouvelles plateformes d'échanges. L'expression massive permise par les réseaux sociaux en ligne entraîne par ailleurs un regain d'intérêt pour certains délits de presse qui étaient tombés en désuétude à l'image du délit de fausse nouvelle.

§2. Le regain d'intérêt du délit de fausse nouvelle

80. La désinformation sur les réseaux sociaux en ligne. Les réseaux sociaux en ligne ont pour effet de modifier certains équilibres au sein de la loi sur la liberté de la presse. En l'occurrence, des infractions tombées en désuétude résurgent avec l'émergence de la communication de masse sur les réseaux sociaux. C'est le cas particulièrement du délit de fausse nouvelle prévu à l'article 27 de la loi sur la liberté de la presse qui apparaît comme un outil susceptible d'appréhender la désinformation rencontrée sur les sites de réseaux sociaux. À ce titre, la fausse nouvelle, connue également sous l'anglicisme « *Fake news* », désigne dans son sens commun une information falsifiée ou mensongère émise par un média, un individu ou un groupe d'individus[273]. Elle peut également se définir comme « *toute allégation ou imputation d'un fait dépourvue d'éléments vérifiables de nature à la rendre*

[272] Crim. 2 octobre 2012, n° 12-80.419 : *Dr. pén.* 2012, n° 12, comm. 157, M. VERON ; Procédures n° 12, décembre 2012, comm. 373, J. BUISSON.
[273] D. GUINIER, « Cyberattaques. Macronleaks et diffusion de fausses informations », *Expertises des systèmes d'information*, juillet 2017, n° 426, p. 262.

vraisemblable »[274]. La diffusion de fausses informations n'est pas un phénomène nouveau, ces dernières appelées également « *faits alternatifs* » sont « *aussi anciennes que le gouvernement des hommes* »[275]. Elles trouvent cependant aujourd'hui une résonance particulière avec le développement des réseaux sociaux en ligne. Plusieurs facteurs expliquent cet attrait massif pour les fausses nouvelles. Les médias classiques et particulièrement la presse papier connaissent actuellement une crise profonde qui se manifeste par un ralentissement économique de leur activité[276] et par la méfiance grandissante du public à leur égard[277]. À l'inverse, internet devient une source grandissante d'information pour le public[278] alors que paradoxalement il constitue le média qui génère le plus de méfiance[279]. Plus généralement, l'extension du phénomène des fausses nouvelles particulièrement sur les sites de réseaux sociaux[280] s'explique également par l'entrée dans l'ère « *post-vérité* » qui fait référence « *à des circonstances dans lesquelles les faits objectifs ont moins d'influence pour*

[274] Définition donnée par Anne-Elisabeth Crédeville sur la base de l'avis consultatif du Conseil d'État sur la « Lutte contre les fausses informations » du 4 mai 2018. V. A.-E. CREDEVILLE, « Fausses nouvelles et nouvelles fausses : la réponse du droit », *Légipresse* n° 364, octobre 2018, p. 467.

[275] « L'histoire vraie des fausses nouvelles », Concordance des temps, France culture, émission du 1er avril 2017. <https://www.franceculture.fr/emissions/concordance-des-temps/lhistoire-vraie-des-fausses-nouvelles> (dernière consultation le 9 octobre 2019).

[276] Par exemple, aux États-Unis 60 % des emplois dans les médias ont disparus en près de 25 ans, soit 275 000 emplois. Sources : département américain du travail/ baromètre la Croix.
<http://www.lefigaro.fr/actualite-france/2017/03/06/01016-20170306ARTFIG00187-fake-news-un-meme-terme-pour-plusieurs-realites.php> (dernière consultation le 9 octobre 2019).

[277] En 2017, Seulement 24 % des Français estiment que les journalistes sont indépendants des pressions politiques et économique. Par ailleurs, la confiance des français dans les médias traditionnels baisse inexorablement : le journal et la télévision accusent une baisse importante de leur crédibilité, à 44% (-7 points) et 41% (-9 points). Pour plus d'un Français sur deux (55%), la télévision ne retranscrit pas fidèlement certains évènements d'actualité. Source : « baromètre la Croix 2017 de la confiance des français dans les médias », étude réalisée par Kantar Sofres.
<http://fr.kantar.com/m%C3%A9dias/digital/2017/barometre-2017-de-la-confiance-des-francais-dans-les-media> (dernière consultation le 9 octobre 2019).

[278] Internent est le moyen d'information principal de environ un quart des français, ce chiffre étant en hausse de 5 points. Sur internet, les sites et applications mobiles de la presse écrite et les réseaux sociaux prennent une importance grandissante : respectivement 22% (+7 points) et 9% (+6 points) des français en font leur moyen principal pour approfondir l'actualité. Source : « baromètre la Croix 2017 de la confiance des français dans les médias », étude réalisée par Kantar Sofres.
<http://fr.kantar.com/m%C3%A9dias/digital/2017/barometre-2017-de-la-confiance-des-francais-dans-les-media> (dernière consultation le 9 octobre 2019).

[279] 26% seulement des Français font confiance à l'information qu'ils relayent, et 52 % des français ne la juge pas crédible. Source : « baromètre la Croix 2017 de la confiance des français dans les médias », étude réalisée par Kantar Sofres.
<http://fr.kantar.com/m%C3%A9dias/digital/2017/barometre-2017-de-la-confiance-des-francais-dans-les-media> (dernière consultation le 9 octobre 2019).

[280] Parmis les utilisateurs des réseaux sociaux, 83 % ont répondu affirmativement à la question : « *Avez-vous déjà repéré des fausses nouvelles ou rumeurs sur les réseaux sociaux ?* ». Source : « baromètre la Croix 2017 de la confiance des français dans les médias », étude réalisée par Kantar Sofres.
<http://fr.kantar.com/m%C3%A9dias/digital/2017/barometre-2017-de-la-confiance-des-francais-dans-les-media> (dernière consultation le 9 octobre 2019).

modeler l'opinion publique que les appels à l'émotion et aux opinions personnelles »[281]. Mais surtout, ce qui autrefois relevait uniquement du pouvoir de la puissance publique à travers les services de propagande et de renseignements[282], relève aujourd'hui de la compétence d'acteurs privés avec l'émergence des médias de masse que sont les sites de réseaux sociaux[283].

81. La nécessité d'un délit de fausse nouvelle au regard du principe de liberté d'information. Le développement des fausses nouvelles sur les réseaux sociaux doit assurément être combattu dans la mesure où elles manifestent un danger certain pour nos sociétés, le jeu démocratique ne pouvant s'exercer correctement dès lors que les choix des individus sont conditionnés par des informations mensongères. Même si son impact réel sur les choix individuels demeure difficilement mesurable[284], la désinformation est devenue un outil visant à influencer les campagnes électorales, à l'image des élections présidentielles américaine[285] et française[286] de 2016. L'appréhension pénale de la diffusion de fausses

[281] Cette définition provient du dictionnaire d'Oxford qui a fait de la notion de « *post-vérité* » le mot international de l'année 2016. <https://en.oxforddictionaries.com/definition/post-truth> (dernière consultation le 9 octobre 2019).

[282] V. sur le sujet : R. JACQUARD, *La Guerre du mensonge. Histoire secrète de la désinformation*, Plon, 1986.

[283] Selon Monsieur Boris Barraud : « *La désinformation a opéré deux mutations. La première est quantitative : les phénomènes de désinformation ne sont plus des cas isolés, mais des parties pleines et entières du système de référence permettant à chacun de prendre des décisions faussement éclairées. La seconde est qualitative, et autrement dangereuse : auparavant, la désinformation était essentiellement utilisée à des fins de guerre psychologique ; désormais, elle est devenue un mal susceptible de ronger de l'intérieur une société ou, du moins, un outil utilisé par diverses puissances afin de modeler les opinions à leur image* », or, « *la démocratie n'a de sens que si les individus sont éclairés et n'opèrent pas leurs choix au hasard ou bien à l'aune de considérations fantaisistes ou de données erronées* ». B. BARRAUD, « La lutte contre les fausses informations sur internet : un jeu de lois », *RLDI*, 2018, n° 154.

[284] V. sur le sujet : D. CARDON, *Culture numérique*, Presses de Science Po, 2019, préc. chap. « Fake news panic : les nouveaux circuits de l'information », p. 261.

[285] V. I. FASSASSI, « Les effets des réseaux sociaux dans les campagnes électorales américaines », *Les nouveaux cahiers du Conseil constitutionnel*, octobre 2017, n° 57, p. 59-86 ; M. STEINKOLER, « Mar a Logos : L'élection de Trump et les *fake news* », *Savoirs et clinique*, 2017/2, n° 23, p. 23-33 : « *Selon un organisme de sondage très connu, sur l'ensemble des fausses nouvelles publiées dans les trois mois qui ont précédé l'élection, celles favorisant Trump ont été partagées trente millions de fois sur Facebook, tandis que celles favorisant Clinton ont été partagées huit millions de fois. Plus de la moitié de ceux qui se souviennent avoir pris connaissance de fausses nouvelles les ont crues* ». Par exemple, Le *Pizzagate* est une théorie qui tenta de mêler la candidate Hillary Clinton à un réseau de pédophilie pendant la campagne américaine de l'élection présidentielle de 2016. Cette théorie relayée sur les sites 4chan et Reddit prétendait que John Podesta, l'ancien directeur de campagne d'Hillary Clinton était impliqué dans un réseau de pédophilie en rapport notamment avec une pizzeria d'un quartier huppé de Washington. Source : « *Pizzagate: comment une folle rumeur a mêlé pédophilie et parti démocrate* », *lexpress.fr*, 7 décembre 2016.
<http://www.lexpress.fr/actualite/monde/amerique-nord/pizzagate-comment-une-folle-rumeur-a-mele-pedophilie-et-parti-democrate_1857478.html> (dernière consultation le 9 octobre 2019).

[286] Dans l'affaire des *Macronleaks* le mouvement politique « En Marche » fut la cible d'une cyberattaque une heure avant la fin officielle de la campagne électorale. Ces attaques ont consisté dans l'introduction de systèmes informatiques de l'équipe de campagne d'Emmanuel Macron et dans la diffusion de fausses informations. C'est ainsi que des dizaines de milliers de documents choisis par les hackers sont apparus sur les réseaux sociaux pour y être très largement propagés et ce, sans aucune garantie d'intégrité. Cette masse de donnée mise en ligne sur Archive.org et relayée sur le forum non modéré 4Chan révèle des échanges d'emails entre certains cadres et

nouvelles se révèle alors être un garde-fou nécessaire dans une société hyper médiatisée[287]. Il convient d'ailleurs de préciser que l'admission d'un délit de fausse nouvelle ne contrevient pas par nature à l'exercice de la liberté d'information. Effectivement, la liberté d'information est autant celle de l'émetteur qui est libre de diffuser toute information de quelque nature qu'elle soit, que celle du récepteur qui est en droit de recevoir des informations de qualité et notamment des informations vraies. Partant, l'instauration d'un délit visant à lutter contre les fausses informations n'entre pas en contradiction avec cette liberté et bien au contraire, la conforte[288]. Sur ce point, la diffusion de fausses nouvelles est prévue dans plusieurs textes d'incrimination du Code pénal sanctionnant l'hypothèse de la divulgation de « *fausses informations* » dans des cas spécifiques[289]. Il existe également différents droits spéciaux qui sanctionnent la diffusion de fausses nouvelles à l'image du Code monétaire et financier[290], du Code de commerce[291], du Code de la santé publique[292] et du Code électoral[293]. Mais surtout,

---

députés du mouvement mais également plusieurs fichiers .doc, .pdf et Excel dont certains contenants des informations liées à des dépenses de campagne. Ces milliers de documents ont été propagés sur les réseaux sociaux sans aucune garantie d'intégrité. Si certains d'entre eux n'ont subi aucune modification, d'autres ne disposaient d'aucune garantie d'intégrité et ont pu ainsi être modifiés voir, conçus de toute pièce. D. GUINIER, « Cyberattaques. Macronleaks et diffusion de fausses informations », *Expertises des systèmes d'information*, juillet 2017, n° 426, p. 262.

[287] C. LIENHARD « Catastrophe, diffusion de fausses nouvelles et diffamation », *D.* 2002 p. 2972.

[288] B. BARRAUD, « La lutte contre les fausses informations sur internet : un jeu de lois », *op. cit.*

[289] L'article 224-8 du Code pénal incrimine : « *le fait par quiconque, en communiquant une fausse information, de compromettre sciemment la sécurité d'un aéronef en vol ou d'un navire* » ; l'article 322-14 alinéa 1 prévoit quant à lui : « *le fait de communiquer ou de divulguer une fausse information dans le but de faire croire qu'une destruction, une dégradation ou une détérioration dangereuse pour les personnes va être ou a été commise* ». Le deuxième alinéa sanctionne : « *le fait de communiquer ou de divulguer une fausse information faisant croire à un sinistre et de nature à provoquer l'intervention inutile des secours* » ; Enfin, l'article 226-8 du Code pénal dispose : « *Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention* ».

[290] Le Code monétaire et financier utilise non pas la notion de fausse nouvelles mais davantage celle d'informations fausses ou trompeuses. L'article L. 465-3-1 du Code monétaire et financier fait référence au fait de donner « *des indications trompeuses sur l'offre, la demande ou le cours d'un instrument financier* », l'article L. 465-3-2 du même code sanctionne les « *informations qui donnent des indications fausses ou trompeuses sur la situation ou les perspectives d'un émetteur ou sur l'offre, la demande ou le cours d'un instrument financier* », enfin l'article L. 465-3-3 du Code monétaire et financier incrimine le fait « *de fournir ou de transmettre des données ou des informations fausses ou trompeuses utilisées pour calculer un indice de référence ou des informations de nature à fausser le cours d'un instrument financier ou d'un actif auquel est lié un tel indice* ». De manière générale le Code monétaire et financier n'incrimine de fausses informations que dans l'hypothèse où elles sont de nature à manipuler le marché ou d'influer sur les cours et les indices.

[291] Le Code de commerce sanctionne la diffusion de fausses nouvelles notamment à son article L. 443-2. Ce dernier puni le fait de diffuser « *des informations mensongères ou calomnieuses* » lorsqu'elles ont pour effet « *d'opérer la hausse ou la baisse artificielle soit du prix de biens ou de services, soit d'effets publics ou privés* ». Ici encore, l'information fausse doit être diffusée dans un but spécifique à savoir la hausse ou la baisse artificielle d'un prix.

[292] Selon l'article L. 2223-2 du Code de la santé publique « *Est puni de deux ans d'emprisonnement et de 30 000 euros d'amende le fait d'empêcher ou de tenter d'empêcher de pratiquer ou de s'informer sur une interruption volontaire de grossesse ou les actes préalables prévus par les articles L. 2212-3 à L. 2212-8 par tout moyen, y compris par voie électronique ou en ligne, notamment par la diffusion ou la transmission d'allégations ou d'indications de nature à induire intentionnellement en erreur, dans un but dissuasif, sur les caractéristiques ou les conséquences médicales d'une interruption volontaire de grossesse* ».

le droit pénal spécial de la presse dispose de sa propre infraction venant sanctionner la diffusion de fausses nouvelles à son article 27.

Or, les prévisions actuelles du délit de l'article 27 de la loi sur la liberté de la presse (A), mettent en évidence une nécessaire modernisation de l'appréhension des fausses nouvelles (B).

A. Les prévisions du délit de fausse nouvelle

82. Une double infraction. Le droit de la presse n'est pas sans voix face au phénomène des fausses nouvelles. L'infraction de l'article 27 de la loi du 29 juillet 1881 prévoit en réalité deux délits distincts. Le premier alinéa définit le délit de fausse nouvelle de nature à troubler la paix publique[294], l'alinéa second vient sanctionner le fait de diffuser une fausse nouvelle de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation[295]. L'infraction prévue à l'alinéa 1er du présent article sera étudiée en priorité en raison de son champ d'application disposant d'une portée plus générale. La rédaction actuelle de l'article 27 de la loi du 29 juillet 1881 est issue de la loi du 15 juin 2000 relative à la présomption d'innocence et aux droits des victimes qui a notamment supprimé les peines privatives de liberté encourues pour ces deux délits[296]. Depuis sa première apparition dans la législation de 1810, le délit de fausses nouvelles est l'un des délits de presse ayant subi le plus de modifications. Sa version actuelle se rapproche en grande partie de celle de l'ordonnance du 6 mai 1944 relative à la répression des délits de presse qui fit du délit de fausse nouvelle une infraction formelle et qui sanctionna « *la publication, la diffusion ou la reproduction* » d'une fausse nouvelle.

---

[293] L'article L. 97 du Code électoral dispose : « *Ceux qui, à l'aide de fausses nouvelles, bruits calomnieux ou autres manœuvres frauduleuses, auront surpris ou détourné des suffrages, déterminé un ou plusieurs électeurs à s'abstenir de voter, seront punis d'un emprisonnement d'un an et d'une amende de 15 000 euros* ». Ce dernier article ne manque pas d'intérêt au vu de l'utilisation actuelle des « *fake news* » sur les réseaux sociaux. Nombreux sont les exemples où des fausses nouvelles auraient été injectées dans le but d'influer sur le cours d'une élection. Concernant les *MacronLeaks* les poursuites initiales ouvertes par le parquet de Paris portaient notamment sur le chef du délit de fausses nouvelles en vue de détourner les suffrages prévu par l'article L. 97 du Code électoral.

[294] L. sur la liberté de la presse du 29 juillet 1881, art 27, al. 1er : « *la publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros* ».

[295] L. sur la liberté de la presse du 29 juillet 1881, art 27, al. 2nd : « *Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation* ».

[296] L. n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes, *JORF* n° 0138, 16 juin 2000, p. 9038.

83. La publicité de la fausse nouvelle. Les poursuites du délit de l'article 27 de la loi sur la liberté de la presse sont subordonnées à l'existence d'un élément de publicité. Pour être sanctionnée, la fausse nouvelle doit être communiquée au public. La simple conception du message n'est donc pas en soi répréhensible, seul le fait de le rendre public le devient. Toutefois, l'infraction de l'article 27 ne renvoie pas à l'article 23 de la loi concernant la détermination du caractère public. L'incrimination vise de manière large « *la publication, la diffusion ou la reproduction par quelque moyen que ce soit* » ce qui est peu contraignant[297]. Reste à dissocier la notion de fausse nouvelle (1), de la finalité de la fausse nouvelle (2).

1) La notion de fausse nouvelle

84. La distinction entre liberté d'opinion et fausse nouvelle. Le texte d'incrimination ne précisant pas la notion de nouvelle, la jurisprudence a dû venir apporter une définition. Selon elle, une nouvelle consiste dans l' « *annonce d'un évènement arrivé récemment, faite à quelqu'un qui n'en a pas encore connaissance* »[298]. Sur la base de cette définition, la nouvelle renvoie nécessairement à un fait d'actualité ce qui a pour conséquence d'exclure le récit d'un fait passé ou qui est du moins déjà connu du public[299]. La nouvelle porte alors sur « *l'annonce d'un fait précis et circonstancié, actuel ou passé, mais non encore divulgué* »[300]. Au final, « *la nature ancienne ou contemporaine de l'évènement est indifférente, ce qui compte c'est la primeur de la nouvelle* »[301]. Par exemple, des commentaires portant sur des faits antérieurement révélés ne peuvent tomber sous le coup de l'article 27 de la loi du 29 juillet 1881[302]. Aussi, l'annonce d'un fait futur, une prédiction ou un pronostic ne peuvent également être considérés comme des fausses nouvelles lorsqu'ils ne se fondent pas sur des données actuelles ou déterminées[303]. Au final, la doctrine considère la nouvelle comme « *une information brute et objective* »[304]. Il est alors d'une certaine importance de préciser que

[297] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 542, n° 897.
[298] Crim. 13 avril 1999, nº 98-83.798 : *Bull. crim.* nº 78 ; *Légipresse* 1999, n° 165, III, p. 141 ; *D.* 1999, p. 406, obs. T. MASSIS ; *D.* 1999, p. 126, obs. B. de LAMY ; *RSC* 2000, p. 203, obs. Y. MAYAUD.
[299] N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 16.
[300] Paris, 11ème ch., 18 mai 1988, n° 1988-025000 : *Gaz. Pal.* 1989, 1, note Domingo, p. 49. ; *D.* 1990, p. 35, note G. DROUOT.
[301] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, *op. cit.*, p. 540, n° 890.
[302] Crim. 13 avril 1999, nº 98-83.798 : *Bull. crim.* nº 78 ; *Légipresse* 1999, n° 165, III, p. 141 ; *D.* 1999, p. 406, obs. T. MASSIS ; *D.* 1999, p. 126, obs. B. de LAMY ; *RSC* 2000, p. 203, obs. Y. MAYAUD.
[303] Crim. 28 juin 1860 : DP 1860. 1. 293.
[304] E. DREYER, *Responsabilités civiles et pénales des médias*, Litec, 2008, p. 172, n° 345.

l'expression d'une simple opinion ne saurait constituer une fausse nouvelle[305]. De même, un simple commentaire tendancieux ne peut caractériser le délit de fausse nouvelle[306]. De manière générale, en aucun cas le délit de diffusion d'une fausse information ne concerne les jugements de valeur. Cela évite l'écueil de proposer un champ d'application qui outrepasserait les limites admissibles de la liberté d'expression. Il est en effet rappelé que le principe de la liberté d'expression « *vaut non seulement pour les informations ou idées accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'État ou une partie quelconque de la population* »[307].

85. Le caractère fallacieux de la nouvelle. Pour qu'une nouvelle soit fausse, cette dernière doit être « *mensongère, erronée ou inexacte dans la matérialité du fait et dans ses circonstances* »[308]. Seule importe donc la fausseté objective du fait et seuls sont retenus, les dires ou les écrits rapportant des éléments objectifs ou matériels[309]. La fausse information présente comme s'étant produit un évènement qui n'a pas eu lieu ou du moins, dont la réalité est difficilement vérifiable[310]. La tonalité générale de l'article peut aiguiller les juges sur le caractère fallacieux de la nouvelle qui se déduit de l'ensemble des éléments de l'information[311]. Les juges recherchent alors si les éléments erronés entachent d'inexactitude l'ensemble de la nouvelle : « *Face à un récit où des éléments véridiques et des éléments erronés se mêlent et coexistent, les juridictions constatent l'existence d'une nouvelle fausse, dès lors que la présentation du fait constitue un ensemble où le mensonge l'emporte. En revanche, le caractère mensonger de certains détails secondaires n'entache pas de fausseté la nouvelle, dès lors que ces détails restent d'une importance mineure et n'ont pas pour conséquence de transformer le sens ou la nature du fait relaté* »[312].

86. La connaissance du caractère fallacieux. L'auteur d'une fausse nouvelle n'est punissable que s'il a diffusé cette dernière de mauvaise foi. Il est, de jurisprudence constante, reconnu que la présomption de mauvaise foi existante pour le délit de diffamation ne peut être

[305] Selon la jurisprudence, des propos constituant une propagande politique « *fussent-ils mensongers, ne sont que l'expression d'une opinion et ne constituent pas une fausse nouvelle* ». Crim. 16 mars 1954 : *Bull. crim.*, n° 111 – Crim. 13 avril 1999, n° 98-83.798 : *Bull. crim.* n° 78 ; *Légipresse* 1999, n° 165, III, p. 141 ; *D.* 1999, p. 406, obs. T. MASSIS ; *D.* 1999, p. 126, obs. B. de LAMY ; *RSC* 2000, p. 203, obs. Y. MAYAUD.
[306] Y. MAYAUD, « Ne pas confondre : commentaires tendancieux et fausses nouvelles », *op. cit.*, n° 1, p. 203.
[307] CEDH, *Handyside c/ Royaume-Uni*, 7 décembre 1976, n° 5493/72, n° 24.
[308] Paris, 11ème ch., sect. A, 7 janvier 1998 : *Dr. pén.* 1998, comm. 63, obs. M. VERON.
[309] N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 18.
[310] B. BARRAUD, « La lutte contre les fausses informations sur internet : un jeu de lois », *RLDI*, 2018, n° 154.
[311] P. AUVRET, « fausses nouvelles », *J.-Cl.* Communication, fasc. 3210, 2003, n° 17.
[312] N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 19.

étendue aux autres délits de presse[313]. Dans l'absence d'une telle présomption, la preuve de la mauvaise foi ne saurait se déduire de la seule constatation de la fausseté de la nouvelle[314]. La négligence ou l'imprudence ne sont pas susceptibles de fonder une répression sur le fondement du délit de fausse nouvelle[315]. En conséquence, il n'y a pas de mauvaise foi lorsque l'on ne vérifie pas une information[316] ou lorsque les sources ne sont pas vérifiées[317]. La preuve de la mauvaise foi est donc difficile à établir, à moins que le prévenu ne reconnaisse lui-même avoir eu connaissance de la fausseté de l'information diffusée. La mauvaise foi est le plus souvent « *déduite des faits eux-mêmes, de leurs circonstances ou encore de la gravité de la faute considérée subjectivement* »[318]. La mauvaise foi et la fausseté de la nouvelle sont alors deux notions qui peuvent se trouver dans certains cas étroitement liées. Le juge peut se positionner sur la mauvaise foi du prévenu notamment au regard de sa profession qui peut être un élément indiquant l'intention de l'auteur. C'est ainsi que la Cour de cassation a approuvé les juges du fond d'avoir déduit la mauvaise foi de la profession de l'auteur qui était journaliste depuis quinze ans. La haute juridiction a considéré que le prévenu, de par sa qualité de journaliste, était plus à même de vérifier et filtrer les renseignements qu'il avait par la suite réutilisés[319].

87. La répression de la reproduction d'une fausse nouvelle. L'article 27 de la loi du 29 juillet 1881 punit la reproduction au même titre que la publication de la fausse nouvelle. En conséquence, tant l'auteur initial de la fausse nouvelle que celui qui la relaye peuvent se voir poursuivre de ce chef. Cette possibilité apparaît cependant entrer en contradiction avec l'exigence posée par la jurisprudence que le fait constitutif de la fausse n'ait pas été encore divulgué ou révélé[320]. Certains auteurs s'accordent alors à dire que cette exigence posée par la jurisprudence n'est plus en phase avec les nouveaux moyens de communication, en particulier

[313] V. notamment : Crim., 16 mars 1950 : *Bull. crim.*, n° 100 – Crim., 28 avril 1950 : *Bull. crim.*, n° 137 – Crim., 21 juillet 1953 : *Bull. crim.*, n° 254 ; *RSC* 1954, p. 368, obs. L. HUGUENEY – Crim., 12 décembre 1957 : *Bull. crim.* n° 837 – Crim., 11 mars 1965 : *Bull. crim.*, n° 77.
[314] Paris, 11ème ch., sect. A, 7 janvier 1998 : *Dr. pén.* 1998, comm. 63, obs. M. VERON.
[315] Ceci permet de distinguer la « *fake news* » de la « *false news* ». La première désigne une information falsifiée ou mensongère alors que la deuxième relève de ce qui est seulement erroné. V. D. GUINIER, « Cyberattaques. Macronleaks et diffusion de fausses informations », *Expertises des systèmes d'information*, juillet 2017, n° 426, p. 262.
[316] Crim., 19 mars 1953 : *Bull. crim.* 1953, n° 100 ; *D.* 1953, n° 390.
[317] Crim., 12 décembre 1957 : *Bull. crim.* 1957, n° 837.
[318] N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 26.
[319] Crim., 18 décembre 1962 : *Bull. crim.*, n° 380.
[320] Par exemple : les juges du fond ont infirmé la caractérisation du délit de fausse nouvelle, notamment parce que le tract poursuivi ne faisait que reprendre une information pérue dans un titre de presse quotidienne régionale quelques jours auparavant. Paris, 7 janvier 1998 : *Légipresse* 1998, n° 157 ; *Légipresse* 2017 n° 352, chron. G. SAUVAGE, p. 428.

les réseaux sociaux en ligne, et doit être abandonnée[321]. Le relayeur d'une fausse nouvelle ne pourra cependant être poursuivi que s'il réunit l'ensemble des éléments constitutifs du délit de l'article 27 y compris l'élément intentionnel exigeant sa mauvaise foi. Cette solution garantit une certaine sécurité juridique dans la mesure où elle prévient d'une extension démesurée du champ d'application de l'infraction de diffusion d'une fausse nouvelle. Seuls le diffuseur initial de la fausse nouvelle et les relayeurs agissant de mauvaise foi peuvent se voir poursuivre sur ce fondement excluant ainsi du champ répressif toute personne qui relayerait la fausse nouvelle de bonne foi. L'élément intentionnel pourrait en l'occurrence se déduire de la personne du relayeur, notamment si ce dernier agit à titre professionnel comme journaliste, homme politique ou influenceur.

2) La finalité de la fausse nouvelle

88. La notion de trouble à la paix publique. Au nom de la liberté d'expression, le droit pénal ne réprime la rumeur, dans sa dimension d'alarme, qu'à condition d'une atteinte grave à un intérêt public ou privé. La sanction pénale n'est donc pas motivée par l'absence de vérité d'un propos mais par le but poursuivi par l'auteur d'un message volontairement erroné, la vérité étant une notion difficile à saisir, voire inexistante. Autrement dit, le mensonge n'est pénalement sanctionné que s'il est commis dans un but précis. Le mensonge ne constitue dès lors que le moyen d'atteindre une valeur qui elle est socialement protégée. En l'occurrence, l'article 27 de la loi sur la liberté de la presse exige que la propagation de l'information fausse ait troublé ou soit de nature à troubler la paix publique. La répression sur ce fondement est donc indifférente lorsque la fausse nouvelle se contente uniquement de troubler des intérêts particuliers[322]. Le trouble à la paix publique signifie que la nouvelle en cause doit être de nature à « *porter atteinte à l'ordre public, si bien qu'il eût été nécessaire de faire intervenir la force publique pour la rétablir* »[323]. Ont ainsi été considérés comme troublant la paix publique « *des désordres, des mouvements de panique, ou du moins des inquiétudes graves, des émotions collectives* »[324]. Les juges du fond ont en ce sens rappelé qu'une fausse nouvelle n'est punissable que si « *elle contient par son objet un ferment de trouble public, c'est-à-dire*

[321] V. en ce sens : G. SAUVAGE, « Quel(s) outil(s) juridique(s) contre la diffusion de "*fake news*" », *Légipresse*, n° 352, septembre 2017, p. 431 ; B. BARRAUD, « La lutte contre les fausses informations sur internet : un jeu de lois », *RLDI*, 2018, n° 154.
[322] Ceci est cependant différent dans l'hypothèse où, « *à travers une personne privée, l'auteur de la fausse nouvelle a entendu impressionner le public et créer un trouble à la paix publique tel que défini précédemment* », N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 39.
[323] Crim., 22 décembre 1955 : *Bull. crim.*, n° 596.
[324] R. MERLE et A. VITU, *Traité de droit criminel, Droit pénal spécial*, Cujas, 1982, p. 1240, n° 1572.

de désordre, de panique, d'émotion collective, de désarroi »[325]. Des informations économiques erronées sont à cet égard susceptibles de former un trouble à la paix publique dans la mesure où elles auraient suscité une panique causant un désordre sur la voie publique[326]. Si un trouble à la paix publique sous-tend des conséquences ayant une certaine gravité, la Cour de cassation n'hésite pas à adopter une conception large de la notion de paix publique[327], la chambre criminelle ayant confirmé qu'une fausse nouvelle de nature à troubler les relations internationales peut constituer une fausse nouvelle au sens de l'article 27 de la loi du 29 juillet 1881[328].

89. Au final, tous les aspects de la désinformation ne peuvent être sanctionnés pénalement. La seule difficulté de reconnaître une vérité absolue invite à la prudence dans la sanction d'une fausse nouvelle. Les personnes qui communiquent les informations doivent bénéficier d'une marge d'appréciation assez grande pour que leur liberté d'expression soit assurée. C'est pourquoi, seules les informations erronées revêtant un certain degré de gravité sont concernées par le texte d'incrimination. Il n'apparaît ainsi pas pertinent d'inclure dans le champ répressif les fausses nouvelles à visée satirique dont sont inondés les réseaux sociaux à l'image des sites de désinformation tels que le « *Gorafi* »[329] ou encore « *Nordpress* »[330]. Ce type de désinformation étant rentré dans les mœurs ne peut susciter de trouble à la paix publique.

90. En outre, l'infraction de diffusion de fausse nouvelle sanctionne non seulement la fausse nouvelle qui a effectivement troublé la paix publique mais également celle qui ne l'a qu'éventuellement perturbée[331]. Aussi, il n'est pas nécessaire que la diffusion de l'information soit une véritable conséquence sur la paix publique, il suffit qu'elle soit susceptible d'atteindre le but recherché par son auteur[332]. Il n'est donc pas exigé de la partie poursuivante que cette dernière démontre un trouble effectif à l'ordre public pour caractériser le délit de fausse nouvelle. Pour autant, l'existence ou la matérialité du trouble ne doit pas être envisagée

---

[325] Paris, 11ème ch., sect. A, 7 janvier 1998 : *Dr. pén.* 1998, comm. 63, obs. M. VERON.
[326] P. AUVRET, « Fausses nouvelles », *J.-Cl.* Comm., fasc. 3210, 2003, n° 28.
[327] N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 37.
[328] Durant la guerre d'Algérie, un journal avait annoncé qu'une base française située à Marrakech servait de point de départ pour des bombardements en Algérie en violation de l'engagement pris à l'égard du gouvernement marocain. Selon les juges, cette nouvelle était susceptible de compromettre les rapports entre les deux pays et caractérisait le délit de l'article 27 de la loi sur la presse. Crim., 7 novembre 1963, *Bull. crim.*, n° 314, *JCP* G 1963, IV, p. 171.
[329] <http://www.legorafi.fr>
[330] <http://nordpresse.be>
[331] P. AUVRET, « fausses nouvelles », *J.-Cl.* Comm., fasc. n° 3210, 2003, n° 25.
[332] Crim., 26 juin 1968 : *Bull. crim.*, n° 210.

de manière abstraite[333]. Le trouble existant ou seulement virtuel s'apprécie *in concreto* en fonction des données propres à chaque situation. C'est ainsi que dans une affaire où un faux reportage photo laissait penser qu'une « *chasse aux flics* » était lancée dans les banlieues, les juges déduisirent par une analyse *in concreto* l'existence d'un potentiel trouble à la paix publique caractérisant le délit de fausse nouvelle[334]. En définitive, le délit de l'article 27 de la loi sur la liberté de la presse constitue depuis l'ordonnance du 6 mai 1944 une infraction formelle qui se caractérise par un potentiel trouble et non plus uniquement par un trouble effectif à la paix publique.

91. Étendue de l'intention coupable, un nécessaire dol spécial. L'intention coupable se déduit non seulement de la connaissance du caractère erroné de la nouvelle mais également de la volonté particulière chez l'auteur de troubler la paix publique, d'ébranler la discipline ou le moral des armées ou encore d'entraver l'effort de guerre de la nation. Il s'agit, en d'autres termes, de déterminer si l'infraction de diffusion de fausse nouvelle exige aussi un dol spécial chez son auteur pour être constituée. La doctrine se montre divisée sur le sujet. Pour certains auteurs[335] l'infraction prévue à l'article 27 de la loi sur la liberté de la presse exige un dol général, l'auteur doit avoir conscience de publier une fausse nouvelle, auquel s'ajoute un dol spécial qui consiste à avoir la volonté de troubler la paix publique, d'ébranler la discipline ou le moral des armées ou encore d'entraver l'effort de guerre de la nation. Cette position doctrinale est appuyée par deux jurisprudences. La chambre criminelle de la Cour de cassation est venue affirmer que la mauvaise foi « *se caractérise par la connaissance tant de la fausseté du fait publié, que du trouble qui pouvait en résulter* »[336]. Par ailleurs, selon les juges du fond : « *en l'absence de toute présomption légale, la preuve doit être apportée que le prévenu avait connaissance, tant de la fausseté du fait publié, que du trouble qui pouvait résulter de cette publication pour la paix publique* »[337]. Le dol spécial ne peut cependant pas se satisfaire de la seule conscience de troubler la paix publique, sa démonstration implique également la volonté chez l'auteur de la fausse nouvelle d'arriver à ce résultat.

---

[333] N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 40.

[334] En l'espèce, les jugent ont relevé afin de prouver le trouble à la paix publique que « *cet article laissant apparaître un climat d'insécurité particulièrement inquiétant a conduit l'autorité municipale, pour apaiser les craintes et ramener la paix publique, à diffuser un tract sur l'ensemble de la commune* ». Les juges en déduisent que « *la vivacité et l'immédiateté de la réaction traduisent de manière flagrante le trouble porté à la paix publique* ». TGI Nanterre, 13 décembre 2000 : *CCE*, février 2001, n° 19, obs. A. LEPAGE : « *L'article de M. A. D. C. est bien une fausse nouvelle établie sur la base de pièces entièrement fabriquées donnant l'illusion d'un véritable reportage rapportant une scène qui en définitive n'a jamais existé pour faire croire aux lecteurs que "la chasse aux flics" est lancée dans les banlieues parisiennes par des jeunes emplis de haine* ».

[335] V. en ce sens, C. DEBBASCH (dir.), *Droit des médias*, Dalloz, 2002, p. 873, n° 2693.

[336] Crim., 21 juillet 1953 : *Bull. crim.*, n° 254 ; *RSC* 1954, p. 368, obs. L. HUGUENEY.

[337] Paris, 4 novembre 1964 : *D.* 1965, somm. p. 35.

92. L'exigence d'un dol spécial ne fait cependant pas l'unanimité au sein de la doctrine. Une partie des auteurs considère que ces décisions jurisprudentielles se méprennent sur l'esprit du texte[338]. Cette position s'explique par le fait que, dans la majorité des cas, la connaissance de la fausseté de la nouvelle ne fait que traduire une intention de nuire. Il a été affirmé en ce sens que « *en établissant que l'agent a eu conscience de publier un message inexact, se trouve démontrée sa volonté de causer à l'ordre public le résultat spécial (le trouble) qui pouvait être la conséquence de la propagation de la fausse nouvelle* »[339]. Cependant, réduire l'élément intentionnel du présent délit au seul dol général est de nature à lui conférer un champ d'application trop large. La répression d'une fausse nouvelle est en effet délicat du point de vue de la liberté d'expression et du débat démocratique. Seule la démonstration d'une réelle volonté de causer un trouble au sein de la société par la diffusion d'une fausse nouvelle doit demeurer répréhensible. Ce principe a été réaffirmé par le tribunal correctionnel de Toulouse[340] suite à la diffusion de fausses nouvelles concernant la cause de l'explosion de l'usine AZF le 21 septembre 2001[341]. Le juge pénal avait déduit de l'ensemble des éléments qui lui étaient rapportés[342] que la démonstration de la volonté de diffusion de fausse nouvelle n'était pas faite, faute de dol spécial consacrant ainsi un « *droit de douter avec discernement* »[343]. En définitive, la seule fausse nouvelle ne suffit pas à caractériser le délit de l'article 27 de la loi sur la liberté de la presse, cette dernière n'étant que l'instrument de l'atteinte.

B. Une modernisation de l'appréhension des fausses nouvelles

93. La désuétude de l'article 27 remise en cause. Le délit de fausse nouvelle n'a jamais été une infraction phare de la loi sur la liberté de la presse à l'inverse des délits de

[338] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 544, n° 898.
[339] *Ibid*.
[340] TC Toulouse, 27 juin 2002 : *D.* 2002 p. 2972, comm. C. LIENHARD.
[341] En l'occurrence, les poursuites visaient des journalistes et deux directeurs de publication à savoir celui du quotidien *le Figaro* et celui de l'hebdomadaire *Valeurs Actuelles*. Les poursuites concernaient des articles publiés entre le 28 septembre 2001 et le 5 octobre 2001, peu de jours après la catastrophe. Les articles en question tendaient notamment à accréditer la piste d'un attentat islamiste et mettaient directement en cause, en le nommant, un ressortissant français d'origine tunisienne décédé dans l'explosion, mais aussi sa compagne et une association de français musulmans ainsi que son dirigeant. V. C. LIENHARD, « Catastrophe, diffusion de fausses nouvelles et diffamation », *D.* 2002, p. 2972.
[342] Le tribunat avait notamment retenu que les faits d'actualité en cause avaient été publiés dans un temps très voisin de la catastrophe. Il n'y avait en conséquence, pas assez d'éléments objectifs au moment de la publication pour écarter irrémédiablement la piste de l'attentat qui n'était à ce moment qu'une piste parallèle à l'enquête officielle. D'autant plus que la piste de l'attentat avait été également avancée antérieurement par d'autres médias dont *Le Journal Suisse, Le Matin, Le Parisien, La Croix et Le Monde*. V. C. LIENHARD, « Catastrophe, diffusion de fausses nouvelles et diffamation », *op. cit.*, p. 2972.
[343] C. LIENHARD, « Catastrophe, diffusion de fausses nouvelles et diffamation », *op. cit.*, p. 2972.

diffamation, d'injure ou encore de provocation. Le chef de poursuite du délit de fausse nouvelle a d'ailleurs été relativement peu utilisé par la jurisprudence[344] posant un problème d'effectivité de la norme. La doctrine s'accorde à dire que ce délit est « *très rarement utilisé* »[345], le juge pénal lui préférant d'autres qualifications pénales[346]. Le législateur avait même imaginé supprimer ce délit des prévisions de la loi du 29 juillet 1881 pour au final le laisser dans le corps du texte[347]. Cette sagesse du législateur fait écho aux paroles de Jean Carbonnier selon lequel : « *L'inapplication n'a pas forcément ici le sens d'un échec, justifiant condamnation, abrogation immédiate, car elle peut tenir, et elle tiendra même généralement, à ce que l'intérêt en vue duquel la loi a été conçue, bien que parfaitement réalisable, ne s'est pas encore trouvé réalisé dans les faits* »[348]. Dans cette hypothèse, la simple disponibilité de la loi, et non plus sa réelle application, devient garante de son effectivité. D'autant plus que dans le domaine pénal, l'absence de poursuites peut se justifier par l'appréhension que suscite la sanction. L'application limitée du délit de fausse nouvelle ne semble toutefois pas s'expliquer par la crainte de la peine encourue en raison de son faible *quantum*[349]. En réalité, le manque d'application du délit de fausse nouvelle questionne davantage sur sa désuétude que sur son effectivité. La désuétude peut se définir comme « *l'inapplication prolongée d'une règle de droit* »[350] ou dans un sens similaire comme « *l'état de non application d'une règle* »[351]. Cette situation est, au vu du phénomène des « *Fake news* » présent sur les sites de réseaux sociaux, de nature à changer. L'infraction de diffusion de fausse nouvelle apparaît en effet comme un outil capable de répondre à la pratique contemporaine des « *Fake news* ». À

[344] Sur une recherche Légifrance associant les expressions : « *fausse nouvelle* » et « *article 27* » présentent dans le texte intégral et sans restriction de dates, seuls 7 résultats apparaissent dont le dernier datant du 13 avril 1999 (Crim. ,13 avril 1999, n° 98-83.798).

[345] C. BIGOT, *Connaître la loi de 1881 sur la presse*, PUF, 2004, p. 115. V. également en ce sens : D. KURI, « L'hypothèse des délits de presse désuets », *in* N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, Coll. Grands Colloques, 2017, p. 66.

[346] Lorsque la fausse nouvelle est de nature diffamatoire ou injurieuse les poursuites se feront alors sous les chefs d'inculpation des délits de diffamation et d'injure (article 29 de la loi sur la liberté de la presse) dont l'usage et la jurisprudence sont extrêmement développés. Par ailleurs, dans l'affaire des *MacronLeaks*, l'enquête préliminaire, ouverte le 4 mai par le parquet de Paris et confiée à la Brigade de répression de la délinquance contre la personne (BRDP), portait sur les chefs suivants : le délit de fausses nouvelles en vue de détourner les suffrages (article L. 97 du Code électoral), faux, usage de faux et recel de faux (articles 441-1 et suivants du Code pénal). D. GUINIER, « Cyberattaques. Macronleaks et diffusion de fausses informations », *Expertises des systèmes d'information*, juillet 2017, n° 426, p. 266.

[347] L'infraction de l'article 27 de la loi sur la presse subit nombre de critiques et fut difficile à admettre pour le législateur de 1881. Certains y virent notamment « *un délit de tendance* » : N. DEFFAINS, J.-B. THIERRY, Rép. pén. Dalloz, juillet 2015, *V°* Fausse nouvelle, n° 4 ; d'autres comme J. SIMON et É. de GIRARDIN combattirent pour la suppression de cette disposition : v. P. MIMIN, obs. *D.* 1946. 2.

[348] J. CARBONNIER, *Flexible droit, pour une sociologie du droit sans rigueur*, LGDJ, 10ème Éd., 2001, p. 138.

[349] La loi sur la presse ne prévoit pas de peine d'emprisonnement mais une simple amende pour ce délit : à savoir une amende de 45 000 euros pour l'infraction de l'alinéa 1er et une amende de 135 000 euros pour l'infraction de l'alinéa 2nd.

[350] R. CABRILLAC, *Dictionnaire du vocabulaire juridique*, Litec, 9e éd., 2018, *V°* Désuétude.

[351] Association H. CAPITANT, *Vocabulaire juridique*, G. CORNU (dir.), PUF, 12ème éd., 2018, *V°* Désuétude.

défaut de récentes applications jurisprudentielles, le regain d'intérêt du délit de fausse nouvelle s'observe pour l'heure principalement d'un point de vue théorique. Une réutilisation de ce délit dans la pratique pourrait résulter d'une réécriture du délit de diffusion de fausse nouvelle (2). Cette piste de réforme semble justifiée au regard de l'utilité nuancée des nouvelles formes de luttes contre les fausses nouvelles (1).

1) L'utilité nuancée des nouvelles formes de lutte contre les fausses nouvelles

94. Proposition de loi créant un nouveau délit. Malgré l'existence du délit de fausse nouvelle dans la loi sur la liberté de la presse, une proposition de loi visant à « *définir et sanctionner les fausses nouvelles ou "fake news"* » a été déposée devant le Sénat le 22 mars 2017[352]. Cette proposition qui n'a finalement pas abouti suggérait notamment l'insertion d'un nouveau délit dans le Code pénal prévoyant dans une formulation très générale de sanctionner la diffusion d'une fausse nouvelle « *lorsque la publication est de nature à tromper et influencer directement le public à agir en conséquence et que sa mise à disposition a été faite de mauvaise foi* »[353]. L'adoption d'une telle disposition aurait cependant contribué encore davantage au mouvement de déspécialisation du droit de la presse. Ceci est vivement critiquable d'autant plus que cette infraction ressemble à s'y méprendre aux prévisions actuelles de l'article 27 de la loi sur la liberté de la presse. Ainsi, la proposition de loi exigeait une « *mise à disposition du public par voie numérique par édition, diffusion, reproduction, référencement ou par quelque moyen que ce soit* » ce qui revient sensiblement au même résultat que le délit de l'article 27 de la loi du 29 juillet 1881.

95. Une nouvelle procédure de recours en référé. Finalement, le législateur a choisi par la loi n° 2018-1202 du 22 décembre 2018[354] d'introduire une nouvelle procédure de recours en référé durant la période électorale à l'article L163-2 du Code électoral. Selon cette nouvelle procédure, le juge des référés peut être saisi pour faire cesser la diffusion d'informations dont il est manifeste qu'elles sont inexactes ou trompeuses et de nature à altérer la sincérité du scrutin. Ces informations doivent en outre avoir été diffusées de manière

[352] Sénat, session ordinaire de 2016-2017, n° 470, Proposition de loi visant à définir et sanctionner les fausses nouvelles ou « fake news », Présentée par Mme le sénateur N. GOULET, le 22 mars 2017.
[353] Le législateur prévoyait de rédiger l'article 226-12-1 du Code pénal comme suit : « *La mise à disposition du public par voie numérique par édition, diffusion, reproduction, référencement ou par quelque moyen que ce soit, de nouvelles fausses non accompagnées des réserves nécessaires est punie d'un an d'emprisonnement avec sursis et de 15 000 € d'amende lorsque la publication est de nature à tromper et influencer directement le public à agir en conséquence et que sa mise à disposition a été faite de mauvaise foi. La nouvelle est l'annonce de faits précis et circonstanciés, actuels ou passés faite à un public qui n'en a pas encore connaissance* ».
[354] L. n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, *JORF* n° 0297, 23 décembre 2018, art. 1.

délibérée, artificielle ou automatisée et massive, par le biais d'un service de communication au public en ligne. Le juge des référés peut être saisi dans le cadre de cette procédure par le ministère public, tout candidat, tout parti ou groupement politique ou toute personne ayant intérêt à agir, « *pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises* ». Ce texte impose au juge des référés de déterminer, dans un court délai de 48 heures, l'existence d'une inexactitude ou d'une tromperie sur la base d'une saisine justifiée par des allégations ou imputations susceptibles d'être « *inexactes ou trompeuses* ». La présente procédure présente cependant l'inconvénient majeur de se centrer davantage sur la véracité de l'allégation qui lui est soumise que sur sa potentielle influence sur le scrutin. Si le juge des référés est le juge de l'évidence, la vérité ne relève pour sa part pas naturellement de l'évidence surtout en période électorale. La preuve négative est particulièrement difficile à rapporter surtout lorsque l'allégation attaquée est un fait purement inventé[355] ou lorsqu'elle résulte d'une interprétation subjective d'un fait ayant réellement eu lieu[356].

[355] A.-E. CREDEVILLE, « Fausses nouvelles et nouvelles fausses : la réponse du droit », *Légipresse* n° 364, octobre 2018, p. 468-469.

[356] Une première application de la procédure de référé de l'article L163-2 du Code électoral a été réalisée par le Tribunal de grande instance de Paris le 17 mai 2019 (TGI Paris, 17 mai 2019, n° 19/53935). L'affaire concernait un tweet envoyé par le ministre de l'intérieur Christophe Castaner renvoyant à l'introduction de manifestants à l'hôpital de la Pitié-Salpêtrière. Le tweet diffusé le 1er mai 2019 était ainsi rédigé : « *Ici, à la Pitié-Salpêtrière, on a attaqué un hôpital. On a agressé son personnel soignant. Et on a blessé un policier mobilisé pour le protéger. Indéfectible soutien à nos forces de l'ordre : elles sont la fierté de la République* ». S'appuyant sur la loi fausse information, les deux élus ont saisi le 10 mai le tribunal de grande instance de Paris en référé pour demander à Twitter France le retrait de ce tweet. La décision ne fut rendue que sept jours plus tard par le tribunal. Le Les juges ont d'abord cherché à établir le caractère inexact ou trompeur des allégations contenues dans le tweet. En s'appuyant sur plusieurs articles de presse produits par les parties, le tribunal a considéré « *que, si le message rédigé par monsieur Christophe Castaner apparaît exagéré en ce qu'il évoque le terme d'attaque et de blessures, cette exagération porte sur des faits qui, eux, sont réels, à savoir l'intrusion de manifestants dans l'enceinte de l'hôpital de la Pitié-Salpêtrière le 1er mai 2019* ». L'information n'est donc pas dénuée de tout lien avec des faits réels et l'allégation n'est pas « *manifestement inexacte ou trompeuse* ». Ensuite, le tribunal a considéré que la diffusion doit également être cumulativement « *massive, artificielle ou automatisée, et délibérée, et opérer sur un service de communication au public en ligne* ». Les juges ont retenus qu'il ne s'agissait pas d'une diffusion automatisée ou artificielle donc selon eux ce critère manquait également. Cependant il aurait pu avoir une autre lecture du texte, notamment en retenant que les critères n'étaient pas cumulatifs. Enfin, le juge des référés doit apprécier le caractère manifeste du risque d'altération de la sincérité du scrutin. En l'occurrence le scrutin concerné était les élections européennes du 26 mai dernier. Selon le tribunal, « *si le tweet a pu employer des termes exagérés, il n'a pas occulté le débat, puisqu'il a été immédiatement contesté* », « *permettant à chaque électeur de se faire une opinion éclairée, sans risque manifeste de manipulation* ». En définitive, selon les juges du fond les conditions n'étaient pas remplies ne permettant pas de faire valoir le retrait du tweet. Cette affaire démontre les limites de la procédure de référé concernant l'appréhension juridique des fausses nouvelles. En effet, d'une part la décision du tribunal n'est intervenue que sept jours après la diffusion du tweet, donc bien au-delà du délai de 48 heures imposé par la loi. D'autre part, les difficultés entourant la détermination du caractère fallacieux de la nouvelle et son réel impact au sein de la société s'accord mal avec la nécessaire célérité de la procédure de référé. P. JANUEL et M. BABONNEAU, « Loi Fake news : première application du référé », *D. actu.*, 21 mai 2019.

Le choix d'une modernisation de l'appréhension pénale de la diffusion de fausses nouvelles par une réadaptation du délit existant de l'article 27 de la loi du 29 juillet 1881 paraît alors justifié.

2) Une nécessaire réécriture du délit de diffusion de fausse nouvelle

96. Le caractère trop restrictif de la notion de trouble à la paix publique. Actuellement, le trouble à la paix publique est essentiellement constaté face à des nouvelles de nature politique, diffusées dans des contextes sociaux conflictuels et susceptibles d'alarmer les citoyens les uns contre les autres ou de troubler les relations internationales[357]. Si la notion de trouble à la paix publique est potentiellement très large, la jurisprudence l'a malgré cela restreinte à des hypothèses très particulières assimilant le trouble à la paix publique à « *l'ordre de la rue* » et à « *la concorde des citoyens* »[358] privilégiant la protection de l'exercice de la liberté d'expression[359]. Cependant, la notion et l'interprétation actuelle du trouble à la paix publique n'est pas en mesure de répondre entièrement aux nouveaux défis suscités par la pratique à grande échelle de la désinformation sur les réseaux sociaux, si bien qu'il conviendrait de moderniser cette notion de manière à redonner à l'incrimination de l'article 27 de la loi du 29 juillet 1881 une effectivité circonstanciée. Cette solution aurait la vertu de laisser le présent délit dans le giron protecteur de la loi sur la liberté de la presse et éviterait ainsi de l'inscrire dans un champ excessivement répressif au sein du Code pénal[360].

97. Première solution : élargir l'interprétation jurisprudentielle de la notion de trouble à la paix publique. L'article 27 de la loi sur la liberté de la presse évite un premier écueil, celui d'un champ d'application trop spécifique à l'image des autres délits existants venant incriminer la diffusion d'une fausse nouvelle[361]. Cependant la notion de trouble à la paix publique, potentiellement large, est interprétée de façon trop restreinte par la jurisprudence conférant à ce délit un faible champ d'application. Une première solution pourrait consister à conserver la rédaction actuelle du délit de l'article 27 de la loi sur la presse mais à faire évoluer l'interprétation jurisprudentielle de la notion de trouble à la paix

[357] N. MALLET-POUJOL, « Rumeur et liberté d'expression : entre mensonge et vérité », *Légipresse* n° 364, octobre 2018, p. 484.
[358] B. BARRAUD, « La lutte contre les fausses informations sur internet : un jeu de lois », *RLDI*, 2018, n° 154.
[359] Selon la Cour de cassation : « *La liberté d'expression est un droit dont l'exercice ne revêt un caractère abusif que dans les cas spécialement déterminés par la loi, et que les propos reproduits, fûssent-ils mensongers, n'entrent dans aucun de ces cas* ». Civ. 1ère, 10 avril 2013, n° 12 10.177.
[360] G. SAUVAGE, « Quel(s) outil(s) juridique(s) contre la diffusion de "*fake news*" », *Légipresse*, n° 352, septembre 2017, p. 431.
[361] V. *supra* n° 81.

publique[362]. Une interprétation plus contemporaine du trouble à la paix publique s'analyserait alors comme une influence d'une fausse nouvelle sur la politique ou l'économie d'un pays ou d'une région dans son ensemble[363]. Néanmoins, reconnaître qu'une fausse nouvelle visant à influencer un scrutin électoral est de nature à troubler la paix publique romprait avec l'exigence de tranquillité et de sécurité publique associée à cette notion. En pareille hypothèse la paix publique ne serait plus seulement assimilée à une absence de panique, d'émotion collective ou de désarroi[364]. Cela contribuerait toutefois à étirer de façon outrancière la notion de paix publique au risque de la vider de tout sens.

98. Seconde solution : réécrire l'article 27 de la loi sur la liberté de la presse. Il est dans ce cas préférable d'utiliser le droit pénal existant et plus précisément, de réadapter l'infraction de l'article 27 de la loi sur la liberté de la presse tombée en désuétude en la reformulant de manière plus contemporaine. La réécriture de l'article 27 implique alors de prévoir d'autres finalités répressives que celle du trouble à la paix publique de manière à étendre le champ d'application du texte d'incrimination. En l'espèce, il serait opportun d'introduire au sein du texte d'incrimination la notion « *d'ordre politique* »[365] qui doit être entendu comme « *l'ensemble des structures constitutionnelles et administratives dont un État se dote pour organiser la vie de la nation et permettre aux habitants de développer dans le calme et la* ***confiance*** *leurs activités individuelles ou collectives* »[366]. L'ordre politique vise donc à éviter une déstructuration et une décomposition de la société. Cette notion présente l'avantage considérable qu'elle peut « *se modifier au fil du temps, s'adapter aux circonstances nouvelles nées de l'évolution des techniques ou des changements des mentalités ou des régimes* »[367]. L'ajout de cette notion permettrait d'étendre le champ répressif de l'incrimination à de nouveaux comportements tout en respectant le principe de légalité de la loi pénale en raison de la précision et de la prévisibilité de la notion d'ordre politique. Cette évolution législative permet en définitive de proposer une incrimination de diffusion d'une fausse nouvelle à portée générale mais circonscrite dans un cadre définitionnel bien établi et surtout, demeurant dans le cadre protecteur de la loi sur la liberté de la presse.

99. Proposition de réécriture. Ainsi, l'article 27 de la loi sur la liberté de la presse pourrait dès lors être rédigé de la manière suivante :

[362] G. SAUVAGE, « Quel(s) outil(s) juridique(s) contre la diffusion de "*fake news*" », *op. cit.*, p. 431.
[363] V. sur ce point : M. MENDRAS, « *From Moscow … With Fake News !*" », *Esprit*, juin 2017, n° 6, p. 17.
[364] Paris, 7 janvier 1988 : *Dr. pén.* 1988, comm. 63, obs. M. VERON.
[365] Notion développée *in* R. MERLE et A. VITU, *Traité de droit criminel, Droit pénal spécial,* Cujas 1982, n° 24, p. 35.
[366] *Ibid.*
[367] *Ibid.*

« *La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faites de mauvaise foi, elle aura troublé ou aura été susceptible de troubler, la paix publique* ***ou l'ordre politique****, sera punie d'une amende de 45 000 euros.*

Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation ».

100. Conclusion de la Section 2. Loin d'être dépassées, les infractions de presse se montrent adaptées aux nouvelles formes de communication rencontrées sur les sites de réseaux sociaux. De manière générale, les infractions de presse ont été rédigées en des termes suffisamment larges pour permettre d'appréhender des abus de la liberté d'expression qui ne pouvaient être envisagés au moment de la rédation initiale de la loi du 29 juillet 1881. Ainsi, les pratiques telles que le partage de contenus ou le *retweet* d'informations se retrouvent aujourd'hui parfaitement dans l'hypothèse de « *reproduction* » envisagée à l'origine par la loi sur la liberté de la presse. Par ailleurs, certaines infractions tombées en désuétude, à l'image du délit de fausse nouvelle, retrouvent avec les réseaux sociaux en ligne leur place dans les outils répressifs moyennant toutefois, dans une certaine mesure, une modernisation de leur rédaction. Il revient alors au juge d'utiliser le corpus des infractions de presse autant que le permet ce dernier.

Conclusion du Chapitre 1

101. Avec l'apparition et l'usage intensif des sites de réseaux sociaux le droit pénal spécial de la presse a su démontrer son exceptionnel pouvoir d'attraction. Il n'est plus l'apanage de quelques professionnels de la communication jouissant d'un pouvoir de publication mais régit désormais la communication réalisée *via* les sites de réseaux sociaux par tout individu[368]. Le droit de la presse devient alors le droit de l'expression citoyenne, le terme « *presse* » ne reflétant plus son réel champ d'application, c'est pourquoi certains parlent de « *droit des médias* »[369], ou de « *droit de la publication* »[370]. Les défis à relever sont considérables mais les infractions de presse sont de taille. De manière générale, il convient d'opter pour une modernisation de la loi sur la liberté de la presse par le biais de quelques ajouts venant consolider ses bases plutôt qu'un mouvement de déspécialisation de cette loi entraînant le glissement progressif d'infractions de presse dans le droit pénal commun. La sauvegarde de la loi du 29 juillet 1881 paraît indispensable en ce qu'elle introduit un régime favorable justifié par la protection de la liberté d'expression. Le transfert d'infractions de presse vers le droit commun, motivé par une volonté de durcir la répression, a en effet pour conséquence d'entraîner l'application d'un régime coercitif difficilement conciliable avec des infractions relevant des abus de la liberté d'expression[371]. À l'opposé, une partie de la doctrine prône un transfert des dispositions de la loi sur la liberté de la presse dans le droit civil comme cela a pu s'observer dans les régimes juridiques belges ou encore luxembourgeois[372]. Cette « *civilisation* » aurait pour but d'effacer les infractions de presse au profit de poursuites sur le fondement de la responsabilité civile délictuelle[373]. Cependant, une telle solution est peu souhaitable car les abus de la liberté d'expression ne seraient plus encadrés par des définitions pénales soumises au principe de légalité criminelle et d'interprétation stricte[374] mais à la seule exigence de la démonstration d'un fait générateur de responsabilité, d'un lien causal et de

[368] Il est nécessaire toutefois que les paramétrages de confidentialité soient suffisamment ouverts pour que le critère de publicité soit rempli, ce qui est le principe plutôt que l'exception.
[369] E. RASCHEL, *La procédure pénale en droit de la presse. Presse & édition, radio & télévision, internet, expressions orales et écrites, publiques et non-publiques*, Gazette du Palais, Guide pratique, 2019, p. 13.
[370] B. ADER, « Évolution de la notion de publication : de la presse écrite à Internet », *Légipresse*, octobre 1999, n° 165, p. 123 et suiv.
[371] Par exemple : les délits de provocation et d'apologie du terrorisme transférés à l'article 421-2-5 du Code pénal dans sa section relative aux actes de terrorisme.
[372] V. sur le sujet : B. ADER, « La loi de 1881, réceptacle naturel de toutes les infractions de "publication", depuis la presse et l'imprimerie jusqu'à internet », *Légicom* n° 57, 2016/2 », p. 19 à 21.
[373] C. civ, art. 1240.
[374] C. pén., art. 111-3 et 111-4.

l'existence d'un préjudice[375]. La loi sur la liberté de la presse a un mérite considérable : « *elle existe, est prévisible, elle comporte des règles légales auxquelles s'ajoute tout un corpus jurisprudentiel* »[376].

Une balance équilibrée des intérêts entre protection de la liberté d'expression et sanction de ses abus est l'un des défis majeurs suscités par les réseaux sociaux en ligne. Les dérives ne se limitent cependant pas à la problématique de la liberté d'expression et donc à la loi sur la liberté de la presse. Les réseaux sociaux en ligne sont la transcription numérique de notre société et les infractions qui y sont commises sont multiples. Aussi, l'ensemble du droit pénal doit se montrer à la hauteur des comportements nouveaux engendrés par ces sites collaboratifs. Il est alors nécessaire de se questionner sur l'adaptation des incriminations du droit pénal commun aux sites de réseaux sociaux.

[375] P. MALAURIE, L. AYNÈS et P. STOFFEL-MUNCK, *Droit des obligations*, LGDJ, 9e éd. 2017, p. 41 et suiv, n° 47 et suiv.
[376] B. ADER, « La loi de 1881, réceptacle naturel de toutes les infractions de "publication", depuis la presse et l'imprimerie jusqu'à internet », *Légicom* n° 57, 2016/2 », p. 19 à 21.

Chapitre 2 – Les incriminations du droit pénal commun confrontées aux réseaux sociaux

102. L'adaptation des incriminations du droit pénal commun aux comportements rencontrés sur les réseaux sociaux en ligne se déduit de la capacité de leurs éléments constitutifs à surmonter les spécificités de la communication numérique induite par ces sites. En l'occurrence, de nombreux comportements infractionnels renvoyant à une délinquance traditionnelle se retrouvent au sein des comportements observés sur les sites de réseaux sociaux. Or, les incriminations préexistantes permettent, en raison de leur mode de rédaction, de saisir sans problème ces comportements. Certaines pratiques observées sur les sites de réseaux sociaux ont cependant incité le législateur à adapter les incriminations voire, à créer de nouvelles incriminations afin de répondre aux effets de l'innovation technologique. Ces dernières ne répondent cependant pas nécessairement à de véritables carences structurelles du droit pénal mais reflètent pour nombre d'entre elles davantage une politique criminelle réactive et répressive criticable au regard des principes fondamentaux régissant le droit pénal.

Les incriminations préexistantes se montrent dans leur ensemble adaptées aux comportements rencontrés sur les sites de réseaux sociaux (**Section 1**), l'instauration de nouvelles incriminations n'est dès lors pas nécessairement justifiée (**Section 2**).

Section 1 : Des incriminations préexistantes adaptées aux comportements rencontrés sur les réseaux sociaux

103. La rédaction des incriminations transcendant l'évolution des techniques. Il est fréquent que la rédaction des incriminations permette d'inclure dans leurs éléments constitutifs des comportements que le législateur n'avait pu prévoir à l'origine notamment ceux issus des réseaux sociaux en ligne. Cette faculté d'adaptation trouve sa source dans le principe de légalité criminelle qui exige que les textes pénaux restent « *généraux et abstraits sous peine de tomber dans la casuistique* »[377]. Comme le reconnaît la Cour EDH, « *l'utilisation de la technique législative des catégories laisse souvent des zones d'ombre aux frontières de la définition* » et « *une certaine souplesse peut même se révéler souhaitable pour permettre aux juridictions internes de faire évoluer le droit en fonction de ce qu'elles jugent être des mesures nécessaires dans l'intérêt de la justice* »[378]. Ainsi, à bien des égards, les incriminations préexistantes se montrent adaptées aux évolutions de la société, particulièrement celles induites par les sites de réseaux sociaux. Internet doit à ce titre être perçu « *tel un bien comme un autre ou un support parmi d'autres, d'expression et de diffusion de la pensée, d'informations, etc. C'est sur le mode d'une neutralité technologique que le droit pénal se saisit alors de lui* »[379].

Au regard des incriminations préexistantes à leur apparition, les réseaux sociaux en ligne constituent un nouveau support de réalisation d'infractions (**§1**) mais également un bien protégé (**§2**).

§1. Les réseaux sociaux en ligne, un nouveau support de réalisation d'infractions

104. Les sites de réseaux sociaux, un support de commission d'infractions. Certaines incriminations liées à des formes de criminalité ou de délinquance « *traditionnelles* » ont démontré leur adaptation aux nouvelles technologies de l'information et de la communication. Les sites de réseaux sociaux peuvent constituer un nouveau vecteur d'une délinquance déjà observée auparavant, autrement dit, un nouveau support de réalisation d'incriminations

[377] R. KOERING-JOULIN, J.-F. SEUVIC, « Droits fondamentaux et droit criminel », *AJDA*, 1998, p. 106.
[378] Dans l'ordre des citations, CEDH, *Cantoni c/ France*, 15 novembre 1996, n° 17862/91 : *JCP* 1997.II.22836, note FOUASSIER et VION ; *RSC* 1997, chron. p. 462 – CEDH, *Goodwin c/ Royaume Uni*, 27 mars 1996, n° 17488/90.
[379] A. LEPAGE, « Droit pénal et internet la part de la tradition, l'œuvre de l'innovation », AJP 2005, p. 217.

préexistantes. De nombreuses formes de délinquances sont observables sur ces sites qui constituent autant un moyen d'atteinte aux personnes qu'un moyen d'atteinte aux biens. Les incriminations préexistantes se montrent en effet capables d'appréhender autant les cyberviolences (A) que les atteintes aux biens présentes sur ces sites (B).

A. L'appréhension des cyberviolences par les incriminations préexistantes

105. Une dématérialisation des formes de violences reçue par le droit pénal. Malgré l'éloignement physique des personnes induit par l'utilisation des réseaux sociaux en ligne, ces derniers peuvent être utilisés pour exposer autrui à des contenus illégaux, choquants ou tout simplement non-désirés pouvant provoquer des atteintes à l'intégrité psychique de la personne[380]. Ces formes de cyberviolences se trouvent appréhendées par les incriminations préexistantes soit au titre de menaces (1) soit, plus généralement, au titre de violences psychologiques (2).

1) La répression des menaces par le droit pénal

106. Les réseaux sociaux vecteurs de menaces. Comme toute communication interpersonnelle, au même titre que le téléphone et le courrier papier ou électronique, les réseaux sociaux en ligne peuvent être le moyen de menacer une personne. Ces menaces ont pour objectif de déstabiliser la personne qui en est la cible. Si les auteurs n'ont pas forcément l'intention de passer à l'acte, les tensions et la peur suscitées chez la victime peuvent avoir des répercussions sur son intégrité physique ou psychique. Les menaces constituent alors une forme de violence psychologique qui porte atteinte à la tranquillité de la victime. Les menaces sont donc punissables parce qu'elles sont de nature à atteindre la sûreté morale d'une personne déterminée[381].

107. Une répression autonome des menaces par le droit pénal. Le Code pénal prend en considération ce type d'atteinte de différentes manières. Les menaces constituent d'abord un des adminicules de la complicité par provocation prévue à l'article 121-7 alinéa 2 du Code pénal[382]. Ensuite, les menaces se retrouvent également en tant qu'élément de définition de

[380] V. CANTAT-LAMPIN, « Les atteintes à la personne par le biais des communications électroniques. Une réponse imparfaite du droit pénal », *in* mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, 2017, p. 307.
[381] P. CONTE, *Droit pénal spécial*, LexisNexis, Manuels, 5ème éd., 2016, n° 495.
[382] L'article 121-7 alinéa 2 du Code pénal dispose : « *Est également complice la personne qui par don, promesse, menace, ordre, abus d'autorité ou de pouvoir aura provoqué à une infraction ou donné des instructions pour la commettre* ».

certaines incriminations notamment le chantage[383] ou les agressions sexuelles[384]. Toutefois, l'action de menacer a été jugée suffisamment grave par le législateur pour l'ériger en infraction autonome. Cette dernière fait l'objet d'une pluralité d'infractions qui distinguent principalement les menaces portant sur les individus[385] ou sur les biens[386]. Lorsque les menaces portent sur une personne elles consistent en l'annonce d'un mal susceptible d'être qualifié de crime ou de délit contre les personnes. De même, les menaces à l'encontre d'un bien sont punissables lorsqu'elles renvoient à l'annonce d'un mal susceptible d'être qualifié de destruction, dégradation ou détérioration de ce bien. Toutefois, la menace est punissable non pas en raison de l'éventuelle atteinte à l'intégrité physique ou à l'intégrité des biens que peut subir la personne, mais davantage en raison de l'atteinte à son ordre moral[387]. Ce type d'atteinte purement morale est alors parfaitement observable dans l'espace numérique et particulièrement dans l'environnement des réseaux sociaux en ligne.

2) La répression des violences psychologiques par le droit pénal

108. Les réseaux sociaux, moyens de commission de violences psychologiques. Le droit pénal vient prendre en considération de manière autonome les violences psychologiques en tant que violence volontaire sans exiger la démonstration d'une atteinte à une autre valeur sociale. Ainsi, la loi n° 2010-769 du 9 juillet 2010[388] est venue créer l'article 222-14-3 du Code pénal selon lequel : « *Les violences prévues par les dispositions de la présente section sont réprimées quelle que soit leur nature, y compris s'il s'agit de violences psychologiques* ». Avec cette nouvelle infraction, les violences ne sont plus seulement sanctionnées lorsque qu'elles représentent une atteinte physique à la personne mais peuvent dorénavant être

[383] L'article 312-10 du Code pénal dispose : « *Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ».

[384] L'article 222-22 du Code pénal dispose : « *Constitue une agression sexuelle toute atteinte sexuelle commise avec violence, contrainte, menace ou surprise* ».

[385] L'article 222-17 du Code pénal incrimine la menace sans condition : « *la menace de commettre un crime ou un délit dont la tentative est punissable* » ; l'article 222-18 du Code pénal incrimine la menace avec condition : « *La menace, par quelque moyen que ce soit, de commettre un crime ou un délit contre les personnes, est punie de trois ans d'emprisonnement et de 45 000 euros d'amende, lorsqu'elle est faite avec l'ordre de remplir une condition* ».

[386] L'article 322-12 du Code pénal incrimine la menace sans condition de commettre une destruction, une dégradation ou une détérioration dangereuses pour les « *lorsqu'elle est soit réitérée, soit matérialisée par un écrit, une image ou tout autre objet* » ; l'article 322-13 du Code pénal incrimine la menace, « *par quelque moyen que ce soit, de commettre une destruction, une dégradation ou une détérioration* » lorsqu'elle est faite avec l'ordre de remplir une condition.

[387] E. DREYER, *Droit pénal spécial*, ellipse, 3ème éd., 2016, p. 227, nos 480-481.

[388] L. n° 2010-769 du 9 juillet 2010 relative aux violences faites spécifiquement aux femmes, aux violences au sein des couples et aux incidences de ces dernières sur les enfants, *JORF* n° 0158, 10 juillet 2010, p. 12762.

matérialisées par une atteinte psychique[389]. Le Code pénal protège ainsi l'intégrité physique de la personne mais également son équilibre psychologique.

109. Une forme de violence adaptée à l'environnement numérique. L'infraction définie à l'article 222-14-3 du Code pénal, initialement créée afin de venir apporter une réponse pénale complète aux formes de violences conjugales, dépasse aujourd'hui largement ce champ d'application. Si la notion de violences psychologiques est difficile à définir avec précision, elle revêt, de par sa nature imprécise, un champ d'application extrêmement étendu. Surtout, une telle infraction permet de poursuivre et sanctionner un individu au titre de violences volontaires en l'absence de tout contact physique entre l'agresseur et l'agressé. Antérieurement à la création de l'infraction de l'article 222-14-3 du Code pénal la jurisprudence sanctionnait déjà ce type de violences sous la qualification de « *voies de faits* ». Cette dernière est une violence d'un degré moindre que la violence physique car elle n'exige pas d'atteinte physique directe entre l'auteur et la victime. Elle s'observe donc non pas par l'existence de traces corporelles mais par des formes de pressions graves exercées sur la victime dont l'impact ne peut être que psychologique[390]. Favorable à l'extension des violences, la jurisprudence a jugé que caractérisaient des violences punissables, le fait de menacer une personne avec un revolver[391], l'envoi d'un colis d'excréments[392] ou encore l'envoi de quarante-cinq lettres anonymes, contenant toutes des croix gammées et des cercueils, ainsi que, pour certaines, des termes injurieux, parfois menaçants[393]. En l'absence de qualifications pénales plus précises, ce type particulier de violence est alors parfaitement susceptible d'appréhender les diverses formes de pressions pouvant se retrouver sur les réseaux sociaux en ligne.

110. Une infraction matérielle. Si les violences psychologiques n'entraînent par définition aucune atteinte corporelle à la personne, cela ne signifie pas pour autant que la violence

[389] Avant la loi du 9 juillet 2010, les violences volontaires nécessitaient nécessairement un acte de nature violente, dirigé contre l'intégrité physique de la victime. Il ne savait ainsi avoir de violences sans violences. Par exemple : Cour de cassation chambre criminelle Audience publique du 5 octobre 2010 N° de pourvoi: 10-0.050. Les faits retenus par la cour d'appel pour justifier la condamnation du prévenu, et relevés par la Cour de cassation, étaient les suivants. Celui-ci avait observé, à l'aide d'un miroir de poche passé sous la cloison séparant les cabines d'une piscine publique, une femme et une jeune fille mineure en train de se changer. Informée de ce fait par une amie, la jeune fille alerta les surveillants de la piscine et sa mère déposa plainte en son nom. Informée de son côté par les policiers, la femme porta plainte contre l'auteur de ces faits pour violences. Les violences n'ayant entraîné aucune ITT constituent en principe la contravention prévue par l'article R. 625-1 du Code pénal, mais elles deviennent un délit s'il s'y ajoute une ou plusieurs des circonstances aggravantes énumérées par l'article 222-13. En l'espèce, avaient été retenus le fait que l'une des victimes était un mineur de quinze ans (1°) ainsi que la préméditation (9°).

[390] *Ibid*, n° 63.

[391] Crim., 7 août 1934 : DH 1934. 477.

[392] Crim., 8 novembre 1990, nº 89-86.904 : inédit ; *Dr. pén.* 1991, comm. 102.

[393] Crim., 13 juin 1991, nº 90-84.103 : *Bull. crim.* nº 253 ; *RSC* 1992. 74, obs. G. LEVASSEUR.

psychique n'exige aucun résultat. Les délits de violences supposent un acte positif sciemment commis avec la prévision qu'il en résultera une atteinte à la personne d'autrui[394]. Il s'agit d'infractions matérielles qui imposent la démonstration d'un résultat à savoir une atteinte à la victime. En l'occurrence, cette atteinte se manifeste dans le fait de provoquer une émotion sérieuse chez la victime[395]. Si le résultat est de fait intériorisé, sa matérialité reste pourtant bien exigée. L'émotion visée doit être personnalisée, il n'est pas question de sanctionner un sentiment vague d'insécurité, même s'il peut être collectivement ressenti[396]. Pour ce faire, il doit systématiquement être démontré une atteinte psychique, à savoir une « *émotion sérieuse* » chez la victime. Ainsi, que la violence soit physique ou psychique cette dernière n'est punissable que si elle engendre un résultat. Autrement dit, la sanction interviendra que lorsqu'elle aura causé « *un seuil visible et sensible de souffrance ou de déstabilisation pour la victime* »[397]. En conséquence, si l'infraction de violences psychologiques est parfaitement adaptée à l'environnement numérique, seules les formes de violences les plus graves ayant entrainé un réel préjudice pour la victime pourront entrer effectivement dans son champ répressif.

B. L'appréhension des atteintes aux biens par les incriminations préexistantes

111. Les sites de réseaux sociaux sont également devenus un vecteur d'atteintes aux biens. Ils constituent en l'occurrence le support privilégié d'une délinquance astucieuse visant à tromper les individus dans l'espace numérique pour obtenir de manière frauduleuse la remise de fonds. Les incriminations se montrent alors parfaitement adaptées aux nouvelles formes de tromperies observées sur les sites de réseaux sociaux à savoir, aussi bien l'escroquerie « *à la nigériane* » (1) que le chantage à la webcam (2).

[394] Y. MAYAUD, Rép. pén. Dalloz, octobre 2008 (mis à jour juillet 2019), *V°* Violences volontaires, n° 39.
[395] La Cour de cassation a ainsi rappelé : « *En visant les violences et voies de fait exercées volontairement, le législateur a entendu réprimer notamment celles qui, sans atteindre matériellement la personne, sont cependant de nature à provoquer une sérieuse émotion* ». Crim. 19 février 1892 : DP 1892. 1. 550 – Crim. 22 octobre 1936 : *Bull. crim.* n° 97 ; DH 1937. 38 – Crim. 16 décembre 1953 : *D.* 1954. 129 – Crim. 3 janvier 1969, n° 68-91.288 : *Bull. crim.* n° 1 ; *D.* 1969. 152 ; *JCP* 1969. II. 15791 ; *Gaz. Pal.* 1969. 1. 249 ; Crim. 14 octobre 1970, n° 69-93.195 : *Bull. crim.* n° 267, *D.* 1970. 774 – Crim. 7 mars 1972, n° 71-91.303 : *Bull. crim.* n° 85, *Gaz. Pal.* 1972. 1. 450 – Crim. 18 février 1976, n° 75-92.403 : *Bull. crim.* n° 63 ; *Gaz. Pal.* 1976. 1. 330, ; *RSC* 1976. 967, obs. G. LEVASSEUR.
[396] Y. MAYAUD, Rép. pén. Dalloz, octobre 2008 (mis à jour juillet 2019), *V°* Violences volontaires, n° 39.
[397] *Ibid.*, n° 36.

1) L'escroquerie « *à la nigériane* » sur les sites de réseaux sociaux

112. Les nouvelles formes de tromperie observées sur les réseaux sociaux. La construction de faux profils numériques renvoyant à de véritables identités ou des identités créées de toute pièce est devenue un moyen d'atteinte privilégié sur les réseaux sociaux. Ces escroqueries dites « *à la nigériane* »[398] ont pour but d'abuser de la crédulité des utilisateurs de messageries en ligne ou désormais des sites de réseaux sociaux en créant de faux comptes sur ces espaces d'échanges. Pour ce faire, les escrocs inventent des profils en récupérant des photos aguicheuses de femmes ou d'hommes à partir d'autres comptes et leur dressent un profil numérique (études, professions, …). Une fois l'identité créée, ils entrent en contact avec des utilisateurs et essayent ensuite d'entretenir une relation visant à gagner leur confiance. Lorsque la confiance de la victime est gagnée, l'escroc sollicite sa générosité pour diverses raisons (un billet d'avion, des frais hospitaliers, des factures impayées, etc.). Cette forme particulière d'escroquerie à l'échelle numérique peut toutefois être parfaitement appréhendée par le délit d'escroquerie de l'article 313-1 du Code pénal.

113. Adaptation du délit d'escroquerie. D'un point de vue matériel, l'infraction d'escroquerie prévue à l'article 313-1 du Code pénal consiste à tromper une personne par l'utilisation de certains procédés. Cette tromperie est caractéristique de l'infraction : « *abuser de la crédulité d'une personne pour obtenir des fonds, valeurs ou un bien quelconque ne constitue pas une escroquerie en l'absence de tromperie*»[399]. L'article 313-1 du Code pénal cite quatre procédés pour qualifier la tromperie, on trouve ainsi l'emploi d'un faux nom, l'emploi d'une fausse qualité, l'abus de qualité vraie et enfin l'emploi de manœuvres frauduleuses. L'emploi d'un faux nom consiste en l'utilisation par l'escroc d'un nom ou d'un prénom qui n'est pas le sien. Il est indifférent que le faux nom auquel recourt l'auteur de l'infraction soit réel ou imaginaire, même si l'usage d'une identité imaginaire peut susciter des interrogations de la part de la victime[400]. La tromperie peut également relever du procédé d'emploi de manœuvres frauduleuses. Le terme de « *manœuvres* » suppose un comportement positif caractérisant une mise en scène, même peu élaborée. La jurisprudence paraît exiger que le mensonge soit accompagné d'un fait extérieur, tel que l'intervention d'un tiers qui

[398] M. QUÉMÉNER, Y. CHARPENEL, *Cybercriminalité Droit pénal appliqué*, Economica, 2010, p. 134, n° 596.
[399] F. STASIAK, *Droit pénal des affaires*, LGDJ, 2ème éd., 2009, p. 25.
[400] *Ibid*, p. 28.

devient complice lorsqu'il est de mauvaise foi[401], accréditant l'allégation mensongère[402]. En définitive, l'usage de manœuvres frauduleuses est entendu comme un comportement positif, qui ne peut se satisfaire d'un simple mensonge, sauf si celui-ci est corroboré par d'autres éléments (c'est-à-dire un stratagème). La création d'une fausse identité sur un réseau social peut être appréhendée par le délit d'escroquerie lorsque cette manœuvre est destinée à tromper un utilisateur afin d'obtenir de lui un avantage souvent de nature pécuniaire. La création d'un faux profil n'est cependant pas sanctionné de manière autonome, le stratagème mis en place par le cyberescrocs devant nécessairement porter préjudice à la personne visée ou à un tiers en le déterminant à remettre « *des fonds, des valeurs ou un bien quelconque* ». En définitive, l'usage du faux profil ne forme qu'un élément du délit d'escroquerie, en l'occurrence la manœuvre consistant à tromper l'internaute.

2) Le chantage à la webcam sur les sites de réseaux sociaux

114. Description de la pratique du chantage à la webcam. La pratique du chantage a trouvé un nouvel élan avec l'émergence sur internet d'un type particulier de chantage appelé « *chantage à la webcam* ». Cette dernière peut se décrire comme le fait pour la victime de se rendre sur un site de rencontre puis d'entamer la conversation avec une jeune femme ou un jeune homme au physique attrayant derrière lequel se cache en réalité un individu mal intentionné. Après lui avoir posé quelques questions sur sa vie privée, cette personne l'invite à approfondir les échanges via une conversation vidéo plus intime. L'individu va ensuite utiliser l'enregistrement vidéo de cette rencontre virtuelle en menaçant de diffuser son contenu sur un réseau social ou sur un site de partage de vidéos si la victime ne lui remet pas une somme d'argent dans un bref délai[403]. Cette forme de chantage peut entraîner des conséquences particulièrement graves, l'exemple du suicide d'un garçon de 18 ans en octobre 2012 en témoigne. Le jeune garçon était entré en l'occurrence en contact sur le site de rencontre « *chatroulette* » avec une jeune femme. Cette dernière l'a ensuite invité à poursuivre leur dialogue sur un réseau social et à s'adonner à des jeux érotiques devant la webcam. La femme a finalement menacé de révéler les vidéos qu'elle avait enregistrées contre le versement d'une

[401] Crim., 31 janvier 2007, n° 06-81.258 : *Bull. Crim.*, n° 25 (deux arrêts) ; *Dr. pén.* 2007, comm. 56, note M. VERON.
[402] Crim., 20 juillet 1960 : *Bull. Crim.*, n° 382 ; Crim., 1er juin 2005 : *Bull crim.*, n° 167 ; *Dr. pén.* 2005, comm. 147, note M. VERON.
[403] <https://www.cnil.fr/fr/reagir-en-cas-de-chantage-la-webcam> (dernière consultation le 9 octobre 2019).

somme d'argent : « *J'ai maintenant une vidéo porno de toi. Si tu ne me donnes pas 200 euros, je vais détruire ta vie en diffusant la vidéo à tous tes amis* »[404].

115. L'appréhension par le droit pénal d'une telle pratique. En l'occurrence, la définition très générale proposée par l'article 312-10 du Code pénal permet de venir sanctionner parfaitement cette hypothèse particulière de chantage réalisée au moyen d'un service de communication au public en ligne. Cet article sanctionne « *le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ». La présente rédaction permet d'en déduire une indifférence du texte d'incrimination au support par lequel la menace est commise. La seule exigence est que cette dernière révèle ou impute des faits de nature à porter atteinte à l'honneur ou à la considération de la victime. L'objet du chantage recouvre donc le même champ d'application que le délit de diffamation[405]. Par ailleurs, le texte se montre totalement indifférent à la forme, à l'origine et à la nature du moyen de pression utilisé par le maître chanteur. Dans ce cas, les faits que menace de révéler le maître chanteur peuvent concerner la commission d'une infraction mais également une attitude ou un comportement contraire aux bonnes mœurs et à la probité[406]. Cependant, à la différence de la diffamation, la présente infraction est commise dans le but précis d'obtenir « *soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ». La largesse du champ d'application de l'infraction se retrouve ainsi également dans la définition de l'avantage convoité par le maître chanteur qui permet de ne pas circonscrire l'infraction à la seule recherche d'une remise de fonds.

§2. Les réseaux sociaux en ligne, un bien protégé

116. Si les sites de réseaux sociaux sont un support permettant la commission d'infractions, ils peuvent également devenir objets d'infractions. Cette affirmation s'observe particulièrement concernant les infractions d'atteintes aux systèmes de traitement automatisés de données[407]. En effet, les sites de réseaux sociaux peuvent être assimilés à un système de

[404] Propos cités *in* : C. BLAYA, « Nature et prévalence de la cyberviolence et du cyberharcèlement », *in Les ados dans le cyberespace. Prises de risque et cyberviolence*, (dir. C. BLAYA), De Boeck Supérieur, 2013, p. 57.
[405] E. DREYER, *Droit pénal spécial*, ellipse, 3ème éd., 2016, p. 444, n° 935.
[406] *Ibid.*
[407] C. pén., Livre III, Titre II, Chapitre III « *Des atteintes aux systèmes de traitement automatisé de données* ».

traitement automatisés de données (STAD) (A) et devenir en conséquence un bien objet d'atteintes (B).

A. Les sites de réseaux sociaux, un STAD

117. La loi n° 88-19 dite Godfrain du 5 janvier 1988[408] a inséré dans le Code pénal un nouveau Chapitre intitulé « *Des atteintes aux systèmes de traitement automatisé de données* ». Les infractions présentes dans ce chapitre viennent définir différents modes d'atteinte par voie informatique[409]. Le législateur distingue le fait de s'introduire et/ou de s'y maintenir frauduleusement dans un système informatique[410] ; le fait d'entraver ou de fausser le fonctionnement d'un système informatique[411] et le fait d'introduire frauduleusement des données dans un système informatique ou de supprimer ou de modifier les données qu'il contient[412]. En l'occurrence, ces outils juridiques en matière de délinquance informatique permettent d'appréhender efficacement des comportements ayant pour cible les sites de réseaux sociaux**.** L'adaptation des infractions relatives à la délinquance informatique est alors fonction de l'adaptation de la notion de système de traitement automatisé de donnée aux réseaux sociaux. Or, la définition pénale du système de traitement automatisé de données (STAD) (1) permet d'assimiler les réseaux sociaux et plus particulièrement le compte d'un réseau social à un système de traitement automatisé de donnée (2).

1) La définition pénale du STAD

118. Élément de définition. Le Code pénal ne définit pas la notion de système de traitement automatisé de données. Il faut se référer à une définition apportée par le Sénat, ce système correspond alors à « *tout ensemble composé d'une ou plusieurs unités de traitement*

[408] L. n° 88-19 du 5 janvier 1988 relative à la fraude informatique, *JORF*, 6 janvier 1988, p. 231.
[409] Depuis le « ver Morris » (*Morris worm)* lancé par un étudiant américain le 2 novembre 1988 les ces dernières se sont à la fois multipliées et diversifiées. Le véritable développement de cette forme de cybercriminalité s'observe à partir du début des années 2000 concomitamment à la démocratisation d'internet, à cette époque, la majorité des ménages mais aussi des entreprises se munissent de ce moyen de communication. Trois types de cyberattaques peuvent être identifiés. Le premier concerne les cyberattaques à visée revendicatrice, leurs auteurs utilisent les failles de sécurité du réseau dans le but de mettre en avant des opinions politiques, philosophiques, religieuses ou terroristes. Les cyberattaques peuvent aussi révéler une finalité mercantile. Il s'agit là de réaliser une exploitation lucrative de données personnelles récoltées pendant une attaque soit par leur revente sur un marché parallèle soit par l'exercice d'un chantage auprès de la personne piratée pour que celle-ci fournisse une somme d'argent contre la non-divulgation de ses données. Enfin les cyberattaques peuvent s'exercer aussi à des fins d'espionnage, cela concerne les attaques diligentées par les services de renseignement d'un pays et visant des systèmes d'information étrangers. Ce type d'espionnage peut s'exercer à des fins économiques ou de sécurité nationale.
[410] C. pén., article 323-1.
[411] C. pén., art. 323-2.
[412] C. pén., art. 323-3.

automatisé de données, tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés »[413]. Cette définition n'apparaissant pas dans la loi, elle n'est qu'une source d'interprétation pour le juge. Deux caractéristiques transparaissent néanmoins à la lecture de la définition : d'une part, l'existence d'un système qui renvoie à un ensemble composé de plusieurs éléments de nature différente[414] (a), d'autre part, un ensemble protégé par des dispositifs de sécurité (b).

a- Un ensemble composé

119. Une variété d'éléments. Un système implique dans un premier temps une variété d'éléments qui le compose. L'énumération de ces éléments dans la définition apportée par le Sénat ne doit pas être interprétée comme exhaustive mais plutôt comme exemplative[415]. Une liste énumérative de ces éléments pouvant être soumise aux aléas de l'évolution du progrès technique, serait susceptible d'être rapidement dépassée. Il est donc impératif que l'incrimination soit en mesure de suivre les évolutions technologiques. La seule exigence concerne le fait que ces éléments soient de nature informatique et qu'ils puissent s'intégrer dans un système. Pour le reste, il peut s'agir autant de biens matériels[416] qu'immatériels[417].

120. Une relation entre les éléments. Un système implique également une relation entre ses éléments. Il ne faut donc pas confondre un « *système de traitement automatisé de données* » avec un simple « *traitement automatisé de données* » qui renvoie à une activité accomplie au sein d'un système automatisé de données. Les délits se constituant dès lors qu'une atteinte est portée au système. La jurisprudence montre cependant une certaine souplesse à l'égard de l'exigence d'une relation entre les différents éléments du système, l'atteinte pouvant se caractériser dès lors que l'intégrité d'un seul de ses éléments est mise en jeu. Par exemple, la qualification de STAD est retenue à l'encontre d'un logiciel pris isolément[418]. De même, le système de carte bleue (CB) constitue un STAD[419]. Une telle

[413] Doc. AN 1987-1988, n° 1009 et plus particulièrement Rapp. Thyraud : Doc. Sénat n°3, 1987-1988, p. 51.
[414] Par exemple : ordinateurs, logiciels, informations codées sous forme de données, mémoires, organes d'entrée et de sortie.
[415] C. ROBACZEWSKI, « Atteintes aux systèmes de traitement informatisés de données », *J.-Cl.* Pénal Code, art. 323-1 à 323-7, Fasc. 2, n° 9.
[416] Par exemple : des ordinateurs, supports de logiciel ou de données. C. ROBACZEWSKI, « Atteintes aux systèmes de traitement informatisés de données », *op. cit.*, n° 10.
[417] Par exemple : des informations codées sous forme de données. C. ROBACZEWSKI, « Atteintes aux systèmes de traitement informatisés de données », *op. cit.*, n° 10.
[418] Douai, 7 octobre 1992 : *JCP* E 1994. I. 359, n° 15, obs. M. VIVANT et C. Le STANC. *Adde* : C. ROBACZEWSKI, « Atteintes aux systèmes de traitement informatisés de données », *op. cit.*, n° 11.

qualification concerne également le réseau wifi (*Wireless Fidelity*)[420]. Enfin, de manière plus récente, un site internet[421] ainsi que le système de messagerie d'un CHU[422] se sont vus reconnaître la qualification de STAD. La jurisprudence retient donc une acception large du support des infractions[423], la notion de STAD ne doit pas être perçue comme une entité rigide mais davantage comme un support infractionnel venant s'adapter aux évolutions technologiques. De ce point de vue, l'absence de définition légale est indispensable pour que le juge puisse entretenir cette souplesse d'interprétation.

121. Un traitement automatisé de données. La définition d'un traitement automatisé de données se retrouve dans plusieurs textes à la fois européens et nationaux. Au niveau européen, cette définition figurait à l'origine à l'article 2 b) de la directive 95/46/CE et se retrouve désormais à l'article 4 (2) du règlement européen sur la protection des données (RGPD)[424] reprenant peu ou prou les prévisions préexistantes. Ces dernières ont été transposées en droit français par la loi n° 2018-493 du 20 juin 2018[425] à l'article 2 alinéa 3 de la loi « *informatique et libertés* ». Le règlement européen conçoit à ce titre la notion de traitement comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ». Selon cette

---

[419] En l'occurrence, l'atteinte avait été portée au terminal de paiement qui a été considéré comme un élément du système carte bleue. V. TGI Paris, 25 février 2000, n° 9821770011 : *D.* Affaires 2000, p. 219, obs. X. DELPECH.

[420] M. QUÉMÉNER, Y. CHARPENEL, *Cybercriminalité Droit pénal appliqué*, Economica, 2010, p. 71.

[421] TGI Paris, 13ème ch. corr., 18 décembre 2014, n°12010064012 : « *Le prévenu doit être condamné du chef d'introduction frauduleuse de données dans un système de traitement automatisé de données. Il a, en profitant d'une faille de sécurité sur le site internet d'un élu, introduit des instructions informatiques à un endroit non prévu à cet effet afin de modifier le comportement de ce site. Il a utilisé la fonction "rechercher" et y a introduit du langage informatique afin de modifier l'affichage de certaines données sur le site* ».

[422] Crim. 16 janvier 2018, n° 16-87.168 : *Bull. crim.* n° 1, janvier 2018 ; *D.* 2018 p. 172 ; *AJ Pénal* 2018 p. 205, obs. J.-B. THIERRY ; *RSC* 2018 p. 480, obs. P. MISTRETTA ; *Dr. pén.* 2018, comm. 74, obs. P. CONTE ; *CCE* 2018, comm. 30, obs. E.-A. CAPRIOLI ; *Gaz. Pal.* 30 avril 2018, p. 65, obs. F. FOURMENT ; *RSC* 2018 p.701, obs. E. DREYER. Selon ce dernier le prévenu qui a utilisé les codes de messagerie de deux employés d'un CHU obtenus au moyen d'un *keylogger* pour prendre connaissance de leurs courriels s'est bien « *introduit dans deux STAD de manière frauduleuse car à l'insu des utilisateurs desdits services de messagerie* ». V. E. DREYER, « Accès frauduleux, indirect, mais certain, dans un STAD et détention du matériel le permettant », *RSC* 2018, p. 701.

[423] E. DAOUD et G. PÉRONNE, « *Cyberattaques : la lutte s'intensifie* », *AJ Pénal* 2015, p. 396.

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

[425] L. n° 2018-493, 20 juin 2018, relative à la protection des données personnelles, *JORF* n° 0141, 21 juin 2018, texte n° 1.

définition, le terme « *automatisé* » ne peut être conçu comme l'équivalent d' « *informatisé* » : la simple utilisation d'un ordinateur lors d'un traitement de données ne suffit pas à emporter l'application de la loi, il a par exemple été jugé que l'utilisation manuelle d'un ordinateur n'entre pas dans la catégorie des traitements automatisés[426]. Il s'agit davantage d'un déroulement systématique, d'une suite d'opérations logiques et mathématiques effectuées par des moyens automatiques (calculateur, ordinateur) sur des données pour les exploiter selon un programme.

b- Un ensemble protégé

122. Un dispositif de protection déterminé. Le Sénat proposait dans sa définition d'un STAD que ce dernier soit protégé par un dispositif déterminé. Le Code pénal ne fait toutefois pas référence à un quelconque dispositif de sécurité à l'entrée dans un STAD. Ce silence législatif a même conduit certains commentateurs de la loi Godfrain à conclure en l'absence d'une telle exigence[427]. La jurisprudence s'est prononcée dans le sens d'une telle lecture notamment par un arrêt qui admettait « *qu'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection, mais qu'il suffit que le maître du système ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées* »[428]. La présence d'un tel dispositif peut cependant s'avérer utile au juge dans la caractérisation des infractions des articles 323-1 et suivants du Code pénal, cela permettant de prouver avec une plus grande facilité le caractère irrégulier et délibéré de l'intrusion. L'absence d'un tel dispositif peut même servir d'argument pour rejeter la qualification de l'infraction, il a ainsi été jugé que « *les parties de site, qui ne font, par définition, l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, doivent être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès* »[429]. Au vu de ces éléments, il est alors question de démontrer qu'un compte de réseau social peut constituer un STAD.

---

[426] Crim., 13 janvier 2009 : *Bull. crim* 2009, n° 13.

[427] V. notamment : J.-P. BUFFELAN, « La répression de la fraude informatique », *Expertises*, février 1988, p. 55. ; H. CROZE, « L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique) », *JCP G* 1988, I, 3333, spéc. n° 7 ; J. DEVEZE, « Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », *RLDI* 1987, mise à jour, février 1988, p. 3, spéc. n° 53 ; M.-P. LUCAS DE LEYSSAC, « Fraude informatique : protection des systèmes de traitement automatisé de données, répression de la falsification de documents informatisés et mesures de prévention : loi du 5 janvier 1988 », RD informatique et télécom. 1988, n° 2, p. 18. spéc. p. 21 ; H. ALTERMAN et A. BLOCH, « La fraude informatique », *Gaz. Pal.* 1988, 2, doctr. p. 530, spéc. p. 532.

[428] Paris, 5 avril 1994, *LPA* 1995, n° 80, chron. Droit de la communication, note V. ALVAREZ ; *JCP* E 1995, I, 461, obs. F. VIVANT et C. Le STANC.

[429] Paris, 30 octobre 2002, Kitetoa c/ Sté Tati : *CCE* 2003, comm. 5 ; *D.* 2003, p. 2827, note C. Le STANC ; *LPA* 2003, n° 104, p. 12, note E. BOURGEOIS.

2) L'assimilation des sites de réseaux sociaux à un STAD

123. Qualification juridique du compte d'un utilisateur. Les sites de réseaux sociaux peuvent être l'objet d'attaques informatiques, cependant, pour poursuivre l'auteur d'un piratage informatique sur un réseau social il doit être démontré en liminaire que cette attaque constitue une atteinte à un STAD. Or, cette notion est en l'occurrence applicable tant à l'échelle du réseau social (a) qu'à l'échelle du compte de l'utilisateur (b).

a- Le réseau social, un STAD

124. Le réseau social, un traitement automatisé de données. Au regard de la jurisprudence européenne il peut être affirmé qu'un site de réseau social organise un traitement automatisé de données. Ceci se déduit en premier lieu de la jurisprudence de la Cour de justice de l'Union européenne du 13 mai 2014[430] venant reconnaître que le moteur de recherche Google opérait un traitement automatisé de données. Pour ce faire, le juge a constaté que : « *en explorant de manière automatisée, constante et systématique Internet à la recherche des informations qui y sont publiées, l'exploitant d'un moteur de recherche "collecte" de telles données qu'il "extrait", "enregistre" et "organise" par la suite dans le cadre de ses programmes d'indexation, "conserve" sur ses serveurs et, le cas échéant, "communique à" et "met à disposition de" ses utilisateurs sous forme de listes des résultats de leurs recherches* ». Or, s'il est évident que le service de moteur de recherche proposé par Google n'a pas les mêmes finalités qu'un site de réseau social, il n'empêche que leur mode de fonctionnement tant dans la collecte des données que dans leur traitement sont similaires. Les réseaux sociaux en ligne collectent en effet de manière systématique les données personnelles générées par leurs utilisateurs et recourent à un traitement de ces données par des systèmes algorithmiques[431]. Les sites de réseaux sociaux organisent alors assurément un traitement automatisé de données. La Cour de justice de l'Union européenne est venue justement reconnaître le 6 octobre 2015[432] que le réseau social Facebook organisait un traitement de données en raison du transfert des données de ses utilisateurs européens vers ses serveurs situés en amérique. La Cour a en effet estimé que « *l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel* ».

[430] CJUE, *Google Spain c/ Mario Costeja González*, grde ch., 13 mai 2014, affaire C-131/12.
[431] Pour une explication plus approfondie : v. *infra* n^{os} 333 à 339 et n^{os} 514 à 517.
[432] CJUE, *Maximilian Schrems c/ Data Protection Commissioner*, 6 octobre 2015, aff. C-362/14.

125. Le réseau social, un système. En outre, il est aisé d'admettre qu'un site organisant un réseau social constitue un système de traitement automatisé de données en raison du nombre important et de la variété des éléments informatiques qui entrent dans son fonctionnement. Par exemple, leurs serveurs informatiques[433] suffiraient à conclure à l'existence d'un système. Plus encore, ces sites ont pour principale caractéristique de mettre en réseau les individus et de favoriser ainsi leur interconnexion, chaque ordinateur personnel constituant dès lors un élément au sein du système pris dans son ensemble. Dès lors, une atteinte informatique portée à l'échelle d'un réseau social peut caractériser une atteinte à un STAD telle qu'envisagée par les articles 323-1 et suivants du Code pénal.

b- Le compte de réseau social, un STAD

126. Un compte de réseau social, un élément du STAD. Le compte d'un utilisateur peut être perçu dans un premier temps en tant qu'élément du réseau social pris dans son ensemble et donc comme un élément entrant dans la composition d'un STAD. Les comptes créés par chaque utilisateur au sein d'un réseau social viennent dans cette hypothèse s'ajouter aux différents éléments qui composent ce dernier en tant qu'élément autonome géré par son titulaire. Chaque compte constitue alors un élément distinct dans le système du réseau social. Dans cette hypothèse, même si l'atteinte ne porte que sur un seul des éléments du STAD, en l'occurrence un compte d'utilisateur du réseau social, la qualification d'une infraction d'atteinte aux STAD peut néanmoins être retenue[434].

127. Un compte de réseau social, un STAD. Cependant, la définition du STAD peut également être rapportée à l'échelle d'un compte d'utilisateur du réseau social lui-même. Le compte d'un réseau social peut en effet être perçu comme un système composé d'éléments informatiques de différente nature mis en relation. Il faut alors distinguer les éléments informatiques matériels composant le compte de réseau social des éléments informatiques immatériels. Concernant les éléments matériels, un compte de réseau social est très souvent relié à une ou plusieurs unités de traitement (ordinateur, smartphone ou tablette numérique). Mais un compte de réseau social se compose principalement d'éléments informatiques immatériels sous forme de données informatiques. Un tel compte est en permanence alimenté

[433] Le mot *serveur* fait référence au rôle joué par un appareil sur un réseau informatique. Un serveur peut se retrouver sous différentes formes : une petite boîte, un micro-ordinateur, ou alors un mini-ordinateur, un mainframe ou même une ferme de calcul. La taille de l'appareil et sa puissance est fonction de la quantité de travail, qui dépend du nombre d'utilisateurs qui demandent des services au même instant.
<https://fr.wikipedia.org/wiki/Serveur_informatique> (dernière consultation le 9 octobre 2019).
[434] V. *supra* n° 120.

par des données à caractère personnel de son utilisateur ou d'autres utilisateurs (photos, vidéos, commentaires, messages privés). Un compte de réseau social est aussi automatiquement relié à l'adresse mail, voire, au numéro de téléphone de son utilisateur. Il est de ce fait facilement observé qu'une pluralité d'éléments de nature informatique viennent entrer dans la composition du compte de réseau social. De plus, ces éléments informatiques mis en relation ne forment pas un simple agrégat mais au contraire une entité interconnectée, un système.

128. Par ailleurs, la directive 95/46/CE renvoie dans sa définition du traitement automatisé de données à tout type de « *procédés automatisés et appliqués à des données à caractère personnel* ». La directive cite en exemple « *la collecte, l'enregistrement, l'organisation, la conservation, la communication* […] *ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion* » de données personnelles. Il est de ce point de vue facilement concevable qu'un compte de réseau social effectue un traitement automatisé de données en ce qu'il organise les données personnelles de son utilisateur, les met à sa disposition et à la disposition du public en fonction de son paramétrage de confidentialité. Il favorise, de plus, les rapprochements et les interconnexions entre les données personnelles des différents membres du réseau social.

129. Enfin, les comptes de réseaux sociaux possèdent un dernier élément déterminant dans la qualification de STAD : un dispositif de sécurité. Le compte de réseau social ne constitue pas un accès ouvert aux internautes mais un accès restreint à son unique titulaire. Les réseaux sociaux ont donc mis en place un système d'authentification par mot de passe généré par le titulaire du compte. Si un dispositif de sécurité n'est pas une condition légale à qualification du STAD, il demeure néanmoins un élément déterminant dans la constitution des infractions qui s'y réfèrent. La protection à l'entrée du système fait ainsi partie du faisceau d'indices utilisé par le juge pour observer la constitution des délits des articles 323-1 et suivants du Code pénal[435].

130. Au vu de ces éléments, un compte de réseau social peut s'analyser comme un STAD en ce qu'il met en relation différents éléments informatiques, qu'il utilise des procédés automatisés de traitement des données et que son accès est restreint par l'existence d'un dispositif de sécurité. Enfin, cette interprétation ne viendrait pas contredire la jurisprudence en la matière qui démontre une certaine souplesse dans la qualification de l'infraction. Il est alors préférable de considérer le STAD à l'échelle du compte de réseau social principalement pour

[435] V. *supra* n° 122.

deux raisons. D'une part, les éléments constitutifs d'un STAD peuvent parfaitement se rapporter à l'échelle du compte d'un utilisateur. D'autre part, il est préférable de considérer l'infraction à l'échelle du compte de l'utilisateur lorsque l'atteinte est dirigée à l'encontre de ce dernier, ce serait ainsi le détenteur du compte de réseau social et non le réseau social lui-même qui serait considéré comme victime de l'infraction.

B. Les sites de réseaux sociaux, un bien objet d'atteintes aux STAD

131. Le Code pénal dans son chapitre « *des atteintes aux systèmes de traitement automatisé de données* »[436] vient incriminer différents types de comportements venant se rapporter à la criminalité informatique et permettant d'appréhender ces pratiques. L'introduction frauduleuse sur un compte de réseau social peut entraîner, sous certaines conditions, la constitution d'infractions prévues aux articles 323-1 et suivants du Code pénal. Les infractions d'atteinte aux STAD prévues dans le Code pénal manifestent plusieurs degrés de répression. L'article 323-1 incrimine le simple accès ou maintien frauduleux dans un STAD (1) alors que l'article 323-3 prévoit les cas d'atteinte à l'intégrité des données du système suite à une intrusion (2).

1) L'accès ou le maintien frauduleux dans un STAD

132. Absence de préjudice. Selon l'article 323-1 du Code pénal « *le fait d'accéder ou de se maintenir, fraudulement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende* ». Le système répressif vise en l'occurrence ce simple accès ou maintien indépendamment de l'existence d'un préjudice lié à cette intrusion. Il s'agit d'un délit instantané qui se consomme en un trait de temps, le préjudice ne faisant pas partie des éléments constitutifs de l'infraction.

133. L'accès. La notion d'accès dans un STAD se caractérise par la pénétration dans un système suite à une manipulation informatique ou tout autre manœuvre opérée de manière frauduleuse[437]. Plus généralement, l'infraction est caractérisée dès lors qu'une personne non habilitée pénètre dans un STAD tout en sachant qu'elle est dépourvue d'autorisation. Ainsi, le fait d'usurper le mot de passe et de se connecter dans un espace réservé d'un système ouvert au public, par exemple le compte d'un réseau social, caractérise l'accès frauduleux. De même, le fait d'utiliser un cracker de mot de passe ou encore d'introduire un cheval de Troie ou tout

[436] C. pén., Livre III, Titre II, Chapitre 2 « *des atteintes aux systèmes de traitement automatisé de données* ».
[437] M. QUÉMÉNER, Y. CHARPENEL, *Cybercriminalité Droit pénal appliqué*, Economica, 2010, p. 72.

autre procédé visant à interroger un système à distance, sont constitutifs de cette infraction. Au final l'ingénierie sociale constitue parfaitement un moyen d'accès frauduleux à un STAD[438]. En revanche, il ne peut être reproché à un internaute d'accéder dans les parties d'un site internet qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation lorsque ces parties ne font l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de service[439].

134. Le maintien. Le maintien peut quant à lui revêtir deux formes. Il peut s'agir dans un premier temps de la situation où l'accès dans le STAD a été régulier mais lorsqu'il est suivi d'un maintien qui lui ne l'est pas. Cela peut concerner l'hypothèse où la personne n'était pas habilitée à se maintenir dans le système, est ainsi frauduleuse « *l'utilisation pendant plus de deux ans d'un code permettant l'accès à une base de données accessibles aux seules personnes autorisées, alors que ce code a été remis à un salarié pour sa période d'essai* »[440]. Dans un deuxième temps, le maintien peut se réaliser par celui qui, par inadvertance accède à un système fermé et qui s'y maintient volontairement tout en sachant qu'il n'en a pas le droit[441]. Dans cette hypothèse, le fait de prendre possession d'un ordinateur où certaines sessions n'auraient pas été auparavant fermées et de naviguer sur les comptes personnels du titulaire de l'ordinateur serait de nature à qualifier l'infraction de maintien frauduleux dans un STAD. Celle-ci ne saurait cependant être qualifiée sans rapporter également le caractère frauduleux du comportement, autrement dit, la preuve que la personne ait agi en connaissance de cause.

135. Élément moral. Le caractère frauduleux suppose la conscience chez l'individu de l'irrégularité de son acte[442]. Plus précisément, le délinquant doit avoir eu conscience d'accéder ou de se maintenir sans droit dans le système. Selon la jurisprudence constante, l'élément intentionnel du délit est caractérisé lorsque l' « *accès [est] fait sans droit et en pleine connaissance de cause […] cette absence de droit résulte de l'absence d'autorisation du maître du système* »[443]. Dans le cas présent l'élément moral ne suppose pas chez l'auteur de l'infraction une intention de nuire, il suppose la seule conscience d'accéder dans un

[438] V. en ce sens : TGI Paris, 2 septembre 2004, nº 0312990195, reconnaissant la méthode du *phishing* comme moyen d'accès frauduleux à un STAD.
[439] Paris, 30 octobre 2002, *LPA* nº 104, 26 mai 2003, p. 12, note BOURGEOIS ; V. dans le même sens, Paris, 30 octobre 2002, *Expertises*, 2003. 266, nº 33.
[440] Crim., 3 octobre 2007, nº 07-81.045 : *AJ Pénal* 2007, p. 535.
[441] V. en ce sens : Paris, 5 avril 1994 : *D.* 1994. IR 130.
[442] F. CHOPIN, Rép. pén. Dalloz, juillet 2013 (actualisation : avril 2018), *V°* Cybercriminalité, § 17.
[443] M. QUÉMÉNER, Y. CHARPENEL, *Cybercriminalité Droit pénal appliqué*, Économica, 2010, p. 73 ; référence : Toulouse, 3ème Chambre, 21 janvier 1999.

système sans droits et la volonté de s'y maintenir. Le maître du système s'interprète comme la personne ou le service compétent pour autoriser l'accès[444], rapportée aux réseaux sociaux en ligne l'infraction est qualifiée à partir du moment où le titulaire du compte de réseau social n'a pas donner son accord exprès à l'entrée sur son espace personnel et que l'individu décide malgré tout d'y accéder ou de s'y maintenir. Toutefois, lorsqu'une attaque informatique vise un réseau social ou les espaces personnels de leurs membres, celle-ci a souvent pour but de tirer bénéfice des données auxquelles cette dernière donnerait accès. Dans cette situation le pirate informatique ne se contente plus uniquement de déjouer les barrières de sécurité mises en place mais poursuit aussi un objectif bien précis et préjudiciable pour la personne visée. Dès lors la répression peut se fonder sur l'article 323-3 du Code pénal qui prévoit l'atteinte à l'intégrité des données du système.

136. Utilisation de la méthode d'ingénierie sociale sur les sites de réseaux sociaux. Les sites de réseaux sociaux sont devenus une cible privilégiée des pirates informatiques. Ces derniers utilisent principalement la méthode d'ingénierie sociale[445] pour accéder aux comptes des utilisateurs. Ce concept fait référence à une acquisition déloyale d'une information ou la divulgation d'une information sensible suite à une manipulation psychologique de l'individu. Ces techniques consistent donc à utiliser les capacités décisionnelles et cognitives des individus pour les induire en erreur. Autrement dit, les failles humaines d'un système d'information vont être utilisées pour casser les barrières de sécurité mises en place. L'ingénierie sociale se base donc sur la force de persuasion et sur l'exploitation de la crédulité de la personne ciblée. Ce concept n'est pas propre au piratage informatique, on le retrouve également sous d'autres formes comme l'utilisation du téléphone ou du courrier écrit. Dans le contexte de la sécurité informatique, l'ingénierie sociale se matérialise par le fait d'induire en erreur un internaute pour ensuite installer sur son ordinateur un programme malveillant destiné le plus souvent à récupérer ses identifiants et mots de passe c'est le cas en particulier de la méthode du *phishing* ou hameçonnage[446]. Le pirate agit au moyen de messages électroniques et de sites internet miroirs revêtant l'apparence de messages émanant d'entreprises légitimes tels que des établissements financiers ou des administrations publiques. La victime croyant s'adresser à un tiers de confiance renseigne en réalité le pirate

[444] *Ibid.*

[445] Cette notion connue sous le terme anglais de *social engineering* a été théorisée dans l'ouvrage de K. D. MITNICK et W. L. SIMON : *L'art de la supercherie, l'importance du facteur humain dans la sécurité informatique*, CampusPress, 2011.

[446] Le terme « *Hameçonnage* » est un néologisme québécois créé en avril 2004 par l'Office québécois de la langue française. En France, la Commission générale de terminologie et de néologie a choisi en 2006 le terme « *filoutage* ».

sur des informations sensibles comme le mot de passe ou le numéro de carte de crédit[447]. En conséquence, avant d'utiliser des procédés complexes nécessitant une maîtrise de l'élément informatique, l'ingénierie sociale constitue un moyen plus simple de détourner les systèmes de sécurité résultant le plus souvent de la simple connaissance de la victime.

137. Exemple d'une attaque au moyen de l'ingénierie sociale. Le 24 juin 2010, le Tribunal correctionnel de Clermont-Ferrand[448] a ainsi condamné un auvergnat de 23 ans connu sous le pseudonyme de « *Hacker Croll* » à 5 mois de prison avec sursis pour s'être introduit, à l'aide de l'ingénierie sociale, sur les comptes Twitter de personnalités parmi lesquels, le compte de campagne du président américain Barack Obama. La méthode utilisée par le pirate fut d'une facilité déconcertante, ce denier s'introduisit dans un premier temps sur la messagerie électronique du PDG du site de microblogging. Pour y parvenir, le jeune auvergnat exploita les failles humaines du dispositif de sécurité en répondant à la question secrète de la boîte de messagerie à savoir : la ville de naissance du titulaire du compte. Cet accès direct à la boîte de messagerie électronique du PDG de Twitter lui a ensuite permis d'obtenir les codes administrateurs du site, d'infiltrer les comptes de son choix et de se procurer des données sensibles relatives à l'entreprise (liste des employés, leur préférences alimentaires, des numéros de carte bleue ou encore des contrats confidentiels entre la société Twitter et d'autres comme Nokia, AOL, Microsoft, Samsung, Dell[449]).

2) Les atteintes à l'intégrité des données du système

138. Éléments constitutifs du délit. L'article 323-3 du Code pénal prévoit que « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier*

[447] Sur les sites de réseaux sociaux, les hackeurs peuvent utiliser plusieurs méthodes de tromperie afin de pirater le compte d'un utilisateur. Une première consiste à reproduire une fausse interface correspondant à la page d'accueil d'un réseau social. L'internaute pensant être sur le site officiel du réseau social fournit au pirate ses identifiants et mots de passe qui lui permettront d'avoir accès au compte de sa victime. Cette duperie est particulièrement efficace avec les sites de réseaux sociaux en raison du fait qu'il est devenu très courant pour un site web d'applications ou de services en ligne d'exiger de l'internaute qu'il se connecte *via* l'un de ses comptes de réseau social. La tactique consiste alors à recréer la page web d'un site, le plus souvent d'application en ligne, qui requiert à l'internaute de se connecter en utilisant un compte Facebook, Twitter ou Google +. Le pirate informatique attrape alors dans ses filets l'internaute qui ne décèlerait pas le caractère non officiel de l'interface. Les pirates peuvent également utiliser les informations rendues publiques par les internautes à travers leurs différents comptes de réseaux sociaux pour organiser ensuite une attaque ciblée. En déterminant les centres d'intérêts de leurs cibles, les hackeurs peuvent ensuite organiser leurs attaques avec précision et ainsi maximiser leur chance de réussite.

[448] TC Clermont-Ferrand, ch. corr., le 24 juin 2010, n° 1138/10.

[449] Le Hacker a fait parvenir une liste de 310 pages d'informations à plusieurs sites spécialisés comme TechCrunch ou Korben.
<http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack> ou <http://korben.info/hack-de-twitter-la-suite.html> (dernière consultation le 9 octobre 2019).

frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende ». Le texte vise deux types de comportements : d'un côté, le fait de venir porter atteinte à l'intégrité du système en introduisant des données à ce système, d'un autre, le fait de porter atteinte à l'intégrité du système en manipulant les données du système. Cette manipulation se traduisant par une suppression, modification, extraction, détention, reproduction, transmission des données de ce système. En outre, l'intention délictueuse se traduit par la conscience chez le délinquant de modifier par son acte l'état du système et la volonté d'agir malgré tout.

139. Précisions quant aux éléments constitutifs. Il n'est pas nécessaire que le fonctionnement du STAD soit mis en péril par l'action du délinquant informatique, l'atteinte à l'intégrité se manifeste par la modification de l'état du système. Cette modification de l'état peut être visible (suppression, ajout, modification de données) ou invisible (transmission, reproduction, détention de données). De même, il semblerait que cet article jouisse d'une autonomie par rapport aux autres infractions du chapitre, notamment celle prévue à l'article 323-1 du Code pénal. Il ne serait alors pas nécessaire pour caractériser l'infraction que celle-ci soit précédée d'un accès frauduleux au système[450]. En conséquence, l'atteinte à l'intégrité des données du système peut être sanctionnée même si l'auteur de l'infraction a accédé de manière licite à celui-ci. Cette interprétation entre en adéquation avec la tendance des juges du fond à interpréter de manière large ces infractions dans l'optique d'une plus grande sévérité pénale.

140. Renforcement de la sévérité pénale. Cette sévérité ne se retrouve d'ailleurs pas qu'au niveau jurisprudentiel, les infractions relatives aux STAD ont à ce titre été sujettes à des aggravations pénales autant concernant la définition de l'infraction elle-même que concernant les *quanta* des peines encourues. La loi n° 2014-1353 du 13 novembre 2014 visant à renforcer les dispositions relatives à la lutte contre le terrorisme[451] est venue modifier la définition de l'infraction de l'article 323-3 du Code pénal en y ajoutant les termes « *d'extraire, de détenir, de reproduire, de transmettre* ». Bien que cette réforme étoffe la définition de l'infraction, il ne faut pas l'interpréter comme une restriction de son champ d'application. Cette nouvelle rédaction pourrait en effet permettre de donner au juge une base juridique claire au vol de

[450] Notons ici que l'article 323-1 alinéa 2 du Code pénal prévoit l'hypothèse d'une introduction frauduleuse suivie d'une suppression, modification des données du système ou d'une altération du système. Les peines sont alors portées à 3 ans et 100 000 euros d'amende.

[451] L. n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, *JORF* n° 0263, 14 novembre 2014 p. 19162.

données[452] sanctionné jusqu'ici par l'infraction d'abus de confiance[453] ou de vol de droit commun[454]. La loi n° 2015-912 sur le renseignement du 24 juillet 2015[455] a, quant à elle, aggravé les peines d'amende encourues, ainsi l'infraction de l'article 323-1 du Code auparavant sanctionnée de 30 000 euros d'amende est désormais punie de 60 000 euros d'amende et l'infraction de l'article 323-3 du Code pénal, punie à l'origine de 75 000 euros d'amende, est portée à 150 000 euros.

141. Application de ces éléments aux réseaux sociaux. Le 15 juillet 2015 un groupe de hackers nommé « *The impact team* » a affirmé avoir piraté le site de rencontre extra-conjugales Ashley Madison[456]. Ces derniers se sont introduits frauduleusement sur le site avant d'en extraire l'ensemble des données personnelles de ses utilisateurs soit plus de 35 millions d'internautes. *The impact team* tenta de faire pression sur la société éditrice du site[457] afin d'obtenir la fermeture des sites Ashley Madison et Establishedmen[458] sous peine de divulguer les données récoltées. Le 18 août 2015 le groupe de hackers mit ses menaces à exécution en publiant plus de 20 Go de données personnelles sur les membres du site de rencontre extra-conjugales comprenant entre autres les adresses mail, numéros de carte de crédit, préférences sexuelles et fantasmes de ses membres[459].

[452] E. DAOUD, G. PÉRONNE, « Cyberattaques : la lutte s'intensifie », *AJ Pénal* 2015, p. 396.
[453] Crim. 22 octobre 2014, n°13-82.630 : *D.* 2015. 415, note A. MENDOZA-CAMINADE ; *CCE* 2015, comm. 17, note E. CAPRIOLI.
[454] Crim. 20 mai 2015, n° 14-81.336 : *D.* 2015, p. 1466, note L. SAENKO ; *D. actu.*, 5 juin 2015, obs. C. DUHIL de BENAZE ; *AJ Pénal* 2015, p. 413, note E. DREYER.
[455] L. n° 2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n° 0171, 26 juillet 2015 p. 12735.
[456] Ashley Madison est un site de rencontre extra-conjugale et un réseau social canadien. Ce site met en relation des internautes mariés ou du moins en couple et souhaitant avoir une relation extra-conjugale. Son slogan est explicite : « *life is short. Have an affair* » (en français : « La vie est courte. Ayez une aventure »).
[457] La société *Avid Life Media*.
[458] Il s'agit d'un site de rencontre géré par la même société éditrice et proposant de mettre en relation des hommes riches avec de jeunes femmes.
[459] D. LELOUP, « piratage : derrière Ashley Madison un groupe à la réputation sulfureuse », *Le Monde*, 19 août 2015.
<http://www.lemonde.fr/pixels/article/2015/08/19/derriere-ashley-madison-un-groupe-a-la-reputation-sulfureuse_4730136_4408996.html> (dernière consultation le 9 octobre 2019).

142. Conclusion de la Section 1. Les comportements infractionnels rencontrés sur les sites de réseaux sociaux correspondent pour leur majorité à une transcription à l'échelle numérique de comportements délictueux déjà présents auparavant. Partant, les incriminations préexistantes du Code pénal permettent de saisir la majorité de ces comportements pouvant entrer notamment sous la qualification pénale des délits de menaces, violences psychologiques, chantage ou encore escroquerie. L'adaptation de ces incriminations provient alors de leur neutralité du point de vue technologique, le moyen de commettre l'élément incriminé étant indifférent à l'utilisation d'un support de communication en particulier. Par ailleurs, certaines incriminations font de l'élément informatique un bien objet d'une protection spécifique à l'encontre des atteintes pouvant lui être porté. Or, le piratage informatique est une pratique qui a largement préexistée aux sites de réseaux sociaux et le développement des piratages des comptes de réseaux sociaux ne révèle pas pour autant un bouleversement des méthodes d'intrusion. En revanche les sites de réseaux sociaux et particulièrement les comptes de leurs utilisateurs sont devenus une cible de premier choix pour les pirates informatiques en raison de la quantité de données personnelles, possiblement sensibles, dont ils recèlent. À ce titre, le système répressif mis en place par la loi Godfrain, bien que datant de 1988, envisage parfaitement les hypothèses particulières d'attaques qui se manifestent sur les sites de réseaux sociaux. L'ensemble des comportements visant à s'attaquer à un réseau social ou à un compte d'un réseau social entrent sous les qualifications pénales envisagées par le législateur en 1988 faisant de ces derniers un bien objet de protection.

Section 2 : L'instauration non justifiée de nouvelles incriminations

143. Des adaptations conjoncturelles critiquables. Les pratiques rencontrées sur les sites de réseaux sociaux ont incité le législateur à incriminer ou à accentuer la lutte à l'égard de nouveaux comportements. Une telle dynamique pourrait être le signe positif d'une adaptation progressive des incriminations aux évolutions de notre société cependant elles témoignent majoritairement d'adaptations davantage symboliques qu'efficaces[460]. Plus encore, certaines nouvelles incriminations méconnaissent les principes fondamentaux attachés à la répression tels que le principe de nécessité de la loi pénale ou encore le principe de personnalité de la responsabilité pénale. L'instauration de nouvelles incriminations n'est pas toujours justifiée soit en raison de leur caractère redondant, c'est le cas de l'incrimination *happy slapping* (**§1**), soit parce qu'elles méconnaissent certains principes fondamentaux du droit pénal (**§2**).

§1. La redondance de l'incrimination de *happy slapping*

144. La pratique du happy slapping. Le « *happy slapping* » ou vidéolynchage identifié consiste à filmer ou photographier l'agression physique d'une personne à l'aide d'un téléphone portable et à diffuser les images à un certain nombre de personnes le plus souvent sur un site de partage de vidéos ou sur un réseau social. Cette pratique suggère alors une double forme d'agression. Dans un premier temps l'agression à l'encontre d'un individu simultanée à la prise d'images à l'insu de la victime et dans un second temps, la diffusion de ces images à une audience plus vaste que les témoins de la scène *via* les plateformes de partage et les sites de réseaux sociaux. Ainsi, l'atteinte à la victime ne s'arrête pas à l'événement même mais perdure en raison de sa diffusion à une plus vaste audience[461]. Cette pratique est pour l'essentiel le fait de mineurs ou de jeunes majeurs inspirés de la « *Trash TV* » mais également par la banalisation de la violence et de sa contemplation[462].

145. L'adoption d'une incrimination spécifique. La loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance[463] est venue sanctionner la pratique dite du *happy slapping* en créant dans le Code pénal, dans le cadre des atteintes à l'intégrité physique ou

[460] J.-B. PERRIER, « l'adaptation des incriminations », *RSC* 2017, p. 373
[461] C. BLAYA, « Nature et prévalence de la cyberviolence et du cyberharcèlement », *in* C. BLAYA (dir.), *Les ados dans le cyberespace. Prises de risque et cyberviolence*, De Boeck Supérieur, 2013, p. 49.
[462] P.-J. DELAGE, « *Happy slappers and bad lawyers* », *D.* 2007, p. 1282.
[463] L. n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, *JORF* n° 0056 du 7 mars 2007 p. 4297, art. 44.

psychique de la personne, une section III *ter* consacrée à « *l'enregistrement et à la diffusion d'images de violences* ». Au sein de cette section, l'article 222-33-3 dispose, dans son alinéa premier, qu' « *est constitutif d'un acte de complicité des atteintes volontaires à l'intégrité de la personne prévues par les articles 222-1 à 222-14-1 et 222-23 à 222-31 et est puni des peines prévues par ces articles le fait d'enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission de ces infractions* ». Son deuxième aliéna incrimine quant à lui « *le fait de diffuser l'enregistrement de telles images est puni de cinq ans d'emprisonnement et de 75 000 € d'amende* ». En l'occurrence, ce dernier alinéa peut être utilisé pour réprimer une nouvelle forme de cybercriminalité, dès lors que la diffusion s'effectue sur le réseau internet, notamment sur un site de réseau social. Cependant, ce type particulier de cybercriminalité était déjà sanctionné auparavant sous d'autres fondements (A), de plus, cette incrimination paraît superflue au vu des incriminations similaires préexistantes (B).

A. Une sanction sous d'autres fondements

146. La poursuite et la répression d'auteurs de *happy slapping* avant la loi du 5 mars 2007. Avant l'adoption de l'article 222-33-3 du Code pénal, la justice, qui avait eu à connaître des faits de *happy slapping*, se fondait sur l'atteinte à la vie privée de l'article 226-1 du Code pénal et l'omission de porter secours à une personne en danger de l'article 223-6 alinéa 2 du Code pénal[464]. La sanction de ce comportement sous le fondement d'une atteinte à la vie privée a fait toutefois l'objet de critiques[465] du fait que l'atteinte observée ne correspondait pas pleinement aux éléments matériels décrits à l'article 226-1 du Code pénal. Les interrogations portaient en premier lieu sur l'élément matériel de l'infraction exigeant que la prise d'image résulte d'un lieu privé. En l'occurrence, les juges déduirent la réalisation de cet élément matériel du fait que la salle de classe n'était « *accessible qu'aux personnes autorisées* ». En second lieu, les interrogations s'attachaient à la condition d'atteinte à la vie privée formulée par le premier alinéa de l'article 226-1 du Code pénal qui punit « *le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui* ». Or, l'atteinte à l'intimité de la vie privée est à la fois une composante de

[464] Ainsi, en avril 2006, une enseignante avait été agressée par l'un de ses élèves au sein même de sa salle de classe et la scène avait été filmée et diffusée par un autre élève dans l'établissement scolaire. L'auteur de la diffusion des images a été condamné à un an de prison dont six mois avec sursis pour atteinte à la vie privée et non-assistance à personne en danger. T. corr. Versailles, 27 juin 2007 : *CCE* n° 11, novembre 2007, A. LEPAGE comm. 137.

[465] V. en ce sens : A. LEPAGE, « Les vertus du droit commun, ou le happy slapping sanctionné sans le secours du nouvel article 222-33-3 du Code pénal », *CCE* n° 11, novembre 2007, comm. 137.

l'élément matériel et constitue également l'élément moral de l'infraction[466]. Le Professeur Agathe Lepage observe ainsi « *qu'il ne serait guère réaliste de soutenir que cette jeune femme a été atteinte dans sa vie privée. La scène se déroulait, rappelle le tribunal, "dans la salle de classe pendant un cours"* »[467]. Au final, la deuxième qualification retenue de non-assistance à personne en danger paraissait en l'espèce davantage adaptée pour poursuivre l'auteur de la vidéo.

L'utilisation des articles 226-1 et 223-6 alinéa 2 du Code pénal ont alors permis au juge pénal d'assurer une sanction des comportements de *happy slapping* avant l'entrée en vigueur du délit spécifique de l'article 222-33-3 du Code pénal. Cependant, l'utilisation de ces délits revenait à étendre un peu trop le champ répressif de ces incriminations, en particulier celui du délit de l'article 226-1. Il aurait été alors davantage judicieux de poursuivre ces faits sous d'autres fondements, d'autant plus que certaines incriminations préexistantes envisageaient déjà la répression de comportements similaires.

B. Des incriminations similaires préexistantes

147. La diffusion d'images violentes susceptibles d'être perçues par des mineurs. Au regard des incriminations préexistantes, certaines d'entre elles permettaient avant l'entrée en vigueur de l'article 222-33-3 du Code pénal de poursuivre un individu pour les faits spécifiques de diffusion d'images à caractère violent. Par exemple, l'article 227-24 du Code pénal réprime les faits de diffusion de messages ou d'images violentes ou portant atteinte à la dignité de la personne sur internet lorsque ces images sont susceptibles d'être perçues par des mineurs. En l'occurrence, la large présence des mineurs sur les sites de réseaux sociaux amène facilement au constat que la diffusion de telles images sur un site de ce type peut être perçue par des mineurs, d'autant plus lorsque l'image résulte et vise des réseaux d'individus issus d'environnements scolaires.

148. La diffusion des circonstances d'un crime ou d'un délit. Plus spécifiquement encore, dans le but d'éviter que la victime d'une infraction pénale ne souffre davantage d'une médiatisation de son malheur, la loi du 29 juillet 1881 incrimine les diffusions qui portent atteinte à sa dignité[468]. Précisément, l'article 35 *quater* de la loi du 29 juillet 1881 incrimine

[466] Crim., 7 octobre 1997, nº 96-81.485 : *Bull. crim.*, nº 324 ; *D.* 1999, p. 152, note J.-C. SAINT-PAU.
[467] A. LEPAGE, « Les vertus du droit commun, ou le happy slapping sanctionné sans le secours du nouvel article 222-33-3 du Code pénal », *CCE* n° 11, novembre 2007, comm. 137.
[468] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 572, n° 959.

précisément « *la diffusion, par quelque moyen que ce soit et quel qu'en soit le support, de la reproduction des circonstances d'un crime ou d'un délit, lorsque cette reproduction porte gravement atteinte à la dignité d'une victime et qu'elle est réalisée sans l'accord de cette dernière* ». Cet article suppose que soit préalablement démontrée l'existence de circonstances d'un crime ou d'un délit dont est victime une personne. Il n'est en l'occurrence pas nécessaire que l'infraction requise ait fait l'objet de poursuites ou d'une condamnation notamment lorsque les auteurs de l'infraction n'ont pu être identifiés ou lorsque l'action publique est éteinte en raison de leur décès[469]. Par ailleurs, le texte exige que la diffusion de telles images soit de nature à porter une atteinte à la dignité de la victime. Bien que le concept de dignité soit particulièrement difficile à définir[470], en l'occurrence une telle atteinte se déduit de la diffusion de tout élément exposant la victime en position d'affaiblissement ou d'infériorité du fait par exemple de ses blessures. Ainsi, « *d'un point de vue pratique, il semble que la dignité de la victime est bafouée chaque fois qu'il est privilégié le caractère sensationnel ou morbide d'une situation au détriment de l'information légitime du public* »[471]. Au final, le comportement incriminé par ces différents textes est particulièrement similaire aux prévisions de l'article 222-33-3 alinéa 2 du Code pénal, l'infraction paraît ainsi redondante.

§2. La méconnaissance de certains principes fondamentaux du droit pénal

149. En réaction à certains comportements rencontrés sur les sites de réseaux sociaux, le législateur est venu créer de nouvelles infractions au risque de méconnaître certains principes fondamentaux du droit pénal. Ainsi, certaines incriminations en matière terrorsite se sont vues censurées (A). Plus récemment, l'extension des infractions d'harcèlements au cas des cyberharcèlements en groupe s'avère délicate au vu du principe de personnalité de la responsabilité pénale (B).

A. La censure d'incriminations en matière terroriste

150. Le soutien au terrorisme sur les réseaux sociaux. Classiquement, le dispositif de lutte contre le terrorisme vise les actes de violence grave contre les personnes ou les biens.

[469] Circ. n° 2001-07 F1/14-05-2001, *Présentation des dispositions de la loi du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes*, *BO min. Justice* 2001, n° 82.
[470] V. sur le sujet : R. KOERING-JOULIN, « La dignité de la personne humaine en droit pénal », *in* M.-L. PAVIA et T. REVET (dir.), *La dignité de la personne humaine*, Economica 1999, p. 83.
[471] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 574, n° 966.

Toutefois, la politique répressive en matière terroriste a rapidement conduit le législateur à élargir le champ des infractions terroristes en y incluant progressivement tous les comportements susceptibles de présenter un lien avec le phénomène terroriste, notamment les infractions préparatoires ou postérieures à l'action terroriste[472]. Dès lors, autant l'action terroriste que le « *soutien* »[473] au terrorisme sont réprimés au titre de la criminalité terroriste. Cette pénalisation progressive des comportements périphériques au terrorisme permet d'appréhender sous le régime des infractions terroristes des comportements issus des sites de réseaux sociaux. En effet, si l'action terroriste implique une forme de violence qui ne peut être caractérisée par la seule utilisation d'un réseau social, certains actes de soutien au terrorisme peuvent quant à eux être constitués *via* ces nouveaux moyens de communication. Plus précisément, les réseaux sociaux en ligne favorisent une multitude de comportements en lien avec le terrorisme comme la propagation de l'idéologie terroriste, de ses techniques, le recrutement, l'apologie, l'incitation au passage à l'acte par des individus parfois isolés. L'ensemble de ces comportements se trouvent incriminés dans divers textes prévus aux articles 421-1 et suivants du Code pénal comme des actes de soutien au terrorisme.

Ces incriminations qui viennent apporter de nouvelles réponses aux comportements rencontrés sur les sites de réseaux sociaux (1) manifestent en réalité une politique répressive menée, parfois, au détriment du principe de nécessité de la loi pénale (2).

1) Des incriminations terroristes répondant aux comportements sur les réseaux sociaux

151. Certaines des incriminations terroristes prévues aux articles 421-1 et suivants du Code pénal se montrent adaptées aux comportements rencontrés sur les sites de réseaux sociaux en raison de leur lien plus ou moins direct avec le terrorisme. Cette hypothèse se vérifie concernant les incriminations de prévention du terrorisme qui peuvent se manifester sur les réseaux sociaux (a), mais surtout, concernant les incriminations d'actions individuelles à caractère terroriste (b).

[472] J. ALIX, *Terrorisme et droit pénal, étude critique des incriminations terroristes*, Nouvelle bibliothèque des thèses, Dalloz, 2010, p. 77, n° 97.
[473] Le soutien au terrorisme doit être entendu comme « *l'ensemble des actes qui contribuent, en amont ou en aval d'une action terroriste, à l'activité terroriste* » : J. ALIX, *Terrorisme et droit pénal, étude critique des incriminations terroristes*, *op. cit.*, p. 77, n° 98.

a- La manifestation d'incriminations de prévention sur les réseaux sociaux

152. La participation à un groupement terroriste. Une distinction au sein des infractions terroristes consiste à séparer les infractions de lésion supposant un résultat dommageable et d'autre part, les infractions de prévention qui n'exigent pas un tel résultat pour leur qualification[474]. Le législateur a ainsi consacré par la loi du 22 juillet 1996[475] le délit de participation à un groupement terroriste à l'article 421-2-1 du Code pénal. Selon le présent article, le délit est formé par « *le fait de participer à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un des actes de terrorisme mentionnés aux articles précédents* ». Le présent délit d'association de malfaiteurs est un délit indépendant tant des crimes préparés ou commis par ses membres que des infractions caractérisées par certains des faits qui la concrétisent[476] et constitue en conséquence un acte de soutien au terrorisme. Cette incrimination est par ailleurs particulièrement large du fait qu'il importe peu que les crimes ou délits auxquels tend l'association soient déterminés ou qu'ils demeurent imprécis[477]. Seule compte la participation consciente de la personne à un groupement ayant un projet terroriste[478]. Cette incrimination s'est alors imposée comme le pilier de la lutte contre le terrorisme en raison de sa dimension anticipatrice[479], cette dernière permettant d'ouvrir une enquête et de punir les individus seulement suspectés de projeter des actes terroristes. C'est ainsi que ce délit fait intervenir la répression très tôt dans *l'iter criminis* au risque de s'apparenter à la répression d'actes préparatoires au terrorisme.

153. Le recrutement en vue de commettre un acte terroriste. Selon l'article 421-2-4 du Code pénal créé par la loi n° 2012-1432 du 21 décembre 2012 : « *le fait d'adresser à une personne des offres ou des promesses, de lui proposer des dons, présents ou avantages quelconques, de la menacer ou d'exercer sur elle des pressions afin qu'elle participe à un groupement ou une entente prévu à l'article 421-2-1, qu'elle commette un des actes de*

---

[474] V. sur la question : A. PONSEILLE, *L'infraction de prévention en Droit pénal français*, Thèse Montpellier, 2001, p. 669 ; V. aussi P. PHILIPPOT, *Les infractions de prévention*, Thèse Université Nancy II, 1977, p. 334; J.-P. DOUCET, « Les infractions de prévention », *Gaz.Pal.* 1973, octobre, p. 764.
[475] L. n° 96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire, *JORF* n°170, 23 juillet 1996, p. 11104.
[476] Crim., 22 janvier 1986, n° 85-92.620 : *Bull. crim.* n° 29.
[477] Crim., 7 juin 1951 : *RSC* 1951, p. 666 note L. HUGUENEY – Crim., 22 août 1959 : *Bull. crim.* n° 393.
[478] V. en ce sens Y. MAYAUD, « Le crime terroriste de participation à une association de malfaiteurs : une aggravation révélée dans sa juste portée », *AJ Pénal* 2016, p. 526.
[479] J. ALIX, « Réprimer la participation au terrorisme », *RSC* 2014, p. 849.

terrorisme mentionnés aux articles 421-1 et 421-2 est puni, même lorsqu'il n'a pas été suivi d'effet ». Très proche du délit d'association de malfaiteurs prévu à l'article 421-2-1 du Code pénal, le présent délit vise à appréhender l'hypothèse où l'entreprise de persuasion du recruteur n'aurait pas été suivie d'effet. L'article 421-2-4 du code pénal fait du recrutement un délit-obstacle, sa matérialité s'observant par le seul fait de prendre des initiatives destinées à déterminer une personne à entrer dans le terrorisme, peu importe qu'elles soient ou non suivies d'effet[480].

154. Application aux réseaux sociaux. En pratique, l'utilisation d'un réseau social peut suffire à constituer les deux infractions vues ci-dessus. Dans un premier temps, l'usage d'un réseau social peut révéler l'appartenance, ou du moins la participation à un groupement terroriste. Cependant, la seule consultation d'une page en lien avec le terrorisme, même de manière habituelle, ne peut constituer en soi l'infraction de l'article 421-2-1 du Code pénal. Un véritable lien, réel ou virtuel, avec une organisation projetant un acte de terrorisme doit être démontré pour caractériser l'infraction. Une simple prise de contact sur un réseau social pour discuter d'un projet terroriste peut toutefois, au vu de la souplesse de la jurisprudence en la matière[481], suffire à caractériser l'infraction[482]. Dans un second temps, un réseau social peut parfaitement être utilisé à des fins de recrutement[483]. L'infraction de l'article 421-2-4 du Code pénal a alors vocation à s'appliquer lorsque les messages échangés sur les réseaux sociaux révèlent la volonté pour un individu d'endoctriner et de recruter une personne dans un groupement à caractère terroriste. En conclusion, les infractions de participation à un groupement terroriste et de recrutement en vue de commettre un acte terroriste ne peuvent se déduire d'une action passive de consultation d'espaces en lien avec de tels groupements sur les réseaux sociaux. Il est nécessaire de démontrer la présence de liens concrets qui se matérialisent par l'échange de messages ou de correspondances démontrant par leur teneur l'une ou l'autre des infractions.

---

[480] Y. MAYAUD, Rép. pén. Dalloz, janvier 2018 (mis à jour juillet 2019), *V°* terrorisme - infractions, n° 105.

[481] V. par exemple : Crim., 21 mai 2014, n° 13-83758 ; *AJ Pénal* 2014, p. 528, note P. de COMBLES de NAYVES ; *Dr. pén.* 2014, n° 7-8, comm. n° 106, M. VERON ; *RSC* 2014, p. 849, note J. ALIX.

[482] P. de COMBLES de NAYVES, « Sauf en matière terroriste », *AJ Pénal* 2014, p. 528.

[483] Sur les méthodes de recrutement terroriste sur les réseaux sociaux V. l'enquête du journaliste G. KRISTANADJAJA, L'Obs avec Rue 89, le 21 octobre 2014 ; V. également D. THOMSON, *Les français jihadistes*, Les Arènes, 2014, p. 91 et suiv.
<http://rue89.nouvelobs.com/2014/10/21/comment-facebook-mis-voie-djihad-255616>

b- L'incrimination d'actions individuelles à caractère terroriste

155. L'entreprise individuelle de terrorisme. Les réseaux sociaux hébergent à la fois des groupes terroristes structurés répondant à la conception objective de l'entreprise terroriste[484] et à la fois des individus esseulés, décrits comme des loups solitaires ne rentrant pas dans la conception classique du terrorisme. Des études[485] ont alors proposé l'adaptation du dispositif pénal à ces nouvelles formes de terrorisme par autoradicalisation. Ainsi, la loi n° 2014-1353 du 13 novembre 2014 visant à renforcer les dispositions relatives à la lutte contre le terrorisme[486], est venue ajouter aux infractions terroristes, l'infraction d'entreprise individuelle de terrorisme marquant sa volonté de ne pas restreindre la répression du terrorisme à un acte de nature collective. Cette nouvelle incrimination vient prendre en compte la préparation d'actes terroristes par un auteur unique et répond ainsi aux nouvelles formes d'actions terroristes qui ne résultent plus nécessairement d'une entreprise collective. Le délit de l'article 421-2-6 du Code pénal consacre, pour ce faire, une formulation en deux temps. Son I. est consacré à la définition de la préparation incriminée et son II. traite des infractions objets de cette préparation. La préparation se caractérise par la réalisation, dans un but terroriste, de plusieurs actes matériels qui doivent nécessairement comporter d'une part, la détention, l'acquisition ou la fabrication d'objets ou substances de nature à créer un danger pour autrui[487] et d'autre part, un autre fait matériel parmi une série d'actes : recherche de renseignements, consultation habituelle de sites terroristes, entraînement, formation au maniement des armes[488]. Ce présent délit entre, au regard de sa structure, dans la catégorie des infractions complexes, chacun des deux éléments matériels devant être distinctement

---

[484] La conception objective de l'entreprise terroriste renvoie à « *l'entreprise-structure* » ou encore à « *l'entreprise-organisation* ». À l'opposé, la conception subjective de l'entreprise terroriste renvoie à « *L'entreprise-dessein* », « *l'entreprise projet* ». V. J. ALIX, *Terrorisme et droit pénal, étude critique des incriminations terroristes*, *op. cit.*, p. 228 et suiv., n^{os} 294 et suivs.

[485] Par exemple, l'étude d'impact du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, du 8 juillet 2014 met en avant notamment « *L'hypothèse d'une personne, totalement isolée, qui dresse des plans pour commettre un acte terroriste (par exemple, elle fait des repérages sur sa cible, elle achète des livres ou consulte des sites expliquant comment fabriquer des explosifs, elle pré-rédige les communiqués qu'elle a l'intention de diffuser après l'attentat – comme un enregistrement vidéo, ou bien elle suit une formation idéologique à l'étranger ou une formation au maniement des armes à l'étranger sans qu'un lien de connexité avec la France soit démontré), sans pour autant commettre aucun délit obstacle (elle n'a pas encore acheté d'armes ou d'explosifs, elle n'a pas diffusé de message apologétiques, etc). Une telle personne ne commet en l'état aucune infraction* ». <http://www.assemblee-nationale.fr/14/projets/pl2110-ei.asp> (dernière consultation le 9 octobre 2019).

[486] L. n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, *JORF* n° 0263, 14 novembre 2014, p. 19162, texte n° 5.

[487] Le texte d'infraction prévoit ici un éventail assez large allant du simple couteau aux explosifs.

[488] H. ROUIDI, « La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme : quelles évolutions ? », *AJ Pénal*, 2014, p. 555.

qualifiés[489]. La consultation de pages ou messages terroristes sur les réseaux sociaux peut ainsi constituer un élément matériel de l'entreprise individuelle de terrorisme[490] mais en aucun cas le délit dans son entier. La seule activité sur un réseau social ne saurait donc englober dans leur ensemble les éléments constitutifs de l'infraction. Cette nouvelle incrimination vise surtout à appréhender « *les cas d'individus isolés décidant de commettre une action violente, comme l'agression à l'arme blanche* »[491].

156. L'apologie et la provocation au terrorisme. Plus proche des comportements spécifiques aux sites de réseaux sociaux, la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme[492] a transféré l'incrimination des délits de provocation à la commission d'actes terroristes et d'apologie du terrorisme depuis la loi sur la liberté de la presse vers le Code pénal[493]. Désormais, l'article 421-2-5 du Code pénal incrimine « *le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes* ». Ce texte prend en compte deux comportements bien distincts. Le premier concerne la provocation directe à la commission d'un acte de terrorisme. Il s'agit en l'occurrence de pousser autrui, en connaissance de cause, à commettre l'une des infractions terroriste prévue aux articles 421-1 et suivants du Code pénal[494]. Le second comportement, davantage de nature apologétique, est caractérisé lorsque l'auteur d'un propos légitime une des infractions prévues aux articles 421-1 et suivants du Code pénal ou valorise son auteur[495]. Ces deux comportements prévus au sein d'une même infraction peuvent en l'occurrence se réaliser par le biais de l'action d'un seul individu sur un réseau social. Ces

[489] Selon le Professeur Yves Mayaud, « *l'infraction complexe est matériellement constituée par une pluralité d'actes de nature différente, chacun de ces actes ne pouvant à lui seul la caractériser, de même que, par leur différence de nature, ils ne procèdent pas de la répétition, mais de la complémentarité* ». Y. MAYAUD, Rép. pén. Dalloz, janvier 2018 (mis à jour juillet 2019), *V°* Terrorisme, n° 99.

[490] Art. 421-2-6 I 2° c) C. pén. : « *Consulter habituellement un ou plusieurs services de communication au public en ligne ou détenir des documents provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie* ».

[491] Étude d'impact du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, du 8 juillet 2014, p. 48. <http://www.assemblee-nationale.fr/14/projets/pl2110-ei.asp> (dernière consultation le 9 octobre 2019).

[492] L. n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, art. 5.

[493] Selon le Professeur Yves Mayaud, ce transfert s'explique par le fait que les comportements incriminés ne caractérisent pas un abus de la liberté mais un « *vecteur principal de propagande, de recrutement et d'incitation* » à la commission d'actes terroriste. Y. MAYAUD, Rép. pén. Dalloz, janvier 2018 (mis à jour juillet 2019), *V°* Terrorisme-Infractions, n° 109.

[494] En l'espèce il ne peut s'agir que d'une provocation non suivie d'effets, sinon elle serait envisagée comme une forme de complicité.

[495] E. DREYER, « L'opportunité d'une sortie des infractions de presse de la loi du 29 juillet 14881 au regard d'un exemple précis : le cas du délit d'apologie du terrorisme et de provocation aux actes de terrorisme », *in* N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, Coll. Grands Colloques, 2017, p. 38.

sites constituent en effet un vivier certain d'actes de provocation ou d'apologie au terrorisme. Ceux-ci peuvent s'y retrouver sous diverses formes, notamment par la création de groupes ou de pages Facebook[496] ou encore, par la publication de vidéos, d'images ou de paroles, mais aussi par des messages ou de simples hashtags[497]. Dès lors, les sites de réseaux sociaux constituent non seulement un foyer de recrutement pour les cellules terroristes mais également d'excellents outils de propagande et de prosélytisme[498]. Un rapport remis au ministre de l'intérieur[499] identifie à ce titre cinq profils sur les réseaux sociaux en ligne « *prêts à croire et à s'engager* » dans une mouvance terroriste[500]. Le jeune public est particulièrement visé en la matière, selon David Thomson les réseaux sociaux ont ainsi permis l'apparition du phénomène de « *Lol Jihad* »[501] qui vise à rendre attractif à l'égard de ce public les mouvances radicales par des discours fondés sur l'humour, la provocation.

157. La consultation habituelle de sites terroristes. Plus loin encore dans cette logique, le législateur est venu créer par la loi n° 2016-731 du 3 juin 2016[502] une nouvelle infraction rattachée au terrorisme à l'article 421-2-5-2 du Code pénal. Dans sa version initiale l'infraction prévoyait la sanction du fait de « *consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie* ». Cette incrimination avait pour but d'enrayer la stratégie de propagande mise en place

[496] Par exemple *SLF, le magazine des Salafi* qui dénombre 3 546 mentions j'aime.

[497] Par exemple, au lendemain de l'attaque de Charlie Hebdo des centaines de tweet faisant l'apologie du terrorisme ont été observés sous les hashtag *#jesuiskouachi* ou *#jesuiscoulibaly*. L'humoriste controversé Dieudonné fut ainsi mis en examen du chef d'apologie au terrorisme à la suite de sa déclaration sur sa page Facebook « *je me sens Charlie Coulibaly* ». V. T. LEGRAIN, « L'utilisation des réseaux sociaux par les bandes criminelles », *Sécurité globale*, 2016/1, n° 5, p. 103.

[498] T. LEGRAIN, « L'utilisation des réseaux sociaux par les bandes criminelles », *Sécurité globale*, 2016/1, n° 5, p. 103 : « *D'après le quotidien belge La libre Belgique, une étude de l'université de Milan réalisée entre le 1er juillet et le 22 octobre 2014, a conclu que la Belgique serait le pays européen d'où partirait en majeur partie la propagande en faveur de Daesh sur les réseaux sociaux (31 % des message arabophones postés en Belgique sont favorables à cette organisation terroriste contre 20 % en France, 19.7 % en Irak, 7.6% en Syrie)* ».

[499] D. BOUZAR, C. CAUPENNE, S. VALSAN, « La Métamorphose opérée chez le jeune par les nouveaux discours terroristes », recherche-action sur la mutation du processus d'endoctrinement et d'embrigadement dans l'islam radical, novembre 2014, p. 82-86.

[500] Les différents profils identifiés sont les suivants : « *1. Le chevalier héroïque : celui qui a besoin de reconnaissance ; 2. Mère Teresa ou celui qui part pour la cause humanitaire ; 3. Le porteur d'eau : celui qui est en quête d'identité ; 4. Le Call of Duty : cible majoritairement masculine désireuse de combattre ; 5. Zeus ou celui qui cherche la toute-puissance, un individu sans limite* ».

[501] D. THOMSON, *Les français jihadistes*, Les Arènes, 2014, p. 89.

[502] Art 18, Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF n°0129 du 4 juin 2016 texte n° 1.

par les groupes terroristes sur les sites de réseaux sociaux. La création de ce texte était alors justifiée par le souhait de déceler par ce moyen l'individu en cours de radicalisation. Cette incrimination visait à ce titre particulièrement les sites de réseaux sociaux qui constituent aisément « *un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme* »[503]. De plus, la manifestation d'adhésion à l'idéologie est facilement observable sur ces sites en raison des outils mis à la disposition de leurs utilisateurs tels que le partage ou le « *like* » de contenus diffusant cette idéologie. « *Cette nouvelle incrimination est, comme beaucoup, éminemment conjoncturelle, en ce qu'elle répond à un épiphénomène mis en évidence ces dernières années, pour ne pas dire ces derniers mois* » observe alors le Professeur Jean-Baptiste Perrier[504]. Au final, cette infraction fait intervenir la répression avant tout passage à l'acte et même avant même tout projet de passage à l'acte. Cette volonté répressive réalisée au détriment du principe de nécessité de la loi pénale a fondé la censure de ce texte.

2) Une volonté répressive au détriment du principe de nécessité de la loi pénale

158. Une politique répressive en matière de terrorisme. Les différentes infractions de prévention du terrorisme engagées depuis ces dernières années ont fait l'objet de nombreuses critiques doctrinales[505]. Par principe, les actes se situant avant le commencement d'exécution sur *l'iter criminis*, à l'image des actes préparatoires, doivent demeurer en dehors du champ de la répression du fait qu'il s'agit d'actes univoques ne permettant pas de révéler de manière certaine l'intention infractionnelle[506]. Ces infractions de prévention entrent par ailleurs en

[503] V. sur le sujet : T. LEGRAIN, « L'utilisation des réseaux sociaux par les bandes criminelles », *Sécurité globale*, vol. 5, n° 1, 2016, pp. 97-111 ; A. GOZLAN « Facebook : de la communauté virtuelle à la haine », *Topique*, vol. 122, n° 1, 2013, pp. 121-134 ; M. GUIDERE, « Le terrorisme avant et après l'État islamique », *Confluences Méditerranée*, vol. 102, n° 3, 2017, pp. 65-74.

[504] J.-B. PERRIER, « l'adaptation des incriminations », *RSC* 2017, p. 373.

[505] V. notamment : J. ALIX, « Réprimer la participation au terrorisme », *RSC* 2014, p. 849 ; Y. MAYAUD, Rép. pén. Dalloz, janvier 2018 (mis à jour juillet 2019), *V°* Terrorisme – infractions ; N. CATELAN et J.-B. PERRIER, « L'entreprise individuelle de terroriste et les axiomes du Conseil constitutionnel », *D.* 2017, p. 1180 ; J-B PERRIER, « l'adaptation des incriminations », *RSC* 2017 p. 373 ; P. SÉGUR, « Le terrorisme et les libertés sur l'internet », *AJDA*, février 2015, n° 3, p. 160-165 ; C. LAZERGES, « La participation criminelle », p.11-30 *in Réflexions sur le nouveau Code pénal*, sous la direction de C. Lazerges, Paris, Pédone, 1995 ; A. PONSEILLE, « Les infractions de prévention, Argonautes de la lutte contre le terrorisme », *RDLF*, 3 juillet 2017, n° 2017-26.
Disponible sur <http://www.revuedlf.com/droit-penal/les-infractions-de-prevention-argonautes-de-la-lutte-contre-le-terrorisme/#_ftn136> (dernière consultation le 9 octbre 2019).

[506] A. PONSEILLE, « Les infractions de prévention, Argonautes de la lutte contre le terrorisme », *RDLF*, 3 juillet 2017, n° 2017-26.
Disponible sur <http://www.revuedlf.com/droit-penal/les-infractions-de-prevention-argonautes-de-la-lutte-contre-le-terrorisme/#_ftn136> (dernière consultation le 9 octobre 2019).

conflit avec le régime de la complicité, défini à l'article 121-7 du Code pénal, qui assimile au complice celui qui aide à la préparation[507] et celui qui provoque[508] à l'infraction. Ainsi, la structure matérielle des incriminations relatives au terrorisme entre en contradiction avec les règles de droit pénal général concernant la complicité[509]. Pis encore, au travers de ces incriminations, le droit pénal vient appréhender l'intention coupable[510] contrevenant au principe selon lequel « *le droit pénal ne s'occupe pas du for intérieur qui est le domaine réservé de la morale et de la religion* »[511]. Ces nouvelles infractions terroristes ne traduisent donc pas une carence structurelle du droit pénal mais plutôt une politique répressive intervenant en réaction à des évènements d'une gravité certaine. Certains auteurs[512] ont alors critiqué cette volonté du législateur et celle des praticiens de renforcer le dispositif pénal de lutte contre le terrorisme[513], le droit de punir reconnu à l'État étant modéré par le principe de nécessité de la sanction pénale.

159. La validation par le Conseil constitutionnel du délit d'entreprise individuelle de terrorisme. À l'occasion de sa décision du 7 avril 2017 statuant sur une question prioritaire de constitutionnalité[514], le Conseil constitutionnel n'a apporté qu'une correction minime à l'incrimination d'entreprise individuelle de terrorisme prévue à l'article 421-2-6 du Code pénal. La censure porte sur les termes « *de rechercher* » se retrouvant au I. 1° de la présente incrimination en ce qu'ils pourraient conduire à réprimer « *des actes ne matérialisant pas, en eux-mêmes, la volonté de préparer une infraction* »[515]. Le Conseil rappelle que « *le législateur ne saurait, sans méconnaître le principe de nécessité des délits et des peines, réprimer la seule intention délictueuse ou criminelle* »[516]. Ce tel constat provient du fait que l'infraction prévue à l'article 421-2-6 ne réprime ni une infraction intégralement consommée,

[507] C. pén., art. 121-7 al. 1er.
[508] C. pén., art. 121-7 al. 2nd.
[509] C. LAZERGES, « La participation criminelle », p.11-30 *in Réflexions sur le nouveau Code pénal*, sous la direction de C. Lazerges, Paris, Pédone, 1995.
[510] J.-B. PERRIER, « L'adaptation des incriminations », *RSC* 2017, p. 373
[511] C. BECCARIA, *Des délits et des peines*, ENS éd., 2009.
[512] En ce sens : J. ALIX, « Réprimer la participation au terrorisme », *RSC* 2014, p. 849 ; J.-B. PERRIER, « l'adaptation des incriminations », *RSC* 2017 p. 373 ; M. Massé, « La criminalité terroriste », *RSC* 2012, p. 89.
[513] Madame Anne Ponseille décrivant une intervention pénale « *hyper-anticipée* » : A. PONSEILLE, « Les infractions de prévention, Argonautes de la lutte contre le terrorisme », *RDLF*, 3 juillet 2017, n° 2017-26. Disponible sur <http://www.revuedlf.com/droit-penal/les-infractions-de-prevention-argonautes-de-la-lutte-contre-le-terrorisme/#_ftn136> ; Michel Massé relevant quant à lui une « *aporie du droit pénal face au terrorisme, en tout cas du droit pénal « classique »* (…) *construit sur le modèle de la responsabilité individuelle d'un auteur sanctionné pour avoir matériellement et en toute connaissance de cause commis un acte qualifié criminel en général directement dommageable pour les personnes ou les biens* » : M. MASSE, « La criminalité terroriste », *RSC* 2012, p. 89.
[514] Cons. const., 7 avril 2017, QPC n° 2017-625
[515] Cons. const., 7 avril 2017, QPC n° 2017-625, §17.
[516] Cons. const., 7 avril 2017, QPC n° 2017-625, §13.

ni même sa tentative mais de simples actes préparatoires[517]. Les sages préconisent alors un nécessaire fait matériel venant corroborer cette intention[518]. Cette critique ne porte cependant que sur le comportement consistant à « *rechercher des objets ou des substances de nature à créer un danger pour autrui* » manifestant une seule intention et non une matérialité. La censure du Conseil constitutionnel est donc de faible importance, ce dernier considérant que, pour le reste, l'infraction d'entreprise terroriste individuelle répond au principe de nécessité de la loi pénale[519].

160. La censure par le Conseil constitutionnel du délit de consultation habituelle de sites terroristes. À l'inverse, le Conseil constitutionnel s'est montré plus intransigeant avec l'infraction de consultation habituelle de sites terroristes. Les sages ont ainsi censuré la première version du texte au nom du principe de nécessité de la loi pénale cette nouvelle incrimination en précisant notamment que « *les dispositions contestées n'imposent pas que l'auteur de la consultation habituelle des services de communication au public en ligne concernés ait la volonté de commettre des actes terroristes ni même la preuve que cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ces services* »[520]. En réaction à la censure du Conseil constitutionnel, le législateur est venu proposer une nouvelle version du présent délit en y ajoutant cette fois que la consultation doit s'accompagner « *d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service* »[521]. Cependant, le Conseil constitutionnel est venu une nouvelle fois censurer ce délit dans sa décision du 15 décembre 2017[522] en affirmant que « *les dispositions contestées portent une atteinte à l'exercice de la liberté de communication qui n'est pas nécessaire, adaptée et proportionnée* ».

B. L'extension délicate des délits de harcèlement

161. Une amplification des harcèlements sur les réseaux sociaux en ligne. Le cyberharcèlement est une forme spécifique de harcèlement qui correspond à une intrusion

[517] N. CATELAN et J.-B. PERRIER, « L'entreprise individuelle de terroriste et les axiomes du Conseil constitutionnel », *op. cit.*, p. 1180.
[518] Cons. const., 7 avril 2017, QPC n° 2017-625, §16.
[519] Selon le conseil constitutionnel : « *eu égard à la gravité toute particulière que revêtent par nature les actes de terrorisme et alors même que les dispositions contestées répriment de simples actes préparatoires à la commission d'une infraction, le reste de l'article 421-2-6 (...) ne méconnaît pas le principe de nécessité des délits et des peines* ». Cons. const., 7 avril 2017, n° 2017-625, § 18.
[520] Cons. const. 10 février 2017, QPC n° 2017-611, § 14 ; *AJ Pénal* 2017. 237, obs. J. Alix ; *CCE* n° 4, avril 2017, comm. 35 A. LEPAGE ; V. la décision de renvoi, Crim. 29 novembre 2016, n° 16-90.024.
[521] L. n° 2017-258 du 28 février 2017 relative à la sécurité publique, JORF n°0051,1 mars 2017, art 24.
[522] Cons. const., 15 décembre 2017, n° 2017-682 QPC : JurisData n° 2017-025795 ; Dr. pén. n° 2, février 2018, comm. 22, P. CONTE ; *CCE* n° 2, février 2018, comm. 13 A. LEPAGE.

continue et menaçante se réalisant dans l'espace numérique. Les cyber-harceleurs utilisent les moyens de communication en ligne comme l'outil de leur activité, la technologie leurs permettant de réaliser de manière répétée des intrusions indésirables en tous lieux et à tout moment. Un rapport du Conseil de l'Europe sur le harcèlement[523], distingue plusieurs formes de cyberharcèlement. Ce dernier peut d'abord relever d'une communication directe avec la victime par l'envoi de messages menaçants, désagréables ou déstabilisants. À l'inverse, un cyberharcèlement peut également se manifester par une communication indirecte avec la victime consistant à poster ou diffuser dans des environnements en ligne des informations la concernant et pouvant aboutir à une représentation déformée de sa personne. Le phénomène du cyberharcèlement qui concerne majoritaire les femmes s'est considérablement développé avec l'utilisation massive des réseaux sociaux en ligne[524]. Au sein de l'Union européenne, 11% des femmes rapportent avoir été victimes de harcèlements en ligne depuis l'âge de 15 ans. Plus généralement, 73% des femmes rapportent avoir reçu des avances inappropriées sur les réseaux sociaux de la part de personnes qu'elles ne connaissaient pas[525]. L'espace numérique et plus particulièrement les sites de réseaux sociaux qui favorisent la mise en relation et les échanges entre personnes ont ainsi contribué à amplifier les comportements de harcèlement qui se retrouvent désormais largement à l'échelle numérique.

Sur ce point, l'extension progressive du dispositif pénal en matière de harcèlements apparaît justifiée du fait qu'elle permet de mieux appréhender les cas de cyberharcèlements (1). Cependant, plus récemment, la prise en compte particulière du cyberharcèlement en groupe témoigne d'une volonté d'adapter les incriminations préexistantes aux pratiques des « *raids numériques* » rencontrées sur les sites de réseaux sociaux au détriment du principe de personnalité de la responsabilité pénale (2).

---

[523] Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336.

[524] Plusieurs études rapportent ce phénomène : *En finir avec l'impunité des violences faites aux femmes en ligne : une urgence pour les victimes*, Rapport n° 2017-11-16-VIO-030 du Haut Conseil à l'égalité entre les femmes et les hommes, 16 novembre 2017, p. 32 ; *UN Broadband/Commission for Digital Development Working Group on broadband and Gender, Report* « Cyber Violence against Women and Girls », 2015 ; Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336.

[525] Chiffres cités *in* : *En finir avec l'impunité des violences faites aux femmes en ligne : une urgence pour les victimes*, Rapport n° 2017-11-16-VIO-030 du Haut Conseil à l'égalité entre les femmes et les hommes, 16 novembre 2017, p. 32.

1) L’extension justifiée du dispositif pénal aux cyberharcèlements

162. Une incrimination générale de harcèlement applicable au cyberespace. Le harcèlement peut se définir de manière générale comme la répétition d’actes d’intrusion dans la vie d’une personne qui vont s’intensifiant au fil du temps[526]. Cette intrusion s’observe dans diverses environnements, elle peut être issue d’une relation professionnelle[527] mais également conjugale[528], plus généralement, les faits de harcèlement peuvent concerner tous milieux qu’ils soient associatifs, sportifs, universitaires, scolaires. Cependant, il arrive également que l’auteur du harcèlement soit une simple connaissance ou même un parfait inconnu pour la victime. Cette dernière hypothèse se rencontre particulièrement avec les harcèlements en ligne qui sont souvent le fait de personnes étrangères à la victime[529]. Or, les délits de harcèlement se sont progressivement généralisés de manière à pouvoir intégrer dans leur champ répressif toutes les formes de harcèlements (a). Cette adaptation du champ d’application de ces délits se couple avec une sévérité pénale accrue à l’égard des harcèlements commis par voie numérique (b).

a- La généralisation progressive des délits de harcèlement

163. Une définition indépendante des relations de travail ou des relations familiales. De manière à répondre efficacement aux formes de harcèlement rencontrées sur internet, et particulièrement sur les sites de réseaux sociaux, il est indispensable que les incriminations de harcèlement moral et sexuel dépassent le seul cadre des relations professionnelles ou conjugales afin de recouvrir l’ensemble des comportements observés. Ce premier enjeu est relevé par le cadre général du délit de harcèlement sexuel (i) et par l’introduction d’un délit de harcèlement moral général (ii).

i. Le cadre général du délit de harcèlement sexuel

164. Initialement, la présence d’une relation d’autorité. Le délit de harcèlement sexuel est apparu au moment de l’entrée en vigueur du Code pénal du 1er mars 1994 à l’article 222-33 disposant : « *le fait de harceler autrui en usant d’ordres, de menaces ou de contraintes, dans le but d’obtenir des faveurs de nature sexuelle, par une personne abusant de*

[526] Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336, p. 1.
[527] Pour une incrimination spécifique du harcèlement au travail v. : C. pén., art. 222-33-2.
[528] Pour une incrimination spécifique du harcèlement conjugal v. : C. pén., art. 222-33-2-1.
[529] Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336, p. 6, n° 8.

l'autorité que lui confèrent ses fonctions, est puni d'un an d'emprisonnement et de 100 000 F d'amende ». La loi n° 98-468 du 17 juin 1998[530] est venue préciser cette définition en ajoutant aux moyens de commission de l'infraction les « *pressions graves* », de sorte que les comportements non constitutifs d'ordres, de contraintes ou de menaces relèvent également du champ de l'incrimination[531]. Dans sa version primitive, le délit de harcèlement sexuel était donc doublement restreint : d'une part parce qu'il ne concernait que les relations de travail, d'autre part du fait qu'il ne pouvait être issu que d'une relation d'autorité.

165. Ensuite, la généralisation outrancière du délit de harcèlement sexuel. Cependant, la loi n° 2002-73 du 17 janvier 2002[532] est venue étendre considérablement le champ d'application de l'incrimination de harcèlement sexuel en supprimant dans un premier temps l'énumération des moyens permettant la commission de l'infraction et dans un second temps, la référence à la relation d'autorité, de sorte que l'incrimination était restreinte aux termes suivants : « *le fait de harceler autrui dans le but d'obtenir des faveurs de nature sexuelle est puni d'un an d'emprisonnement et de 15000 euros d'amende* ». Cette définition manifestement tautologique[533] a toutefois été censurée par le Conseil constitutionnel dans sa décision du 4 mai 2012[534], ce dernier la considérant comme insuffisante au regard du principe de légalité des délits et des peines qui impose une définition clair et précise des éléments constitutifs de l'infraction[535].

166. Désormais, une généralisation encadrée par une définition de l'acte incriminé. Dans le souci de suivre les recommandations du Conseil constitutionnel, la loi n° 2012-954 du 6 août 2012[536] est venue poser les bases d'une nouvelle définition du harcèlement sexuel respectant les exigences du principe de légalité criminelle, encore complétée postérieurement par la loi n° 2018-703 du 3 août 2018[537]. L'article 222-33 I. dispose dorénavant : « *le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste qui soit portent atteinte à sa dignité en*

[530] L. n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, *JORF* n° 0139, 18 juin 1998, p. 9255, Art. 11.
[531] E. DREYER, *Droit pénal spécial*, ellipse, 3ème éd., 2016, p. 160, n° 347.
[532] L. n° 2002-73 du 17 janvier 2002 de modernisation sociale, *JORF*, 18 janvier 2002, p. 1008, Art. 179.
[533] Pour une critique de la rédaction de l'incrimination de harcèlement sexuel issue de la loi n° 2002-73 du 17 janvier 2002 : v. P. CONTE, « Une nouvelle fleur de légistique : le crime en boutons. À propos de la nouvelle définition du harcèlement sexuel », *JCP* G n° 30, 24 juillet 2002, act. 320.
[534] Cons. Const., 4 mai 2012, QPC n° 2012-240.
[535] Pour une justification de la censure du Conseil constitutionnel : v. S. DETRAZ, « Harcèlement sexuel : justification et portée de l'inconstitutionnalité », *D.* 2012, p. 1372.
[536] L. n° 2012-954 du 6 août 2012 relative au harcèlement sexuel, *JORF* n° 0182 du 7 août 2012 p. 12921, Art. 1.
[537] L. n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, *JORF* n° 0179 du 5 août 2018, Art. 11.

raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante ». Cette nouvelle définition du harcèlement sexuelle ne réinstaure donc pas un rapport d'autorité comme condition de l'infraction, cette dernière se caractérisant peu importe le contexte des agissements, qu'ils relèvent du monde du travail, de milieux sportifs ou scolaires[538]. Le harcèlement sexuel devient multidirectionnel[539] : il peut être vertical ou horizontal, il peut également être caractérisé indépendamment de tout rapport d'autorité, la seule condition posée par la loi est qu'il vise une personne[540]. Par ailleurs, le texte d'incrimination bénéficie d'une portée générale en raison de son indifférence aux moyens ou supports de commission de l'infraction. Les faits de harcèlements peuvent résulter d'actes physiques mais également de paroles orales ou écrites, peu importe qu'elles soient proférés publiquement ou non sur un support matériel ou immatériel[541].

167. La portée générale du délit de harcèlement sexuel est toutefois contrebalancée par une définition plus étoffée du comportement incriminé. Le comportement de harcèlement sexuel consiste à imposer de façon répétée des propos ou comportements à connotation sexuelle ou sexiste. Cette nouvelle définition affirme ainsi que le harcèlement sexuel est une infraction d'habitude supposant la répétition d'actes. En outre, ces comportements ou propos répétés doivent recevoir une connotation « *sexuelle ou sexiste* ». Il s'agit en l'occurrence de deux réalités distinctes. D'un côté, le propos ou comportements à connotation sexuelle présentent une dimension sexuelle, ce qui implique que ces derniers soient nécessairement relatifs à l'activité sexuelle. D'un autre côté, les actes sexistes se définissent davantage « *comme tout agissement lié au sexe d'une personne* »[542] et revêtent en conséquence une réalité plus large que les propos à connotation sexuelle. Pour finir, le comportement de harcèlement sexuel doit soit porter atteinte à la dignité de la personne en raison de leur caractère dégradant ou humiliant, soit créer à son encontre une situation intimidante, hostile ou offensante. Le harcèlement n'a donc plus comme objectif l'obtention de faveurs sexuelles, il est désormais

[538] E. DREYER, *Droit pénal spécial*, ellipse, 3ème éd., 2016, p. 161, n° 350.
[539] P. MISTRETTA, Rép. pén. Dalloz, *V°* Harcèlement, n° 27.
[540] Précisons toutefois que même si le texte d'incrimination ne fait plus référence à l'abus d'autorité conféré par les fonctions au titre des modalités matérielles constitutives du délit de harcèlement sexuel, l'existence d'un lien d'autorité demeure en pratique une donnée fréquemment utilisée par le juge pour déduire la qualification de l'infraction. V. Crim., 16 novembre 2016, nº 16-82.377 : Publié au Bulletin ; cité *in* : P. MISTRETTA, Rép. pén. Dalloz, *V°* Harcèlement, n° 27.
[541] Par exemple, la jurisprudence retient la qualification de harcèlement sexuel lorsqu' une personne a « *de manière insistante et répétée, en dépit du refus des salariées de céder à ses avances, formulé, verbalement ou par messages électroniques (SMS), des propositions explicites ou implicites de nature sexuelle* ». Crim. 18 novembre 2015, nº 14-85.591 : *Bull. crim.* n° 840 ; cité *in* : P. MISTRETTA, Rép. pén. Dalloz, *V°* Harcèlement, n° 21.
[542] C. trav., Art. L1142-2-1.

punissable lorsqu'il entraîne une atteinte à la dignité de la victime, plus précisément, une atteinte à son intégrité morale[543].

ii. L'introduction d'un délit de harcèlement moral général

168. Une première incrimination dépendante d'un environnement de travail. Le harcèlement moral est d'abord défini au sein du Code pénal dans le cadre de la relation de travail. L'article 222-33-2 définit ainsi le harcèlement moral comme « *le fait de harceler autrui par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel, est puni de deux ans d'emprisonnement et de 30 000 € d'amende* »[544]. Les auteurs potentiels de ce type de harcèlement sont possiblement tous les acteurs du monde du travail ou intervenants à l'occasion d'une relation de travail. Le plus souvent, le harceleur est un supérieur hiérarchique de la victime, il s'agit alors d'un harcèlement moral vertical descendant. Le harcèlement peut également être horizontal lorsqu'il résulte d'une simple relation de travail entre collègues[545]. Enfin, le harcèlement peut également être vertical ascendant lorsque le harceleur est le subordonné de la victime[546].

169. Une deuxième incrimination dépendante d'une relation conjugale. Le législateur est également venu prévoir par la loi n° 2010-769 du 9 juillet 2010[547] une deuxième forme de harcèlement en incriminant à l'article 222-33-2-1 du Code pénal « *le fait de harceler son conjoint, son partenaire lié par un pacte civil de solidarité ou son concubin par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale* ». Ce type de harcèlement est donc spécifique aux relations de couple entre conjoints, partenaires ou concubins.

[543] E. DREYER, *Droit pénal spécial*, ellipse, 3ème éd., 2016, p. 162, n° 351.
[544] Créé par la loi n° 2002-73 du 17 janvier 2002 de modernisation sociale, *JORF* 18 janvier 2002, p. 1008, art. 170.
[545] V. par exemple : Rennes, 31 mai 2007 : *AJ Pénal* 2007, p. 376.
[546] Crim., 6 décembre 2011, nº 10-82.266 : *JCP* 2012, nº 410, note P. MISTRETTA.
[547] L. n° 2010-769 du 9 juillet 2010 relative aux violences faites spécifiquement aux femmes, aux violences au sein des couples et aux incidences de ces dernières sur les enfants, *JORF* n° 0158, 10 juillet 2010, p. 12762, art. 31.

170. L'adoption d'une troisième incrimination à portée générale. Le législateur a finalement adopté par la loi n° 2014-873 du 4 août 2014[548] un texte d'infraction venant incriminer de manière générale le harcèlement moral. L'article 222-33-2-2 sanctionne « *le fait de harceler une personne par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale* ». À la lecture de l'incrimination, cette dernière suppose dans un premier temps la démonstration d'agissements répétés, de quelque nature qu'ils soient, sans aucune référence à un contexte professionnel ou familial. Cette généralisation du champ d'application permet ainsi de poursuivre tout types de harcèlements, y compris ceux rencontrés dans les milieux scolaires, universitaires ou encore associatifs, que la victime soit majeure ou mineure. Dans un second temps, pour que l'infraction soit constituée, ces agissements doivent aboutir à une dégradation de la santé physique ou mentale de la victime. Il s'agit alors d'une infraction matérielle exigeant de démontrer que le résultat voulu par l'auteur ait effectivement été atteint[549].

b- Une sévérité pénale particulière à l'égard des harcèlements commis par voie numérique

171. La communication numérique rentrant dans les prévisions des incriminations de harcèlement. Le terme harcèlement fait appel à une pluralité de comportements qui peuvent revêtir des aspects bien divers. Les incriminations relatives aux harcèlements prévoient de manière large que tout « *propos ou comportements* » peuvent être à l'origine de harcèlements. L'étendue des actes entrant sous les définitions pénales du harcèlement sexuel ou moral permet d'intégrer les moyens de communication en ligne comme le vecteur d'actes constitutifs des délits de harcèlements. Plusieurs catégories de harcèlements peuvent être distinguées[550], notamment les harcèlements résultants d'une intrusion physique[551] ou

[548] L. n° 2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les hommes, *JORF* n° 0179, 5 août 2014, p. 12949, Art. 41.
[549] P. LEGER, « Le cyberharcèlement, une infraction adaptée à la protection de la jeunesse en ligne », *Dalloz IP/IT* 2018, p. 346.
[550] V. Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336, p. 5, n° 3.
[551] Le harcèlement par intrusion physique dans la vie d'une personne relève des pratiques « *consistant à suivre cette personne, à la surveiller, à rôder près de chez elle, à l'aborder directement, à entrer par effraction dans son logement, à se rendre sur son lieu de travail ou à aborder ses amis ou ses proches* », Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336, p. 5, n° 3, b.

digitale[552] dans la vie d'une personne mais également les harcèlements par communication[553] pouvant aller jusqu'à de véritables campagnes de dénigrements à l'encontre d'une personne[554]. Les moyens de communication numériques constituent ainsi un outil privilégié pour les harceleurs qui est cependant encadré par les incriminations existantes. L'utilisation d'un site de réseau social peut donc être, en tout ou partie, constitutive d'un délit de harcèlement.

172. L'utilisation d'un moyen de communication au public en ligne, source d'aggravation de la sanction encourue. Plus encore, l'utilisation d'un moyen de communication numérique est spécifiquement prévue comme une hypothèse d'aggravation de la sanction pénale. À ce titre, le législateur a, au moment de la création du délit de harcèlement moral général, précisé une série de circonstances aggravantes portant notamment les peines à deux ans d'emprisonnement et 30 000 euros d'amende dans le cas où le harcèlement aurait été commis par l'utilisation d'un service de communication au public en ligne[555]. Dans cette même dynamique, la loi n° 2018-703 du 3 août 2018[556] a, afin de mieux lutter contre les faits de harcèlement sexuel en ligne, ajouté une nouvelle circonstance aggravante au harcèlement sexuel, portant les peines à trois ans d'emprisonnement et à 45 000 euros d'amende, lorsqu'il a été fait utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique.

2) La prise en compte du cyberharcèlement en groupe au détriment du principe de personnalité de la responsabilité pénale

173. Une volonté de lutter contre les « *raids numériques* ». Le législateur est venu récemment enrichir encore un peu plus le dispositif pénal de lutte contre le harcèlement en

[552] Le harcèlement par intrusion peut également se réaliser de manière digitale notamment par des comportements d'usurpation d'identité consistant pour le harceleur à effectuer des démarches au nom de la victime, comme par exemple : annuler une prestation de services, commander des produits, donner sa démission ou envoyer des lettres ou des e-mails malveillants à des tiers. Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336, p. 5, n° 3, c.

[553] Le harcèlement par communication peut s'effectuer par divers moyens : téléphonique, sous forme la forme d'un écrit physique comme l'envoie d'une lettre ou électronique comme l'envoi de SMS ou la communication sur Internet. Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336, p. 5, n° 3, a.

[554] Les campagnes de dénigrement peuvent être faites dans un premier temps sous la forme de diffusion d'accusations mensongères ou de médisances, au moyen d'affiches, de tracts ou d'autres encarts publicitaires. Dans un second temps, elles peuvent également se réaliser au moyen de publication, sur internet et sur les réseaux sociaux en particulier, de documents au contenu pernicieux ou embarrassant comme des photos à caractère sexuel. Rappr. Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, 15 octobre 2013, Doc. 13336, p. 5, n° 3, e.

[555] C. pén., art. 222-33-2-2, al. 3, 4°.

[556] L. n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, *JORF* n° 0179 du 5 août 2018.

prévoyant spécifiquement l'hypothèse du cyberharcèlement en groupe appelée encore « *raids numériques* ». Ce type particulier d'agissement consiste dans l'attaque coordonnée et simultanée de plusieurs individus qui unissent leurs forces pour harceler en ligne une personne désignée[557]. Cette nouvelle forme de harcèlement en groupe permise par les sites de réseaux sociaux marque une rupture avec la conception classique de harcèlement (a) et démontre certaines limites au regard du principe de personnalité de la responsabilité pénale (b).

a- Une rupture avec la conception classique de harcèlement

174. Si le harcèlement constitue classiquement une infraction d'habitude commise individuellement (ii), désormais il constitue également une infraction d'habitude commise collectivement (ii).

i. Classiquement, une infraction d'habitude commise individuellement

175. Le harcèlement, une infraction d'habitude. Le harcèlement moral exige de manière constante au travers de ses multiples définitions « *des propos ou comportements répétés* », ce dernier constitue donc par définition une infraction d'habitude[558]. La répétition signifie dans le langage courant le fait d'exprimer à nouveau ce que l'on a déjà exprimé[559]. D'après une lecture stricte de la définition du harcèlement, seule la réitération d'un même comportement peut matérialiser l'habitude et donc constituer l'infraction. La Cour de cassation a ainsi déjà déduit la constitution d'un harcèlement moral du fait de la répétition habituelle d'actes de même nature[560]. Cependant, le harcèlement vise « *plus largement des agissements insistants, provenant toujours du même auteur et toujours dirigés contre la même victime mais sans que*

[557] M. QUEMENER, « Cyberharcèlement : quelles évolutions législatives ? », *RLDI*, 2018, nº 153.
[558] Une infraction d'habitude est une infraction complexe qui consiste en la réitération d'actes semblables dont chacun pris isolément n'est pas constitutif d'une infraction. L'infraction est donc constituée par la répétition de ces actes. C'est le cas de l'exercice illégal de la médecine (C. santé publ., art. L. 4161-1 [anc. art. L. 372]), c'est aussi le cas du recel de malfaiteurs (C. pén., art. 434-6). Pour qu'il y ait habitude, il n'est pas nécessaire que les actes aient été accomplis à l'égard de personnes différentes (V. Crim. 9 décembre 1993, nº 93-81.669 : *Bull. crim.*, nº 379). Enfin, à moins que la loi n'en prévoit autrement, il n'est pas nécessaire que le nombre d'actes soit élevé. Ainsi, deux actes peuvent constituer l'habitude, quel que soit le temps qui les a séparés (V. Crim. 21 octobre 1841 : *S.* 184, 1, 904 ; 24 mars 1944, *DA* 1944, 75, note A. LEBRUN).
[559] Dictionnaire Larousse en ligne, *V°* Répéter.
<https://www.larousse.fr/dictionnaires/francais/repeter> (dernière consultation le 9 octobre 2019).
[560] Crim., 2 octobre 2012, nº 11-82.239 ; Crim., 12 décembre 2006, nº 05-87.658. Dans ce dernier arrêt, les juges du fond avaient refusé de voir dans le fait de se moquer d'un collègue et de le qualifier de « petit nègre » un acte de harcèlement moral. Selon la Cour de cassation, les juges du fond auraient dû *« rechercher si la manière de parler du prévenu n'était pas constitutive, par son caractère habituel, d'agissements répétés ayant pour objet ou pour effet une dégradation des conditions de travail* ».

ces agissements aient besoin d'être eux-mêmes identiques »[561]. Selon cette lecture, le harcèlement ne serait plus le fruit de la répétition d'un acte mais plutôt de l'adjonction de plusieurs actes de nature différente. En réalité, le harcèlement se caractérise par « *la répétition et la systématisation d'attitudes, de paroles, de comportements, qui pris séparément peuvent paraître anodins, mais qui à la longue, sous l'effet de la réitération deviennent punissables* »[562]. Pour parvenir à une condamnation, la jurisprudence exige non pas un acte répété mais davantage une adjonction d'actes répétés de différente nature. Le harcèlement est donc rarement nourri de la répétition d'un seul acte de même nature, il s'agit d' « *un enchaînement indivisible d'actes à la fois diversifiés et réitérés* »[563].

176. Le harcèlement, une infraction individuelle. Par ailleurs, une infraction est réputée consommée lorsque les éléments matériels et moral décrits par le texte d'incrimination ont été accomplis par l'agent. Les infractions supposent alors une action personnelle entraînant une consommation individuelle tant matérielle que morale de l'infraction. Les délits de harcèlements sont ainsi punis parce que la réitération des propos ou des comportements émane d'un seul et même individu. C'est donc précisément le choix pour un individu de répéter à l'encontre d'une même personne des actes constitutifs de harcèlement qui justifie la sanction pénale de ce dernier. À cette conception classique du délit de harcèlement s'ajoute aujourd'hui une nouvelle forme de harcèlement résultant d'une action collective.

ii. Désormais, une infraction d'habitude commise collectivement

177. Une répétition résultant de l'action concertée de plusieurs personnes. Le principal apport de la loi n° 2018-703 du 3 août 2018 concerne l'extension de la définition des comportements définis à l'article 222-33 du Code pénal pour le harcèlement sexuel et à l'article 222-33-2-2 du Code pénal pour le harcèlement moral. Ces délits sont désormais également constitués lorsque les propos ou comportements sont imposés à une victime par plusieurs personnes, soit « *de manière concertée ou à l'instigation de l'une d'elles* », soit, en l'absence de concertation, si elles « *savent que ces propos ou comportements caractérisent une répétition* ». Ces nouvelles dispositions caractérisent une extension de la notion de répétition au sein des incriminations de harcèlement. Il n'est plus exigé que les propos ou comportements constitutifs du harcèlement sexuel ou moral soient le fait d'une personne, une

[561] V. MALABAT, « À la recherche du sens du droit pénal du harcèlement », Dr. soc. 2003. p. 491 ; Également en ce sens : C. DUVERT, « Harcèlement moral », *J.-Cl.* Pénal Code, art. 222-33-2, fasc. 20, 2003, n° 7.
[562] P. MISTRETTA, Rép. pén. Dalloz, *V°* Harcèlement, n° 57.
[563] *Ibid.*

pluralité de personnes ayant accompli un acte unique peut entraîner pour chacune d'entre elles l'engagement de sa responsabilité pénale. L'évaluation de la répétition des comportements se déplace ainsi de l'auteur du harcèlement vers la victime. L'exigence de répétition du comportement ne concerne alors plus que l'intention coupable de l'auteur du harcèlement qui doit avoir nécessairement conscience de la pluralité des actes subis par la victime. Madame Myriam Quéméner en déduit que « *les envois de messages sexuels ou sexistes à un même destinataire par plusieurs personnes utilisant les réseaux sociaux sur internet, soit lorsque ces envois résultent d'une concertation préalable, soit - ce qui est plus fréquent - lorsqu'en l'absence de concertation, chaque internaute a nécessairement eu connaissance des précédents envois avant de transmettre lui-même son message, pourront constituer le délit de harcèlement sexuel aggravé* »[564].

b- Les limites au regard du principe de personnalité de la responsabilité pénale

178. Une infraction critiquable au regard du principe de responsabilité pénale du fait personnel. Le délit de cyberharcèlement en groupe constitue une infraction collective rendant impossible une responsabilité pénale du fait personnel de chaque individu au sein du groupe (i). En réalité cette nouvelle prévision de la loi pénale organise une responsabilité pour la participation à un fait collectif qui n'est pas exempte de critiques (ii).

i. Une impossible responsabilité pénale du fait personnel

179. Une infraction collective. Le cyberharcèlement en groupe sanctionne l'adjonction d'actes individuels formant à l'échelle du groupe une infraction unique. L'auteur de cette infraction n'est pas poursuivi pour sa seule action mais parce que cette dernière constitue un élément de l'action globale consistant à mener un « *raid numérique* » à l'encontre d'une personne au moyen, le plus souvent, d'un site de réseau social. Les dispositions prévues aux articles traduisent la création d'une infraction collective qui manifeste en quelque sorte « *le passage de la criminalité du stade artisanal au stade industriel* »[565]. L'infraction collective renvoie à l'incrimination en un délit autonome d'un agissement commis, projeté ou tenté par plusieurs personnes délinquantes. Elle constitue alors une catégorie originale d'incrimination qui prend en considération le groupe délictuel plutôt qu'une juxtaposition d'infractions

[564] M. QUEMENER, « Cyberharcèlement : quelles évolutions législatives ? », *RLDI*, 2018, nº 153.
[565] C. DUPEYRON, « L'infraction collective », *RSC* 1973, p. 357.

individuelles et indépendantes[566]. Le Code pénal dénombre en l'occurrence plusieurs infractions de ce type. Ainsi, le délit d'association de malfaiteurs est une infraction collective qui sanctionne « *tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement* »[567]. De même la loi n° 2010-201 du 2 mars 2010[568] est venue incriminer le fait pour une personne « *de participer sciemment à un groupement, même formé de façon temporaire, en vue de la préparation, caractérisée par un ou plusieurs faits matériels, de violences volontaires contre les personnes ou de destructions ou dégradations de biens* »[569]. Enfin, on relève également les infractions de participation délictueuse à un attroupement prévues aux articles 431-3 et suivants du Code pénal qui constituent également des infractions collectives[570].

180. L'impossible sanction autonome de chaque individu au sein du groupe. Pour ce type particulier d'infraction, les individus au sein du groupe ne peuvent pas être qualifiés de coauteurs. En effet, à l'instar de l'auteur matériel, le coauteur est celui qui a personnellement accompli l'ensemble des éléments constitutifs de l'acte prohibé. Le coauteur est donc un auteur à part entière qui peut être poursuivi indépendamment de l'action des autres coauteurs[571]. Le cyberharcèlement en groupe n'engendre donc pas une responsabilité pénale du fait personnel mais davantage une responsabilité pénale en raison de la participation à un fait collectif qui s'avère critiquable.

ii. Une responsabilité pour participation à un fait collectif critiquable

181. Un type de responsabilité s'opposant au principe constitutionnel de responsabilité pénale du fait personnel. Le cyberharcèlement en groupe introduit une hypothèse de responsabilité pénale pour participation à un fait collectif où tous les membres du groupe supportent la responsabilité des agissements de ce dernier. Dans cette hypothèse, c'est le groupe qui est poursuivi, et c'est à lui que la peine est infligée. Les membres ne seront donc pas poursuivis au titre du groupe mais davantage au sein de ce dernier dans la mesure où ils

[566] *Ibid.*
[567] C. pén., art. 450-1.
[568] L. n° 2010-201 du 2 mars 2010 renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public, *JORF*, 3 Mars 2010, art. 1.
[569] C. pén., art. 222-14-2.
[570] J.-P. FREDERIC, « La judiciarisation du maintien de l'ordre : des maux…aux actes ! », *AJ Pénal* 2013, p. 208.
[571] B. PEREIRA, Rép. pén. Dalloz, Juin 2017 (mis à jour novembre 2018), *V°* Responsabilité pénale, n° 46.

participent à son existence et à son activité[572]. Ce postulat entre toutefois en contradiction avec le principe selon lequel : « *nul n'est responsable qu'en raison de son fait personnel* »[573]. Ce principe consacré à l'article 121-1 du Code pénal et disposant d'une valeur constitutionnelle[574] exige de constater avec certitude que « *la responsabilité pénale repose sur des éléments matériels et intellectuels accomplis personnellement par la personne poursuivie* »[575]. Le Code pénal admet toutefois une responsabilité pénale du fait de la participation à une infraction au titre de la complicité selon ses articles 121-6 et 121-7. Ainsi, celui qui a aidé, assisté ou provoqué à la commission de l'infraction peut engager sa responsabilité pénale alors qu'il n'a pas commis lui-même l'acte incriminé. Cependant, le délit de cyberharcèlement en groupe ne se situe dans aucune de ces hypothèses du fait qu'il établit une responsabilité pénale collective permettant au juge de sanctionner une personne pour des actes commis par des tiers sans qu'il soit nécessaire de prouver qu'elle a été coauteur ou complice.

182. L'admission d'un lien trop distendu entre les personnes constituant le groupe. Par ailleurs, au regard des autres incriminations collectives prévues au Code pénal le délit de cyberharcèlement en groupe possède des particularités tant du point de vue de ses éléments matériels que de son élément intentionnel. Concernant d'abord l'élément matériel, un individu peut être poursuivi au titre d'un cyberharcèlement en groupe alors même qu'il n'aurait pas agi de manière répétée. Un acte unique peut dans ce cas entraîner la constitution du présent délit à l'inverse des autres infractions de nature collective prévues au Code pénal qui semblent exiger en plus de la participation à un groupement, la réalisation de certains actes matériels pour chacun de leurs membres. La matérialité de l'acte exigé est donc particulièrement faible en l'espèce. Ensuite, concernant l'élément moral, le cyberharcèlement en groupe peut être caractérisé même en l'absence de concertation, du moment que chaque individu sait que son propos ou comportement caractérise une répétition à l'échelle du groupe. En définitive, le cyberharcèlement de groupe est une infraction collective qui peut être constitué par un acte

[572] G. LEVASSEUR, « La responsabilité collective et le droit pénal », *lumière et vie*, 1953, n° 10, p. 130.
[573] Ce principe est consacré par une jurpsirdudence constante de la Cour de cassation depuis la moitié du XIX^{ème} siècle. V. notamment : Crim. 3 mars 1859 : *Bull. crim.* n° 69 ; Crim. 3 mars 1933 : *Bull. Crim.* n° 49 ; Crim. 16 décembre 1948, *Bull. crim.* n° 291 ; Crim. 26 février 1956, *JCP* 1956, II., 9304. Arrêts cités *in* : J.-C. SAINT-PAU, « Le principe de responsabilité pénale du fait personnel », *in Entre tradition et modernité : le droit pénal en contrepoint*, mélanges en l'honneur d'Yves Mayaud, Dalloz, 2017, p. 255.
[574] Le Conseil constitutionnel a déduit la valeur constitutionnelle de ce principe des principes de nécessité des peines et de présomption d'innocence prévus aux articles 8 et 9 de la Déclaration des droits de l'homme et du citoyen. V. Cons. const., 16 juin 1999, n° DC n° 99-4141 ; Cons const., 25 février 2010, DC n° 2010-604 ; Cons. const., 4 mai 2012, QPC n° 2012-339.
[575] J.-C. SAINT-PAU, « Le principe de responsabilité pénale du fait personnel », *in* mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, 2017, p. 258.

isolé de chacune des personnes réalisant l'infraction indépendamment de la manifestation d'adhésion de l'individu au groupe. Le lien entre les personnes se trouve distendu contribuant encore plus à vider de son sens la notion de harcèlement. Au final, la responsabilité du fait de l'activité du groupe permet de sanctionner des actes dont la matérialité mais également l'intentionnalité apparaissent comme très inconsistantes[576].

183. Conclusion de la Section 2. Au final, la modernisation de l'arsenal répressif français s'avère être une entreprise particulièrement délicate qui lorsqu'elle n'aboutit pas à des incriminations redondantes au regard des textes préexistants, fleurte trop souvent avec les limites admissibles en matière pénale. Le risque est de franchir ces limites justifiant alors l'abrogation du texte par le Conseil constitutionnel comme ce fut le cas pour le délit de consultation habituelle de site terroriste. L'évolution des incriminations en matière de harcèlement que semblent justifier les pratiques observées sur les sites de réseaux sociaux doivent toutefois être reçues avec nuance. Ainsi, la nouvelle hypothèse des cyberharcèlements en groupe apparaît comme une incrimination *sui generis* difficilement conciliable avec le principe fondamental de responsabilité pénale du fait personnel.

[576] V. sur le sujet : V. MALABAT, « Vers une collectivisation de la responsabilité pénale ? », *in La cohérence des châtiments*, Dalloz, coll. Essai de philosophie pénale et de criminologie, vol. 10, 2012, p. 27.

Conclusion du Chapitre 2

184. Les incriminations du droit pénal commun se montrent majoritairement à la hauteur des comportements issus des réseaux sociaux en ligne. L'utilisation de ces moyens de communication dans un but délictueux peut matérialiser un élément constitutif d'une infraction[577] voire, être constitutif en tant que tel d'une infraction[578]. Ceci est rendu possible par la méthode de rédaction des incriminations qui soit, propose des infractions neutres d'un point de vue technologique, soit permet d'englober les sites de réseaux sociaux dans les définitions préexistantes. En ce sens, ces derniers ne sont qu'un nouveau moyen, une nouvelle méthode de commission d'infractions, encadrés par les prévisions préexistantes du droit pénal. Certaines adaptations apportées au droit pénal, notamment en matière de terrorisme, traduisent en réalité davantage une politique répressive en la matière qu'une inadaptation du système pénal aux comportements rencontrés sur les réseaux sociaux en ligne. Ces derniers peuvent dès lors être source d'une surpénalisation des comportements, ceci s'étant observé avec le délit de consultation habituelle de sites terroristes censuré à deux reprises par le Conseil constitutionnel[579] mais aussi avec le nouvel article 222-33-3 du Code pénal venant incriminer spécifiquement les cas de *happy slapping* alors que le comportement pouvait déjà être saisi par des incriminations préexistantes. Plus récemment encore, si les nouvelles prévisions du Code pénal en matière de cyberharcèlement en groupe apparaissent justifées au regard des pratiques constatées sur les sites de réseaux sociaux, la méthode de rédaction choisie par le législateur s'avère quant à elle criticable tant elle fleurte avec les limites du principe fondamental de responsabilité pénale du fait personnel.

[577] Par exemple : la consultation habituelle d'un site terroriste est l'un des éléments constitutifs de l'infraction d'entreprise individuelle de terrorisme prévue à l'article 421-2-6 du Code pénal.
[578] Par exemple : les infractions d'atteintes aux systèmes de traitement automatisé de données prévues aux articles 323-1 et suivants du Code pénal ; la participation à un groupement terroriste prévue à l'article 421-2-1 du Code pénal ; le recrutement en vue de commettre un acte terroriste prévu à l'article 421-2-4 du Code pénal.
[579] Cons. const., 7 avril 2017, QPC n° 2017-625 ; Cons. const., 10 février 2017, QPC n° 2017-611.

Conclusion du Titre 1

185. Loin de représenter un droit rigide et statique incapable d'appréhender l'évolution constante des comportements rencontrés sur les sites de réseaux sociaux, le droit pénal s'affirme en de nombreux points comme un droit adapté à son époque. Plus encore, le droit pénal spécial de la presse a su démontrer son extraordinaire pouvoir d'attraction en s'érigeant aujourd'hui comme le principal droit régissant l'expression citoyenne à l'échelle numérique. Certes, par certains aspects la loi du 29 juillet 1881, plus que centenaire, mériterait une modernisation mais il est nécessaire de maintenir l'essence de ce régime spécial et d'éviter un basculement trop massif de ses incriminations dans le droit pénal commun. Ce dernier dispose justement d'un corpus d'infractions qui apparaît aujourd'hui adaptées aux nouvelles formes de délinquances permises par les sites de réseaux sociaux. Les textes préexistants permettent ainsi parfaitement d'appréhender autant les atteintes aux personnes que les atteintes aux biens rencontrées dans ces espaces numériques. Plus encore, en sa qualité de système de traitement automatisé de données, le réseau social ou plus précisément le compte de réseau social, constitue un bien juridiquement protégé contre les attaques informatiques prévues aux articles 323-1 et suivants du Code pénal. En conséquence, certaines réformes législatives entreprises afin d'adapter l'arsenal répressif aux sites de réseaux sociaux se révèlent inutiles à l'image du délit prévu au deuxième alinéa de l'article 222-33-3. Pis encore, certaines lois se sont révélées dangereuses au regard des principes fondamentaux du droit pénal tel que le principe de nécessité de la loi pénale ou au regard du principe de responsabilité pénale du fait personnel, c'est le cas notamment du délit de consultation habituelle de site terroriste abrogé finalement par le Conseil constitutionnel et de l'évolution des incriminations de harcèlement qui ont intégré en leur sein la nouvelle notion de cyberharcèlement en groupe.

Les sites de réseaux sociaux ont cependant fait émerger de nouvelles pratiques qui révèlent une réelle inadaptation de certaines incriminations du droit pénal commun, particulièrement concernant les incriminations classiques protegeant la vie privée des individus.

Titre 2 – L'adoption justifiée de nouvelles incriminations

186. Les réseaux sociaux, à l'origine d'une évolution de la protection pénale de la vie privée. Certaines pratiques permises par les réseaux sociaux en ligne ont mis en relief de réelles carences au sein du dispositif pénal préexistant. Ces manquements d'ordre structurel s'observent dès lors que les incriminations préexistantes ne permettent pas d'appréhender, en raison du principe d'interprétation stricte de la loi pénale, des nouvelles formes d'atteintes rencontrées à l'échelle numérique alors que ces dernières portent sur des valeurs protégées par le droit pénal. En l'occurrence, la modification des rapports sociaux et de la représentation des individus induite par les sites de réseaux sociaux a entrainé une évolution ou plutôt, une complexification de certaines valeurs fondamentales propres à nos sociétés. Plus particulièrement, l'usage massif des sites de réseaux sociaux a impulsé une évolution profonde de la protection de la vie privée. Le concept de vie privée qui apparaît comme « *une notion légale à contenu indéterminé* »[580] accompagne en réalité de manière constante l'évolution de notre société. La vie privée ne doit ainsi pas être interprétée comme un concept figé[581] mais au contraire comme un concept flucutant aussi bien dans le temps que dans

[580] G. CORNU, *Droit civil approfondi : l'apport des réformes récentes du code civil sur la théorie du droit civil*, Cours de doctorat, Les cours de droit, 1970, p. 187.

[581] Classiquement, la vie privée se définit par opposition à la vie publique (R. BADINTER, « Le droit au respect de la vie privée », *JCP* G 1968, I, n° 2136 ; R. LINDON, « La presse et la vie privée », *JCP* G 1965, II, 1887). Cependant, prendre appui sur une autre notion pour définir la vie privée ne fait que déplacer le problème. Cela revient à « *vouloir définir l'incertain par le flou* » (B. BEIGNER, Le droit de la personnalité, Coll. « Que sais-je ? », PUF, 1992, p. 53). La vie publique peut se définir comme la participation de l'individu « *à la vie de la cité sous trois aspects fondamentaux : ses travaux, ses jeux, ses institutions* » (R. BADINTER, « Le droit au respect de la vie privée », *op. cit.*, n° 14). Cette définition d'apparente simplicité révèle toutefois des lacunes concernant sa mise en œuvre, les frontières entre vie privée et vie publique étant parfois minces. Un même fait peut selon les circonstances relever de la vie privée ou de la vie publique de l'individu. L'exemple du mariage d'une personnalité proposé par le Professeur Bernard Beignier l'illustre parfaitement : « *se marier en grande pompe à la Madeleine et sortir en cortège est la manifestation, qu'à ce moment de la cérémonie, il s'agit d'un acte public. Le faire discrètement, en semaine, dans une mairie de province est la preuve qu'il s'agit d'un acte privé* » (B. BEIGNER, *La protection de la vie privée*, *in* Libertés et droits fondamentaux, Coll. CRFPA Grand oral, Dalloz, 2014, n° 340). Par conséquent, le concept de vie privée se réduit aujourd'hui à un agrégat d'éléments construits au fil du temps par la jurisprudence et dont les auteurs tentent d'en établir une liste (V. notamment D. CHAUVET, *Vie privée, étude de droit privé*, Thèse Université Paris-Sud, 2014). La vie privée fait donc référence au domicile, la vie sentimentale, la sexualité, l'état de santé, au patrimoine, etc. (J.-M. BRUGIÈRE et B. GLEIZE, *Droits de la personnalité*, ellipses, 2015, p. 142 et suiv.). Cette méthode de définition est forcément « *décourageante et décevante* » (J. EYNARD, L*es données personnelles, Quelle définition pour un régime de protection efficace ?*, Michalon, 2013, p. 57). Non seulement la liste des éléments relevant de la vie privée varie nécessairement d'un auteur à l'autre mais en plus, la définition de la vie privée n'est que descriptive.

l'espace[582] si bien qu'il s'inscrit dans « *une culture individuelle et collective évolutive* »[583]. La vie privée apparaît au final comme un concept relatif et propre à chaque société. Partant de cette observation, la protection pénale de la vie privée est amenée à évoluer au gré de la modernisation de notre société. Sur ce point, deux éléments centraux semblent accompagner de façon permanente l'évolution de la notion de vie privée, à savoir l'intimité et l'identité[584]. L'évolution de la représentation des individus et les nouvelles formes de sociabilité permises par les réseaux sociaux en ligne ont justifié l'évolution de la rédaction de certaines incriminations voire, la création de nouvelles. Plus précisément, deux incriminations concernant la protection de l'identité et de l'intimité témoignent de cette nécessaire évolution du droit pénal. Loin d'être de simples réactions répressives, ces nouvelles incriminations caractérisent pour chacune d'entre elles une évolution profonde et nécessaire de la protection pénale de la vie privée. Le droit suit donc ici un mouvement d'adaptation aux comportements issus des sites de réseaux sociaux.

Les nouvelles formes d'atteintes générées par les sites de réseaux sociaux ont alors justifié l'adoption de nouvelles incriminations entraînant une extension de la protection pénale de l'identité (**Chapitre 1**) ainsi qu'une extension de la protection pénale de l'intimité (**Chapitre 2**).

[582] A. LUCAS, J. DEVEZE et J. FRAYSSINET, *Droit de l'informatique et de l'Internet*, PUF, Thémis droit, 2001, p. 30, n° 44.
[583] *Ibid.*
[584] Le Professeur Jean-Christophe Saint-Pau identifie l'identité et l'intimité comme les deux éléments objectifs et permanents qui composent la vie privée : « *plutôt que de tenter de définir la vie privée par opposition à la vie publique, c'est-à-dire en raisonnant sur les contours de la notion, il faut prendre le concept de l'intérieur en précisant clairement quels sont les éléments objectifs et permanents qui composent la vie privée de toute personne : il s'agit de l'identité civile […] et de l'intimité de l'être et de l'avoir* ». J.-C. SAINT-PAU, *L'anonymat et le droit*, thèse Bordeaux IV, 1998, p. 594, n° 617.

Chapitre 1 – L'extension de la protection pénale de l'identité

187. L'extension de la protection de l'identité à l'espace numérique. Les sites de réseaux sociaux ont permis aux individus de développer leur identité à l'échelle numérique. Si la notion d'identité numérique préexistait aux sites de réseaux sociaux, elle s'est vue toutefois transformée avec le développement de ces nouveaux moyens de communication. En l'occurrence, au-delà d'être un support de communication, les réseaux sociaux en ligne constituent un nouvel outil de mise en avant et d'exposition de soi ayant contribué à un développement fulgurant et protéiforme de l'identité à l'échelle numérique. En conséquence, aujourd'hui, l'identité numérique devient l'égal, si ce n'est dépasse, l'identité civile. Or, les sites de réseaux sociaux ont également favorisé le développement de nouveaux modes d'atteinte à l'identité des individus, en particulier à travers la méthode de la création de faux profils numériques. Ces nouvelles formes de délinquance se sont toutefois trouvées hors d'atteinte d'une quelconque infraction. Cette incapacité du droit pénal à saisir les atteintes portées à l'identité des individus à l'échelle numérique révèle alors une inadaptation structurelle des incriminations traditionnelles ayant justifié un mouvement d'adaptation du droit pénal.

Ainsi, les comportements issus des réseaux sociaux en ligne ont manifesté des carences dans la protection préexistante de l'identité (**Section 1**) justifiant une extension de sa protection (**Section 2**).

Section 1 : Les carences de la protection préexistante de l'identité

188. L'identité, objet de protection pénale. L'identité des individus représente un élément de leur personnalité, plus précisément, un élément de leur vie privée. En effet, l'identité est la première source d'intégration de l'individu au monde extérieur et représente un premier pas dans l'exposition de sa vie privée[585]. La vie privée des individus se nourrit ainsi également des relations sociales qu'ils entretiennent et de leur place au sein de la société. Dès l'instant où une personne peut être individualisée, sa vie privée est concernée et dès l'instant où elle perd la maîtrise de l'information, sa vie privée est violée[586]. Au final, « *identifier un individu, c'est déjà porter atteinte à sa vie privée* »[587]. Le droit pénal n'a pas attendu le développement des usurpations d'identité sur les réseaux sociaux en ligne pour prendre en considération ce phénomène délinquant qui n'est en réalité pas nouveau. Plusieurs infractions renvoyaient déjà avant l'adoption de la loi n° 2011-267 du 14 mars 2011 à des comportements d'usurpation d'identité. Toutefois, si les comportements d'usurpation d'identité sont traditionnellement pris en compte par le droit pénal, le développement des formes d'atteintes à l'identité numérique (**§1**) a révélé une protection pénale incomplète de l'identité par les incriminations préexistantes (**§2**).

§1. Le développement des formes d'atteintes à l'identité numérique

189. L'évolution de la notion d'identité. L'identité peut se définir comme étant « *ce qui détermine une personne ou encore comme un ensemble de données qui détermine chaque personne et qui permet de la différencier des autres* »[588]. La notion d'identité est indubitablement liée au cadre de la société au sein du quel prospère l'individu. Plus largement, selon le sociologue Jean-Claude Kaufmann[589], l'identité est une obsession issue de

[585] La notion de vie privée ne peut dès lors être limitée à l'intimité des individus qui n'en constitue qu'une facette. Suivant cette idée, le Professeur Jacques Ravanas explique la difficulté de déterminer le contenu de la vie privée : « *le privé, c'est la solitude, c'est l'intimité ; mais c'est aussi la rencontre, c'est-à-dire un ensemble d'activités non solitaires et pas forcément intimes, si bien que l'intimité n'est que l'un des aspects de la vie privée* » (J. RAVANAS, *La protection des personnes contre la réalisation et la publication de leur image*, LGDJ, coll. « Bibliothèque de droit privé », 1978, p. 129, n° 107). Dans le même sens, Madame Delphine Chauvet affirme que « *la personne ne vit pas que dans le secret et qu'il ne faut pas sous-évaluer la protection de sa vie privée à son intimité* » D. CHAUVET, *Vie privée, étude de droit privé*, Thèse Université Paris-Sud, 2014, p. 89, n° 99.

[586] D. CHAUVET, *Vie privée, étude de droit privé*, Thèse Université Paris-Sud, 2014, p. 83-84, n° 91.

[587] D. GUTMANN, *Le sentiment d'identité*, LGDJ, coll. « Bibliothèque de droit privé », 2000, p. 317, n° 381.

[588] T. CASSUTO, « Usurpation d'identité numérique », *AJ Pénal* 2010, p. 220.

[589] J.-C. KAUMFMANN, « L'identité, une nouvelle religion ? », conférence du 22 mars 2006, en ligne sur le site de la Cité des Sciences.

la modernité et d'une mutation civilisationnelle. L'évolution de la société fait donc évoluer l'identité et plus la société est évoluée, plus les facettes de l'identité sont nombreuses. Classiquement, l'identité est envisagée comme « *la somme des éléments dont le droit tient compte pour individualiser les personnes physiques, à savoir le nom, la filiation, la nationalité, le domicile, la date de naissance et le sexe* »[590]. L'identité des individus s'est ainsi d'abord construite autour des éléments de l'état civil des individus constituant son socle primaire. Ensuite, avec le développement de la science et des techniques, d'autres éléments sont venus enrichir cette notion telle que les éléments de l'identité biométrique[591] ou génétique[592]. Désormais, l'espace numérique constitue un nouveau cadre de définition pour l'identité. Or, si les sites de réseaux sociaux ne sont pas à l'origine de la création de l'identité numérique, qui est apparue concomitamment avec internet, ils ont cependant fortement contribué à la développer au point qu'elle devienne une forme distincte et massive de définition des individus. Cette extension de l'identité au domaine numérique (A) a cependant également contribué à diversifier les formes d'atteinte à l'identité (B).

A. L'extension de l'identité au domaine numérique

190. L'identité numérique à l'heure des réseaux sociaux en ligne, un concept élargi. Dans le langage courant la notion d'identité numérique est souvent utilisée pour désigner l'ensemble des informations concernant une personne, accessibles sur l'internet et permettant d'établir son profil[593]. L'identité numérique ne doit cependant pas être opposée à l'identité

À voir sur <https://www.youtube.com/watch?v=8L7nonjxbiE> (dernière consultation le 9 octobre 2019).

[590] F. GRANET-LAMBRECHTS, « Le droit à l'identité », *in* F. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 193.

[591] La biométrie réside « *dans les éléments physiques ou physiologiques de l'individu qui conduisent à son identification* » (D. FOREST, *Droit des données personnelles*, Gualino, coll. « Droit en action », 2011). En conséquence, l'identité biométrique permet « *de reconnaître ou d'identifier un individu à partir d'une caractéristique physique stable, de la mesure et du calibrage de son corps* » (G. DUBEY, « L'identité à l'épreuve de la biométrie », *in* S. LACOUR (dir.), *La sécurité aujourd'hui dans la société de l'information*, L'Harmattan, 2007, p. 87). Les marqueurs biométriques sont nombreux, l'identification peut ainsi résulter de l'iris, de la rétine, de l'empreinte digitale, de l'empreinte vocale mais aussi le réseau veineux. Les techniques d'identification biométriques se classent en trois catégories : il peut s'agir d'une analyse biologique mais aussi d'une analyse comportementale (démarche, tracé de signature, frappe clavier) ou morphologique (empreintes digitales, iris, traits du visage) (M. MARZOUKI, « Biométrie : corps étrangers sous contrôle », GISTI, *Plein droit*, 2008/1, n° 76). Par principe, elle constitue une preuve irréfutable de l'identité d'une personne puisqu'elle manifeste des caractéristiques biologiques uniques qui ne peuvent être associées qu'à un seul individu.

[592] Les données génétiques des individus apportent des informations qui caractérisent la personne et sont susceptibles d'être transmises à sa descendance. Les informations que contiennent ces données révèlent l'unicité et la singularité de chaque individu et constituent un patrimoine particulièrement sensible relevant assurément de sa vie privée. C. GIRAULT, « Identification et identité génétiques », *AJ Pénal* 2010, p. 224.

[593] A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *JCP* G n° 35, 29 août 2011, doctr. 913, citant : G. DESGENS-PASANAU et E. FREYSSINET, *L'identité à l'ère numérique*, Dalloz, coll. Présaje, 2009.

réelle, des éléments communs se retrouvant dans ces deux formes d'identité à l'instar du nom de la personne. L'identité numérique doit davantage être perçue comme l'identité dans le domaine numérique ou encore « *l'identité à l'ère numérique* »[594]. Partant il convient d'en définir les contours et les spécificités particulièrement à l'heure de l'usage massif des sites de réseaux sociaux. Sur ce point, l'identité numérique n'est pas un concept figé mais mouvant. Certains éléments demeurent constants ou du moins, jouissent d'une certaine stabilité (adresse IP, adresse de messagerie) mais dans la majorité des cas, les informations entrant dans le champ de l'identité numérique sont évolutives ou éphémères (photos de profils, commentaires). L'identité dans le domaine numérique ressemble alors à un agrégat d'éléments variés, c'est pourquoi la définir semble être une entreprise audacieuse d'autant plus qu'elle révèle non pas une identité singulière mais une multiplicité d'identités propres à chaque individu. Il est en revanche plus simple de relever et de catégoriser les éléments qui en font partie. Il peut ainsi être distingué d'un côté les éléments classiques de l'identité dans le domaine numérique (1) d'un autre côté, les éléments nouveaux intimement liés à l'utilisation des réseaux sociaux et formant une « *identité numérique sociale* »[595] (2).

1) Les éléments classiques de l'identité dans le domaine numérique

191. Monsieur Olivier Iteanu a identifié quatre composantes classiques dans l'identité numérique : le pseudonyme, l'adresse de messagerie, le nom de domaine ou l'URL et enfin l'adresse IP[596]. Ces 4 types d'informations sont la base de l'identification dans la sphère numérique, parmi elles, nous distinguerons d'une part les informations identifiantes que sont le pseudonyme et l'adresse de messagerie (a) et d'autre part, les informations techniques qui renvoient au nom de domaine, à l'URL et à l'adresse IP (b).

a- Les informations identifiantes

192. Le pseudonyme. L'acte de nomination étant le début de toute identité[597], l'emploi d'un pseudonyme permet alors l'existence d'une identité alternative. Le pseudonyme masque par essence l'identité civile et satisfait ainsi une fonction de protection[598]. Etymologiquement,

[594] V. en ce sens : A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *JCP* G n° 35, 29 août 2011, doctr. 913 ;
[595] F. GEORGES, « L'identité numérique sous emprise culturelle. De l'expression de soi à sa standardisation », *Les Cahiers du numérique*, vol. 7, n° 1, 2011, pp. 31-48 ; V. *supra* n° 19.
[596] O. ITEANU*, L'identité numérique en question*, Eyrolles, 2008, pp. 5-22.
[597] H. CAUCHAT et A. DURAND-DELVIGNE, *De l'identité du sujet au lien social*, Paris, PUF, 1999, p. 62.
[598] P. FRANÇOIS, « Pseudonyme en ligne. Remarques sur la vérité et le mensonge sur soi », *Sens-Dessous*, 2014/2, n° 14, p. 15-22.

le mot pseudonyme vient du grec *pseudônoumos*, ce mot est fondé sur la racine *pseudês* qui signifie menteur, littéralement, le pseudonyme est un faux nom[599]. L'usage d'un pseudonyme entre en opposition avec l'identité civile de l'individu qui elle est du ressort du *nomen verum*, autrement dit, du nom vrai. Le pseudonyme peut se définir comme un « *nom de fantaisie, librement choisi par une personne physique dans l'exercice d'une activité particulière […] afin de dissimuler au public son nom véritable* »[600]. Le recours au pseudonyme n'est pas une pratique récente, elle est fréquemment utilisée dans les domaines littéraires ou artistiques afin de dissimuler au public sa véritable identité[601]. L'usage du pseudonyme s'est toutefois considérablement étendu, voire généralisé dans la sphère numérique. Au sein de cet espace, le terme pseudonyme s'est d'ailleurs raccourci au profit de *pseudo*, cette nouvelle terminologie traduit en réalité une évolution dans son usage[602]. L'identité alternative est devenue sur internet une pratique dépassant largement les cadres préexistants. Nombreux sites ou forums exigent même que l'internaute s'identifie à travers un *pseudo* pour pouvoir avoir accès à leurs services. Certains réseaux sociaux comme Twitter ou Instagram suivent cette pratique en encourageant leurs utilisateurs à utiliser un *pseudo*. En conséquence, cette identité alternative devient une pratique largement consacrée mais également banalisée au sein de l'espace numérique.

193. L'adresse de messagerie. Sur internet, l'identité de l'individu est également largement représentée par son adresse de messagerie, dénommée souvent par son terme anglais *e-mail* (*electronic mail*). Il s'agit d'un des services les plus populaires d'internet qui permet aux individus de s'échanger des messages électroniques pouvant comprendre des fichiers textuels, graphiques ou sonores[603]. L'*e-mail* est ainsi devenu un mode de communication basique tant dans le domaine des relations privées que celui des relations professionnelles. L'adresse de messagerie constitue alors un élément certain de l'individualisation des individus dans la sphère numérique et donc de leur identité.

---

[599] O. ITEANU, *L'identité numérique en question*, Eyrolles, 2008, p. 8.
[600] Association H. CAPITANT, *Vocabulaire juridique*, G. CORNU (dir.), PUF, 12ème éd., 2018, *V°* Pseudonyme. Cette définition est également reprise par la jurisprudence : Civ. 1ère, 23 février 1965 : *JCP*, 1965, II, 14255, note P. NEVEU.
[601] Ainsi, François-Marie Arouet utilisait le pseudonyme de Voltaire, Amantine Aurore Lucile Dupin utilisait le nom de plume de Georges Sand. De nombreux musiciens ont également eu recours au pseudonyme tels que David Robert Jones (David Bowie) ou encore James Newel Osterberg Jr (Iggy Pop).
[602] O. ITEANU, *L'identité numérique en question*, Eyrolles, 2008, p. 9.
[603] *Ibid.*, p. 12.

Outre les informations explicites que sont le pseudonyme et l'adresse de messagerie, l'identité dans le domaine numérique renvoie également à des informations davantage techniques mais tout autant identifiantes.

b- Les informations techniques

194. Le nom de domaine et l'URL. À l'ère numérique, l'identité se caractérise également par des informations techniques qui permettent une identification précise de l'individu. Parmi ces informations, le nom de domaine est l'une des plus identifiantes. Le nom de domaine est situé soit après le @ soit après le *www.*, il s'agit en réalité du nom d'un site Web[604]. Une URL (*Uniform Resource Locator*) renvoie à une information plus détaillée que le nom de domaine, c'est l'adresse complète qui permet de renvoyer à une page internet en particulier. Autrement dit, le nom de domaine renvoie au nom du site internet alors que l'URL renvoie à l'une des pages du site visité. Par exemple, l'URL de la page wikipédia consacrée à cette notion est la suivante : <https://fr.wikipedia.org/wiki/Uniform_Resource_Locator>, on y distingue le protocole de communication utilisé (ici : *https*), le nom de domaine (*fr.wikipedia.org*) et enfin, le chemin d'accès vers la page demandée (*wiki/Uniform_Resource_Locator*).

195. L'adresse IP. L'adresse IP (*Internet Protocol*)[605] est le numéro qui identifie tout matériel informatique (ordinateur, routeur, téléphone IP, etc.) connecté à un réseau informatique utilisant le protocole internet[606]. Chaque utilisateur du réseau internet est identifié au moment de sa connexion au moyen de l'adresse IP que lui a attribué son FAI (Fournisseur d'Accès Internet). L'adresse IP constitue alors un moyen d'identification certain et précis, et permet de lever efficacement l'anonymat de l'internaute qui cacherait son identité sur internet. C'est pourquoi, les autorités publiques recourent à ce moyen d'identification pour lever l'anonymat de certains internautes malveillants. Cette identification dépend toutefois de

[604] Par exemple : google.com, wikipedia.org, youtube.com son des noms de domaines.
[605] Dans la version 4 du protocole internet (IPv4), l'adresse IP comporte quatre nombres compris entre 0 et 255, séparés par des points comme par exemple : 211.135.15.159. Cette version a cependant rapidement montré ses limites en raison de leur nombre limité et parallèlement, du besoin grandissant d'adresses IP conduisant à la saturation des adresses IPv4 disponibles. L'adresse IPv6 comporte pour sa part 8 nombre compris entre 0 et 65 535 (notés en hexadécimal), séparés entre eux par des deux-points comme par exemple : 1FFF:0:A99:90A3:0:0:AC1F:8001. L'adresse IPv6 permet ainsi de pallier les difficultés liées à la croissance continue du nombre d'adresses IP demandé. Deux types d'adresses IP peuvent être distingués : les adresses IP fixes et les adresses IP dynamiques. Les adresses IP fixes sont assignées définitivement à un matériel informatique par un fournisseur d'accès à internet (FAI). À l'inverse, une adresse IP dynamique identifie un matériel qui se connecte pour un temps limité, appelé « session ». Dans cette hypothèse, l'adresse IP dynamique est renouvelée à chaque connexion au réseau internet. O. ITEANU, *L'identité numérique en question*, *op. cit.*, p. 15.
[606] O. ITEANU, *L'identité numérique en question*, *op. cit.*, p. 14.

la bonne coopération du FAI ou de l'hébergeur du site internet sur lequel a agi l'internaute malveillant[607].

Ces composantes classiques de l'identité dans le domaine numérique ne suffisent cependant plus à circonscrire cette notion qui s'est largement développée avec l'apparition des réseaux sociaux en ligne. L'identité n'est plus la somme de divers éléments prédéfinis mais s'apparente désormais davantage à une entité en perpétuelle évolution. Le développement de l'utilisation des sites de réseaux sociaux a ainsi fait émerger une nouvelle forme d'identité : l'identité numérique sociale.

2) L'identité numérique sociale, spécifique aux réseaux sociaux en ligne

196. Une identité numérique se superposant à l'identité réelle. Dans l'environnement numérique, le système d'identité est représenté classiquement par les pseudonymes, les adresses de messagerie, le nom de domaine et l'adresse IP. Cependant, les manifestations de l'identité dans le domaine numérique ne se réduisent plus à ces quatre éléments classiques, le monde virtuel démultipliant les modes d'identification. Ainsi, l'identité numérique présente un aspect bien plus large que l'identité réelle du fait de la multiplicité des sources de sa définition. En conséquence, « *à l'ère du numérique, l'identité est une notion qui s'est étendue et diversifiée* »[608]. Les attributs de l'identité à l'echelle numérique peuvent être constants[609] mais aussi variables[610]. Enfin ces attributs ne sont pas nécessairement liés à ceux du monde réel permettant une dissociation entre l'identité numérique et l'identité réelle[611]. Les réseaux sociaux en ligne participent à cet élargissement en démultipliant les sources et les acteurs de l'identification. Les individus révèlent alors différentes facettes de leur personnalité *via* une liste abondante d' « *identitèmes* »[612]. Au final, l'identité numérique des individus devient plus complexe que leur identité réelle circonscrite pour l'essentiel aux éléments de leur état civil.

197. Sur les sites de réseaux sociaux, une identité fonction d'acteurs multiples. Madame Fanny Georges observe un déploiement sous différentes formes de l'identité des individus sur les sites de réseaux sociaux. Elle distingue d'une part une « *identité déclarative* » résultant de la mise en scène de l'individu sur le réseau social et d'autre part,

[607] La coopération des opérateurs des réseaux sociaux se révèle en l'occurrence délicate : v. *infra* n° 378.
[608] T. CASSUTO, « Usurpation d'identité numérique », *AJ Pénal* 2010, p. 220.
[609] Par exemple : le nom, le prénom, la profession ou encore le sexe.
[610] Par exemple : les mots de passe, les adresses de messagerie, les adresses IP etc.
[611] M. LAURENT et S. BOUZEFRANCE (dir.), *La gestion des identités numériques*, éd. Iste, 2015, p. 21.
[612] Néologisme désignant les différentes facettes de l'identité d'un individu *in* F. GRANJON et J. DENOUEL, « Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie*, 2010/1, vol. 1, p. 28.

une « *identité agissante* » fruit de l'activité de l'internaute sur le réseau social et de ses interactions avec les autres utilisateurs[613]. En conséquence, sur les sites de réseaux sociaux, l'identité des individus peut d'un côté être produite par l'internaute lui-même à travers la mise en ligne d'informations au sein de son profil (nom, âge, sexe, profession, domiciliation, auto description, etc.) et d'éléments davantage expressifs sur son « *mur* » (statuts, textes, commentaires, partages, photos, vidéos, liens, etc.) ; d'un autre côté, l'identité peut être construite indépendamment de soi, au travers de contenus publiés par d'autres utilisateurs[614]. S'observe alors une nouvelle forme d'identité propre aux sites de réseaux sociaux. Cette identité numérique sociale est plus explicite que les éléments classiques de l'identité dans le domaine numérique, mais surtout, l'identité devient fonction sur les sites de réseaux sociaux d'acteurs multiples : l'utilisateur lui-même mais également d'autres utilisateurs peuvant agir sur cette dernière[615].

B. La diversification des formes d'atteintes à l'identité

198. La création de faux profils sur les sites de réseaux sociaux. L'usurpation d'identité correspond au fait de porter un autre nom que le sien ou porter le nom d'un tiers. Autrement dit, l'usurpation d'identité se retrouve dans le « *comportement de quelqu'un qui s'attribue une identité à laquelle il ne peut prétendre* »[616]. L'usurpation d'identité devient pénalement répréhensible lorsque ce comportement devient préjudiciable soit à l'égard de la personne dont l'identité a été usurpée, soit pour les tiers trompés par l'emploi de la fausse identité. En France, plus de 300 000 individus seraient confrontés à cette forme particulière de délinquance[617]. Le nombre d'usurpation d'identité serait même en constante augmentation, plaçant ce phénomène devant les cambriolages et les vols d'automobiles[618]. Classiquement, les usurpations d'identité portent sur les éléments de l'identité civile des individus. L'hypothèse la plus courante concerne la situation d'une personne interpellée en possession de faux papiers d'identité ou de papiers falsifiés et qui se présenterait sous l'identité

[613] F. GEORGES, « Représentation de soi et identité numérique. Analyse sémiotique et quantitative de l'emprise culturelle du Web 2.0 », *Réseaux*, 2009, vol. 27, n° 154, p. 165-193.
[614] M. LAURENT et S. BOUZEFRANCE (dir.), *La gestion des identités numériques*, éd. Iste, 2015, p. 49.
[615] V. *supra* n° 19.
[616] C. LACROIX, Rép. pén. Dalloz, Juin 2012, *V°* Usurpation d'identité, n° 1.
[617] Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes. Rapport sur la cybercriminalité*, février 2014, p. 153.
[618] Rapport *Les Français face à l'usage frauduleux de leurs documents papiers - Connaissances, attitudes et comportements*, Étude réalisée par le département Consommation du Credoc, juin 2009.

mentionnée sur ces papiers[619]. Le développement d'internet a toutefois entrainé une diversification des formes d'usurpation d'identité, plus encore, ce nouveau support de communication a accru de manière considérable le risque d'usurpation d'identité[620]. Ainsi, par exemple, la pratique du *phishing* ou « *hameçonnage* »[621] consiste à s'accaparer à l'insu de la personne des éléments formant son identité dans le domaine numérique tels que l'identifiant ou le mot de passe de sa messagerie dans le but de lui soutirer de l'argent ou de prendre possession de ses données personnelles. Par ailleurs, l'usurpation d'identité à l'échelle numérique se retrouve également dans d'autres nouvelles formes d'atteintes comme les vols de compte de jeu vidéo[622]. Mais surtout, les sites de réseaux sociaux ont favorisé le développement d'une nouvelle pratique consistant à créer un faux profil permettant de générer à l'insu d'un tiers une identité à son nom, le plus souvent dans le but de lui porter préjudice. Ce cas particulier d'atteinte à l'identité numérique s'est notamment rencontré dans une affaire concernant la mise en ligne d'un faux profil Facebook au nom de l'acteur-humoriste Omar Sy[623]. Le profil comportait une photographie de l'acteur ainsi qu'une rubrique « *photos* » contenant cinq autres clichés de ce dernier et des commentaires inventés par l'usurpateur. Le faux profil a semé le doute dans l'esprit du public si bien que les véritables connaissances de l'acteur pensaient s'adresser à la véritable personne. D'autres exemples similaires peuvent être mentionnés notamment celui d'un individu qui créa en 2007 sur le réseau social Facebook un profil au nom d'Alain Juppé qui resta actif pendant près de trois semaines[624]. Plus généralement, si cette pratique concerne l'ensemble des sites de réseaux sociaux elle se recentre néanmoins le plus souvent sur les sites les plus utilisés à l'image de Facebook ou encore Twitter[625].

199. Une nouvelle forme d'atteinte à la vie privée. Ce nouveau moyen de porter atteinte à l'identité des individus révèle en réalité une forme nouvelle d'atteinte à la personnalité et plus particulièrement à la vie privée. Les créations de faux profils ont été sanctionnées dans un premier temps sur le fondement de l'article 9 du Code civil en tant qu'atteinte à la vie privée et au droit à l'image. Par exemple, dans l'affaire du faux profil d'Omar Sy, le demandeur a

[619] S. REVEL, « Précision sur la notion d'usurpation d'identité ou l'inexistence de l'ubiquité », *AJ Pénal* 2010, p. 218.
[620] Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes. Rapport sur la cybercriminalité*. février 2014, p. 153.
[621] V. s*upra* n° 136.
[622] V. sur la question : G. BRUNAUX, « Le vol de compte de jeu vidéo », *CCE* n° 10, octobre 2011, étude 17.
[623] V. : TGI Paris, 17ème ch. civ., 24 nov. 2010, n° 09/16298 : *CCE* n° 3, mars 2011, comm. 28, A. LEPAGE.
[624] <https://www.01net.com/actualites/un-faux-alain-juppe-sur-facebook-365566.html> (dernière consultation le 9 octobre 2019).
[625] V. par exemple : TGI Paris, réf., 4 avril 2013 : *CCE* n° 7-8, juillet 2013, comm. 83, A. LEPAGE.

fait valoir que cette mise en ligne constituait un « *avatar fictif qui parasite sa vie privée* »[626] et que les pages internet litigieuses violaient également son droit à l'image. Si l'expression d' « *avatar fictif* » ne renvoyait pas à une notion juridique précise le juge a toutefois accueilli ses propos en précisant que « *les noms et prénoms du demandeur ainsi que sa date de naissance sont des éléments d'identité ne relevant pas de la vie privée, en revanche, aucun élément ne justifiait que les informations concernant ses goûts ainsi que le nom de certains de ses amis soient portés à la connaissance du public. De la même façon, le défendeur ne pouvait, sans le consentement du demandeur, publier des photographies de celui-ci pour illustrer un site portant atteinte à sa vie privée* »[627]. Dans cette affaire, la violation de l'article 9 du Code civil concerne en réalité la diffusion sans l'autorisation de la victime d'informations personnelles et de photographies la concernant. Le juge civil n'est pas venu sanctionner le comportement même d'usurpation d'identité mais ses conséquences dommageables pour la victime. Ainsi, si l'article 9 du Code civil permet d'appréhender comme une atteinte à la vie privée la création d'un faux profil sur un site de réseau social, la décision rendue par les juges du fond ne permet pas de conclure pour autant à une prise en compte spécifique du problème lié à l'atteinte de l'identité numérique de la personne. Le Professeur Agathe Lepage observe alors un *hiatus* entre d'un côté une décision de justice « *d'un parfait classicisme* » et de l'autre une nouvelle forme d'atteinte à la vie privée[628].

Les comportements consistant à créer de faux profils sur les sites de réseaux sociaux ont cependant révélé l'incapacité des incriminations antérieures à appréhender cette nouvelle forme d'usurpation d'identité à l'échelle numérique.

§2. Une protection pénale incomplète de l'identité par les incriminations préexistantes

200. Avant l'adoption du délit spécifique d'usurpation d'identité numérique par la loi n° 2011-267 du 14 mars 2011, le droit pénal disposait déjà d'incriminations permettant, dans certaines circonstances, de sanctionner des comportements d'usurpation d'identité. Plus précisément, le Code pénal disposait de deux incriminations venant sanctionner des comportements d'usurpation d'identité. Ainsi, l'article 433-19 du Code pénal sanctionne diverses fraudes concernant l'état civil des personnes, notamment celles résultant de la prise d'un nom autre que celui assigné par l'état civil dans un document destiné à l'autorité

[626] TGI Paris, 17ème ch. civ., 24 nov. 2010, n° 09/16298 : : *CCE* n° 3, mars 2011, comm. 28, A. LEPAGE.
[627] TGI Paris, 17ème ch. civ., 24 nov. 2010, n° 09/16298 : : *CCE* n° 3, mars 2011, comm. 28, A. LEPAGE.
[628] A. LEPAGE, « Faux profil sur Facebook », *CCE* n° 3, mars 2011, comm. 28.

publique ; l'article 434-23 du Code pénal réprime pour sa part 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. Par ailleurs, l'utilisation d'une fausse identité dans le domaine numérique pouvait également entrer dans le champ répressif de certaines autres incriminations en tant qu'élément constitutif, à l'instar du délit d'escroquerie ou en tant que moyen de porter atteinte à une autre valeur sociale protégée, à l'image des délits d'atteinte aux STAD ou du délit de diffamation. Ceci étant, une interprétation stricte de ces incriminations révèle leur inadaptation à appréhender de manière autonome les formes particulières d'atteintes à l'identité permises par les sites de réseaux sociaux. En effet, dans certains cas, la protection préexistante de l'identité par le droit pénal s'est révélée trop spécifique pour appréhender l'identité dans sa dimension numérique (A). Dans d'autres cas, les incriminations se sont révélées insuffisantes pour permettre une appréhension des différentes formes d'usurpation d'identité observées sur les sites de réseaux sociaux (B).

A. Une protection trop spécifique de l'identité

201. Antérieurement à la création du délit d'usurpation d'identité numérique par la loi LOPPSI II, plusieurs infractions renvoyaient déjà à des comportements d'usurpation d'identité. L'article 434-23 du Code pénal prévoit ainsi l'usurpation de nom[629], de même l'article 433-19 du Code pénal sanctionne l'usage d'un faux nom dans un acte public[630]. Ces infractions ont toutefois révélé des carences sur deux points : soit le champ d'application de l'incrimination ne concerne que les éléments de l'identité civile (1), soit l'identité usurpée doit être utilisée à des fins précises (2).

1) Le renvoi de l'incrimination aux éléments de l'identité civile

202. L'incrimination d'usage d'un faux nom. L'usurpation ou l'altération de noms est définie par l'article 433-19 du Code pénal comme « *le fait, dans un acte public ou authentique ou dans un document administratif destiné à l'autorité publique et hors les cas où la réglementation en vigueur autorise à souscrire ces actes ou documents sous un état civil*

[629] Le premier alinéa de l'article dispose : « *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* ».

[630] Selon l'article 433-19 du Code pénal : « *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 et hors les cas où la réglementation en vigueur autorise à souscrire ces actes ou documents sous un état civil d'emprunt :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* ».

d'emprunt : 1º De prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil ; 2º De changer, altérer ou modifier le nom ou l'accessoire du nom assigné par l'état civil ». En l'occurrence, le seul usage de l'identité d'un tiers est de nature à engager une sanction pénale. Cependant, si l'identité est protégée de manière indépendante, l'incrimination renvoie toutefois au nom en tant qu'élément de l'identité civile, autrement dit, au nom en tant qu'émanation de la chose publique[631]. De plus, le texte n'a vocation à s'appliquer que lorsque l'identité d'un tiers est utilisée dans un acte public, authentique ou tout document administratif. Par exemple, l'infraction est constituée par l'emploi du nom d'un tiers au cours de l'interrogatoire de garde à vue[632] ou par l'utilisation d'un pseudonyme dans une plainte avec constitution de partie civile[633].

203. L'exclusion de l'identité numérique du champ répressif. En conséquence, le texte ne protège pas l'identité en tant qu'élément de la personnalité mais davantage en tant que document administratif émanant de l'autorité publique. L'univers numérique des sites de réseaux sociaux se trouve alors à l'écart de la répression envisagée par ce texte. En effet, d'une part, les comptes de messagerie ou les profils ne correspondent pas toujours à l'identité civile de leurs titulaires, d'autre part, aucun acte public ou document administratif ne sont susceptibles d'émaner d'un site de réseau social. Le juge pénal ne peut donc au vu de son devoir d'interprétation stricte de la loi pénale étendre les prévisions de l'article 433-19 du Code pénal aux éléments de l'identité numérique de l'individu.

2) L'utilisation de l'identité usurpée à des fins précises

204. L'incrimination d'usurpation d'état civil transposable à l'environnement numérique. L'article 434-23 du Code pénal sanctionne 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. Cette incrimination vise « *le nom d'un tiers* » correspondant à l'identité d'une personne réellement existante[634]. De prime abord, « *le nom d'un tiers* » doit s'entendre comme l'un des attributs de la personne au sens du Code civil[635]. La jurisprudence a toutefois adopté une interprétation large de cet élément constitutif en précisant qu'il n'était pas nécessaire que l'usurpation de l'état civil soit complète, une usurpation d'identité même

[631] L. SAENKO, « Le nouveau délit d'usurpation d'identité numérique », *RLDI*, 2011, n° 72.
[632] Agen, 20 août 2008, n° 2008-002884.
[633] Crim., 11 janv. 1990, n° 89-80.642 : *Gaz. Pal.* 1991,1, p. 298, note J.-P. DOUCET.
[634] Crim., 15 avril 1972 : *Bull. crim.* 1972, n° 123 – Crim., 7 mai 1972 : *Bull. crim.* 1972, n° 162 – Crim., 13 Mai 1991, n° 90-86.419 : *Bull. crim.* 1991, n° 201.
[635] É. CAPRIOLI, « De l'usurpation d'identité en matière pénale », sous Crim. 29 mars 2006, nº 05-85.857 : *Bull. crim.* nº 94 ; *CCE* nº 7, juill. 2006, comm. 117.

partielle suffit à constituer l'infraction[636]. Plus encore, la Cour de cassation a reconnu que l'usurpation d'identité pouvait être observée à l'échelle numérique. Les juges ont en effet admis que l'utilisation d'une adresse électronique faisant apparaître le nom d'un tiers était de nature à constituer l'infraction prévue à l'article 434-23 du Code pénal[637]. Ainsi, la présente incrimination protège aussi bien les éléments de l'identité civile que de l'identité numérique de l'individu. Au final, seule compte la mention du nom d'un tiers peu importe le support utilisé.

205. Une protection justifiée par le risque de poursuites pénales. L'article 434-23 du Code pénal démontre cependant lui aussi son manque d'adaptation à la délinquance numérique mais cette fois ci par les finalités de l'utilisation du nom. Cette infraction ne protège pas le nom lui-même mais davantage son mauvais usage. Le législateur entend ici sanctionner l'utilisation du nom d'un tiers dans des circonstances qui ont ou qui auraient pu déterminer des poursuites pénales à son encontre. Dès lors, ce n'est pas le nom en tant que tel qui est protégé mais les droits des tiers susceptibles d'être affectés par son mauvais usage[638]. La limite de ce texte est rapidement trouvée : si une personne utilise le nom d'un tiers pour diffamer au nom de celle-ci, l'infraction est constituée, à l'inverse, si une personne utilise le nom d'un tiers pour le diffamer lui-même, l'infraction n'est plus constituée. Tel est le cas dans une affaire où un individu, se faisant passer pour un autre, avait envoyé un e-mail à plusieurs personnes dans lequel il tenait des propos diffamatoires à l'encontre de la personne dont il avait usurpé l'identité. La Cour de cassation a invalidé sa condamnation en précisant que le message électronique ne comportant aucune imputation portant atteinte à l'honneur ou à la considération de personnes nommément désignées, le délit de diffamation n'était pas constitué et par extension, le délit de l'article 434-23 également[639]. L'usurpateur doit ainsi nécessairement diffamer une autre personne que l'usurpé lui-même pour que ce texte d'infraction puisse s'appliquer. Au final, si l'article 434-23 du Code pénal permet d'appréhender un comportement d'usurpation d'identité à l'échelle numérique, ce n'est pas ce comportement en tant que tel qui justifie la sanction mais davantage le risque que fait encourir ce dernier à l'égard de la personne dont l'identité a été usurpée. Partant, ce n'est pas l'identité qui est l'objet de protection mais en réalité l'entrave à l'action en justice qu'elle implique.

[636] Crim. 13 janv. 1955 : *Bull. crim.* n° 33 – Crim. 13 janv. 1987, n° 86-93.252 : *Bull. crim.* n° 19 ; *RSC* 1987, p. 420, obs. DELMAS SAINT-HILAIRE.
[637] Crim. 20 janv. 2009, n° 08-83.255 : inédit ; *CCE* n° 6, juin 2009, comm. 59, obs. A. LEPAGE.
[638] L. SAENKO, « Le nouveau délit d'usurpation d'identité numérique », *op. cit.*
[639] Crim., 26 mars 2006 : *Bull. crim.*, n° 94, *RLDI*, 2006, n° 17 ; *CCE* 2006, n° 7, p. 39, obs E. CAPRIOLI ; *Dr. pén.* 2006, n° 6, comm. M. VERON.

Cette *ratio legis* se vérifie notamment par l'emplacement de l'incrimination au sein du Livre IV du Code pénal prévoyant les atteintes portées à la Nation, l'État et la paix publique[640].

B. L'appréhension insuffisante des différentes formes d'usurpation d'identité par les autres incriminations

206. L'usurpation d'identité numérique, un élément du délit d'escroquerie. Face aux comportements très variés d'usurpation d'identité, les qualifications pénales préexistantes permettent le plus souvent de venir appréhender ces actes malveillants y compris lorsqu'elles relèvent des nouveaux aspects de l'identité numérique permise par les sites de réseaux sociaux. Ce comportement se retrouve cependant dans une définition plus large et n'est dès lors pas sanctionné de manière autonome. Ainsi, l'usage d'un faux nom constitue l'un des moyens frauduleux visés par l'article 313-1 du code pénal pour commettre une escroquerie. Par conséquent, la création d'un faux profil sur un site de réseau social peut, sous certaines conditions, entrer sous la qualification pénale du délit d'escroquerie. Un tel comportement ne pourra toutefois être sanctionné que s'il est réalisé dans le but de tromper autrui pour le déterminer à remettre certains fonds, valeurs ou un bien quelconque[641]. L'usurpation d'identité ne sera alors pas sanctionnée de manière autonome mais uniquement parce qu'elle constitue le moyen d'atteindre une valeur sociale protégée différente à savoir le patrimoine de l'individu victime de l'infraction. En réalité, il convient mieux dans cette hypothèse particulière de parler d'une identité inventée que d'une identité usurpée[642]. À la différence d'une identité usurpée, l'identité inventée revient à créer de toutes pièces une personne inexistante et d'ouvrir en son nom des comptes en ligne. Monsieur Fabrice Mattatia observe alors que : « *si l'invention d'identité peut servir de base à des trafics ou à des escroqueries au détriment de tiers, elle diffère de l'usurpation proprement dite par l'absence d'une victime d'un vol d'identité. Autrement dit, les éventuelles infractions commises sous le couvert de la fausse identité ne seront pas imputées à tort à une personne innocente* »[643].

207. La protection incomplète de l'identité numérique sociale par les délits d'atteinte aux STAD. Enfin, certaines incriminations ne permettent pas d'envisager toutes les formes d'usurpations, en particulier celles résultant de la création d'un faux profil. Par exemple, les

[640] A. LEPAGE, « D'une pierre deux coups : atteinte à l'intimité de la vie privée commise à l'occasion de l'usurpation de l'identité d'un tiers », *CCE* n° 6, juin 2009, comm. 59.
[641] C'est le cas par exemple de l'escroquerie « *à la nigériane* ». V. *supra* n° 112.
[642] F. MATTATIA, « L'usurpation d'identité sur internet dans tous ses états », *RSC*, vol. 2, nº 2, 2014, p. 331.
[643] *Ibid.*

délits d'atteinte aux STAD permettent de sanctionner dans une certaine mesure des usurpations d'identité sur les réseaux sociaux. Ces délits présentent l'avantage de faire du compte d'un réseau social un élément objet de protection pénale. Ainsi, indirectement, les délits des articles 323-1 et suivants du Code pénal protègent l'identité numérique de l'individu. Le compte d'un réseau social est en effet protégé de manière autonome à l'encontre de toute intrusion, accès, maintien ou usage frauduleux des données du compte de l'utilisateur. Cependant, ces délits démontrent leurs limites dès lors que l'acte d'atteinte à l'identité numérique ne consiste pas à s'introduire frauduleusement sur un compte existant, mais au contraire, à créer un faux compte à partir d'une identité existante. Ceci s'explique du fait que pour ces infractions le bien juridique protégé n'est pas l'identité de l'individu mais le système de traitement automatisé de données représenté en l'occurrence par un compte de réseau social déjà existant.

208. L'usurpation d'identité sanctionnée sous le fondement de la diffamation. Les comportements d'usurpation d'identité numérique peuvent en outre dans certaines hypothèses être sanctionnés sous le fondement du délit de diffamation prévu à l'article 29 de la loi sur la liberté de la presse. Par exemple, un homme a été condamné sur ce fondement[644] suite à la création d'une fausse fiche au nom de son ancien supérieur hiérarchique sur le réseau social à vocation professionnelle Viadeo. L'auteur de la fausse page avait notamment tenu des propos insinuant que son ancien supérieur hiérarchique avait obtenu son poste en octroyant des faveurs sexuelles et en harcelant ses collègues. Dans cette situation l'infraction de diffamation avait pu être retenue puisque l'auteur de la fausse page avait utilisé cette dernière pour imputer des faits précis portant atteinte à l'honneur et à la considération de la personne visée. Les usurpations d'identité peuvent être poursuivies sur le fondement de la diffamation dès lors que l'usurpateur a utilisé le faux profil pour assener des propos pouvant porter atteinte à l'honneur ou à la considération d'autrui. Autrement dit, soit l'internaute mal intentionné utilise le faux profil d'une personne pour la discréditer elle-même, soit pour parler en son nom pour nuire à d'autres personnes. Dans les deux cas le délit de diffamation est constitué. Cependant, aucune distinction n'est faite entre une diffamation faite en son nom[645] et une diffamation faite au travers de l'identité d'une autre personne. D'un point de vue répressif les deux situations sont traitées à égal alors que d'un point de vue criminologique ces deux situations reflètent des hypothèses bien distinctes. Enfin, les poursuites sous le fondement de

[644] TGI Bobigny, 14ème ch. corr., 15 novembre 2012, Éric R., MMA Vie c/ M.L.

[645] Par exemple en utilisant son propre compte de réseau social pour proférer des propos portant atteinte à l'honneur ou à la considération d'autrui

la loi sur la liberté de la presse impliquent l'application d'un délai de prescription extrêmement court de 3 mois. Dans la présente affaire, le juge avait considéré que le délai de prescription n'était pas écoulé puisque l'auteur du faux profil avait modifié le 17 mai 2010 des informations du profil Viadeo et que dès lors, ceci constituait une nouvelle publication qui fait repartir le délai de prescription qui n'était alors pas écoulé lors de la plainte le 16 juin 2010. Certaines situations similaires n'ont cependant pas entraîné de condamnation[646].

209. De manière générale, l'ensemble des éléments constitutifs du délit de diffamation doivent être rapportés pour que le comportement soit sanctionné. Or, aux termes de l'article 29, alinéa 1[er] de la loi du 29 juillet 1881, seule l'allégation ou l'imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne à laquelle le fait est imputé présente un caractère diffamatoire[647]. La personne diffamée doit ainsi être nommément désignée dans le propos incriminé pour que ce dernier devienne punissable. La jurisprudence reconnaît toutefois qu'il n'est pas nécessaire que la personne soit désignée, dès lors que son identification est rendue possible « *par les termes du discours ou de l'écrit ou par des circonstances extrinsèques qui éclairent et confirment cette désignation de manière à la rendre évidente* »[648]. Cette situation particulière où l'identité d'une personne réelle est constituée de toute pièce dans le but de lui nuire ne se satisfait pas entièrement des éléments constitutifs du délit de diffamation[649]. En sus, cette infraction ne sanctionne pas le comportement même d'usurpation d'identité mais l'utilisation préjudiciable pour la réputation de la victime qui en est faite. Par ailleurs, la diffamation est soumise au délai de prescription abrégé des infractions de presse[650], ce délai se justifiant par la volonté d'instaurer un régime favorable aux abus de la liberté d'expression. L'application en l'espèce du régime de faveur de la loi sur la liberté de la presse ne se justifie donc pas entièrement au regard de la réalité infractionnelle de ce comportement qui concerne davantage une atteinte à la personne qu'un simple abus de liberté d'expression. Une incrimination autonome du comportement d'usurpation d'identité se révèle alors être un complément nécessaire à la répression des pratiques rencontrées sur les sites de réseaux sociaux.

---

[646] Par exemple : Crim., 26 mars 2006 : *Bull. crim.*, n° 94, *RLDI*, 2006, n° 17 ; *CCE* 2006, n° 7, p. 39, obs E. CAPRIOLI ; *Dr. pén.* 2006, n° 6, comm. M. VERON.

[647] Crim., 30 septembre 2003 : *Bull. crim.* 2003, n° 172.

[648] Crim., 15 octobre 1985 : *Bull. crim.* 1985, n° 315 – Civ 2[ème]., 3 février 2000 : *Bull. civ.* 2000, II , n° 23.

[649] Prenons l'exemple suivant : publier sur internet un éloge du vin de Bourgogne sous le nom d'un élu de Bordeaux ne constitue pas nécessairement une atteinte à l'honneur de l'élu mais constitue sans doute une atteinte à son électorat. F. MATTATIA, « La création d'un délit d'usurpation d'identité sur l'Internet », *Gaz. Pal.*, 26 juillet 2008, n° 208, p. 6.

[650] Selon l'article 65 de la loi sur la liberté de la presse : « *L'action publique et l'action civile résultant des crimes, délits et contraventions prévus par la présente loi se prescriront après trois mois révolus, à compter du jour où ils auront été commis ou du jour du dernier acte d'instruction ou de poursuite s'il en a été fait* ».

210. Conclusion de la Section 1. Les réseaux sociaux en ligne ont permis une extension et une démultiplication de la notion d'identité des individus à l'échelle numérique. Désormais, les individus se définissent aussi bien à travers les éléments de leur identité civile qu'à travers les éléments de leur identité numérique. Plus encore, les sites de réseaux sociaux ont fait émerger une identité numérique sociale chez les individus dont la précision dépasse de loin les éléments de l'identité civile. Or, une interprétation stricte des incriminations traditionnelles démontre les carences de la protection pénale concernant cette manifestation particulière de l'identité des individus. D'une part, les incriminations protégeant spécialement l'identité sont inadaptées à l'environnement numérique soit parce qu'elles ne protègent que l'identité civile des individus, soit parce que l'infraction ne protège pas l'identité en elle-même mais son mauvais usage. D'autre part, les autres incriminations se révèlent également incapables de protéger de manière autonome toutes les formes d'atteinte à l'identité des individus permises par les sites de réseaux sociaux. En réalité ces différentes carences observées s'expliquent par l'absence d'une protection pénale autonome de l'identité quel que soit le support sur lequel elle repose. Pour ce faire, la protection de l'identité en matière pénale mérite une protection autonome au titre d'une atteinte à la personnalité et plus particulièrement d'une atteinte à la vie privée. En réaction aux carences observées, le législateur est ainsi venu créer légitimement un délit spécifique d'usurpation d'identité à l'article 226-4-1 du Code pénal.

Section 2 : Une extension justifiée de la protection de l'identité

211. Une loi inspirée d'exemples étrangers. La création d'un délit d'usurpation d'identité numérique devenant une nécessité, plusieurs propositions de loi ont émergé avant que le délit ne soit définitivement adopté par la loi n° 2011-267 du 14 mars 2011[651]. Pour ce faire, le législateur français s'est notamment inspiré de ses homologues anglais et américain qui avaient déjà légiféré en la matière. Une qualification pénale spécifique pour le vol d'identité en ligne est en effet prévue aux États-Unis depuis le 15 juillet 2004 tant au niveau de la législation fédérale que de la législation des différents États[652]. Au niveau européen, le Royaume-Uni a fait figure de pionnier en la matière par l'adoption d'un délit spécifique

[651] L. n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite LOPPSI, *JORF* n° 0062, 15 mars 2011, p. 4582, art. 2.
[652] V. en l'occurrence : *Identity Theft Penalty Enhancement Act* , Public Law No: 108-275 (07/15/2004). V. M. PRUD'HOMME, « L'usurpation d'identité bientôt un nouveau délit », *Gaz. Pal.*, 24 avril 2010, n° 114, p. 8.

d'usurpation d'identité en ligne aux termes du « *Fraud Act* » entré en vigueur le 15 janvier 2007[653] et prévoyant une lourde répression pouvant aller jusqu'à dix ans d'emprisonnement. Ces évolutions ont alors préfiguré l'adoption d'un délit spécifique dans l'ordre juridique français.

212. Des propositions de loi non abouties. la France a procédé par tâtonnements avant d'aboutir au présent délit d'usurpation d'identité numérique, plusieurs choix répressifs ayant été débattus devant le Parlement. Le législateur a souhaité dans un premier temps la création d'un délit venant appréhender le comportement d'usurpation d'identité numérique en intégrant une nouvelle infraction dans la section du Code pénal relative aux atteintes aux STAD[654]. Il en a résulté plusieurs propositions de loi visant à créer un nouvel article 323-8 qui n'ont cependant pas abouti. Le Sénat s'est ainsi intéressé une première fois aux problématiques liées à l'appréhension pénale de l'usurpation d'identité numérique le 4 juillet 2005[655]. La proposition de loi mise en avant suggérait la création d'un nouvel article 323-8 du Code pénal punissant « *d'un an d'emprisonnement et de 15 000 € 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* ». Le texte précisait 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* ». Cette mesure présentait beaucoup d'avantages : premièrement, le choix du terme « *tout réseau informatique de communication* » permettait d'englober les réseaux internes d'entreprises ou d'administrations alors que celui de « *réseaux de communication au public en ligne* » se limite à internet ; deuxièmment, le texte d'infraction prévoyait expressément l'atteinte à une personne physique mais également à une personne morale, publique ou privée ce qui contribuait encore à la largesse de son champ d'application et à la capacité du texte d'infraction à saisir les hypothèses diverses et variées que peut révéler un comportement d'usurpation d'identité numérique ; enfin, l'incrimination proposait d'exclure la confusion des peines assurant une effectivité de la sanction. Cette proposition de loi, bien qu'en partie saluée[656], n'a cependant pas aboutie. Une autre proposition fondée sur une rédaction différente fut déposée le 15 octobre 2008 à l'assemblée

[653] *UK Public General Acts*, *Fraud Act* 2006 (c. 35).
[654] C. pén., Livre III, Titre II, Chapitre III « *Des atteintes aux systèmes de traitement automatisé de données* ».
[655] Proposition de loi n° 452 tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques présentée par Michel DREYFUS-SCHMIDT, session extraordinaire de 2004-2005, annexe au procès-verbal de la séance du 4 juillet 2005.
[656] V. en ce sens : F. MATTATIA, « L'usurpation d'identité sur internet dans tous ses états », *RSC* 2014, p. 331 ; F. MATTATIA, « La création d'un délit d'usurpation d'identité sur l'Internet », *Gaz. Pal.*, 26 juillet 2008, n° 208, p. 6.

nationale[657]. Le groupe de députés à l'origine de cette proposition estimait que les incriminations préexistantes de contrefaçon, d'escroquerie ou d'atteinte à un STAD révélaient un « *vide juridique ayant impliqué une jurisprudence casuistique* » et proposèrent en réaction la création d'un article 323-8 du Code pénal selon lequel « *le fait de récupérer des données personnelles sensibles telles des données nominatives, bancaires ou professionnelles par le biais de l'usurpation d'identité adaptée au support numérique* [soit] *puni d'une peine d'emprisonnement comprise entre une et trois années en fonction de la gravité de l'usurpation réalisée ainsi que d'une amende s'élevant à 45 000 €* ». La présente proposition associait cependant maladroitement la notion de « *données personnelles sensibles* » à celles de « *données nominatives, bancaires ou professionnelles* » qui regroupent des réalités bien différentes[658]. Par ailleurs, le comportement répréhensible était assimilé au fait de « *récupérer des données personnelles sensibles […] par le biais de l'usurpation d'identité* », par conséquent, une telle rédaction ne permettait pas d'appréhender le comportement d'usurpation d'identité de manière autonome.

Le législateur a souhaité dans un deuxième temps intégrer ce nouveau délit dans la section du Code pénal relative aux atteintes volontaires à l'intégrité de la personne et plus particulièrement dans le paragraphe relatif aux violences[659]. le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure enregistré à la présidence de l'Assemblée nationale le 27 mai 2009[660] proposait alors sur la base du délit d'appels téléphoniques malveillants prévu à l'article 222-16 du Code pénal un nouvel article 222-16-1 réprimant « *le fait d'utiliser, de manière réitérée, sur un réseau de communication électronique l'identité d'un tiers ou des données qui lui sont personnelles, en vue de troubler la tranquillité de cette personne ou d'autrui* » et sanctionnant ces comportements d'une peine d'un an d'emprisonnement et de 15 000 € d'amende. Le projet de loi prévoyait également la rédaction d'un second alinéa punissant des mêmes peines « *le fait d'utiliser, sur un réseau de communication électronique, l'identité d'un tiers ou des données qui lui sont personnelles, en vue de porter atteinte à son honneur ou à sa considération* ». Cependant, cette idée

[657] Proposition de loi n° 1172 visant à lutter contre la récupération de données personnelles sensibles par le biais de l'usurpation d'identité adaptée au support numérique, enregistrée à la Présidence de l'Assemblée nationale le 15 octobre 2008.
[658] Selon l'article 9 du RGPD reprenant les termes de l'article 8 de la directive 95/46/CE, les données sensibles comprennent les données qui révèlent « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».
[659] C. pén., Livre II, Titre II, Chapitre II, Section 1, Paragraphe 2 « *Des violences* ».
[660] AN. n° 1697, projet de loi, d'orientation et de programmation pour la performance de la sécurité intérieure enregistré à la présidence de l'Assemblée nationale le 27 mai 2009, art. 2.

d'incrimination ne fut pas adoptée, certains observant notamment que « *le rattachement aux violences de l'usurpation d'identité semblait procéder d'un certain artifice* »[661].

213. La nouvelle incrimination de l'article 226-4-1 du Code pénal. Le délit d'usurpation d'identité numérique a finalement trouvé sa place au sein du Code pénal dans la section relative aux atteintes à la vie privée[662] suite à l'adoption de la loi n° 2011-267 du 14 mars 2011 dite LOPPSI II. Depuis les travaux préparatoires de la loi LOPPSI II, jusqu'à l'insertion du délit d'usurpation d'identité numérique dans le Code pénal, la présente incrimination subit toutefois de nombreuses modifications, seul le terme « *d'identité* » perdurant tout au long de l'écriture du texte[663]. Ainsi, initialement cantonné au seul espace numérique, le texte d'infraction s'est par la suite élargi afin d'être applicable aussi bien à l'espace virtuel qu'à l'espace réel. La rédaction s'est également progressivement affinée en distinguant d'un côté « *le fait d'usurper l'identité d'un tiers* » et d'un autre côté, « *le fait de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier* ». Enfin, la condition de réitération prévue dans la première version du texte a été écartée lors des débats parlementaires. Malgré ces multiples évolutions rédactionnelles le délit manifeste dès son origine la volonté de faire de l'usurpation d'identité un délit autonome « *dont la constitution n'est soumise à aucune autre condition que celles ressortant de la réunion de ses propres éléments matériels et moral* »[664].

Désormais, il est prévu à l'article 226-4-1 du Code pénal que « *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, est puni d'un an d'emprisonnement et de 15 000 € d'amende* ». Cette nouvelle incrimination démontre en l'occurrence son adaptation aux nouvelles formes d'atteintes à l'identité des individus permises par les réseaux sociaux en ligne, d'une part en appréhendant les différentes facettes de l'identité des indvidus (**§1**) et en offrant d'autre part une large protection contre les atteintes à l'identité (**§2**).

[661] A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *JCP* G n° 35, 29 août 2011, doctr. 913.
[662] C. pén., Livre II, Titre II, Chapitre VI, Section 1 « *De l'atteinte à la vie privée* ».
[663] A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *op. cit.*
[664] L. SAENKO, « Le nouveau délit d'usurpation d'identité numérique », *RLDI*, 2011, n° 72.

§1. Une appréhension des différentes facettes de l'identité des individus

214. Le délit d'usurpation d'identité entré en vigueur en 2011 a été l'occasion pour le législateur d'appréhender la notion d'identité numérique dans son entier et d'adapter ainsi la protection pénale de l'identité aux différents supports sur lesquels elle se manifeste. En l'occurrence, l'étude des éléments matériels de l'incrimination de l'article 226-4-1 du Code pénal révèle une appréhension particulièrement large de la notion d'identité permettant d'y inclure les éléments de l'identité numérique sociale (B). Cette nouvelle incrimination possède toutefois avant tout l'avantage d'appréhender de manière autonome l'identité (A).

A. Une appréhension autonome de l'identité

215. Une incrimination protégeant l'identité. Contrairement aux infractions antérieures, l'idée n'est plus de protéger un usage préjudiciable de l'identité d'un individu mais la personnalité même de ce dernier. Plus particulièrement, cette nouvelle incrimination manifeste l'intention du législateur d'appréhender les différentes formes d'atteintes à l'identité, y compris à l'échelle numérique, de façon efficace et explicite. La volonté première du législateur fut en conséquence d'adopter un délit sanctionnant le comportement d'usurpation d'identité de manière autonome, là où les délits de diffamation, d'escroquerie ou d'atteinte aux STAD ne permettent pas de sanctionner le comportement. Principalement, la nouvelle incrimination rend condamnable l'usurpation de l'identité d'autrui sur internet alors même qu'il n'en n'aurait résulté aucun préjudice financier ou aucune atteinte à l'autorité de l'État[665]. La seule identité de l'individu devient l'élément central de l'incrimination alors qu'elle constituait auparavant davantage un moyen de commission de l'infraction.

216. Une protection rattachée à une atteinte à la personnaltié. La place occupée par le délit d'usurpation d'identité numérique au sein du Code pénal n'est en outre pas anodine. Ce dernier figure dans la Section du Code pénal relative aux atteintes à la vie privée et *a fortiori* dans la partie du Code consacrée aux atteintes à la personnalité[666]. Ce choix du législateur doit être salué du fait que les autres délits précédemment mentionnés et protégeant l'identité, civile cette fois, se retrouvent à d'autres endroits du Code pénal bien loin des atteintes à la

[665] Rapport AN n° 2271, sur le projet de loi n° 1697 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2), enregistré à la présidence de l'assemblée nationale le 27 janvier 2010, p. 36.
[666] C. pén., Livre 2, Titre 2, Chap. VI « *Des atteintes à la* personnalité », Section 1 « *de l'atteintes à la vie privée* », Art. 226-1 et suiv.

personnalité[667]. En effet, alors que les infractions préexistantes protégeaient des valeurs sociales telles que l'autorité de l'État pour l'article 433-19 ou encore l'exercice de la justice pour l'article 434-23, l'infraction de l'article 226-4-1 instaure une protection autonome de l'identité de l'individu sur le fondement d'une atteinte à la vie privée. Le résultat redouté consiste dès lors dans une atteinte à la personnalité, et plus particulièrement dans une atteinte à la vie privée contribuant ainsi à une évolution profonde de l'appréhension pénale de l'identité au regard des textes préexistantes. Le législateur est venu toutefois complexifier l'identification de la *ratio legis* du texte en exigeant que le comportement d'usurpation d'identité soit réalisé en vue de troubler la tranquillité de l'individu ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération. Partant, « *L'usurpation d'identité apparaît alors réprimée non pas* per se *mais seulement comme vecteur de ce risque de trouble ou d'atteinte* »[668]. L'incrimination n'élève cependant pas ce risque d'atteinte en élément matériel de l'infraction mais simplement en but poursuivi par l'auteur. Partant, le risque de trouble à la tranquillité, ou l'atteinte à l'honneur ou à la considération, peut s'envisager comme la conséquence de l'atteinte primaire consistant à usurper l'identité d'un tiers et portant une atteinte directe à la personnalité de ce dernier.

B. Une appréhension large de l'identité

217. Une protection de l'identité numérique et civile. Le délit de l'article 226-4-1 du Code pénal ne vise plus le « *nom* » en tant qu'émanation de l'identité civile mais « *l'identité* » ou les « *données de toute nature permettant l'identification* ». En raison du caractère englobant de ces notions, cette rédaction permet d'inclure autant les éléments de l'identité civile d'une personne que ses attributs numériques. Toutefois, si le champ d'application de cette infraction ne se cantonne pas à l'univers numérique, ce dernier n'en est pas moins le fer de lance de la réforme. L'article 2 de la loi du 4 mars 2011 prévoyant la création du délit d'usurpation d'identité figure d'ailleurs dans un chapitre intitulé « *lutte contre la cybercriminalité* ». Le législateur a cependant jugé nécessaire de prévoir au second alinéa de l'article que « *cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne* ». Ce second alinéa qui peut s'interprêter comme la volonté pour le législateur d'affirmer de manière explicite l'application de ce délit à

[667] Le délit d'usage d'un faux nom de l'article 434-23 du Code pénal se retrouve par exemple dans la section du Code pénal consacrée aux « *entraves à l'exercice de la justice* ». Le délit de l'article 433-19 du Code pénal se trouve quant à lui dans la section du Code pénal consacrée aux « *atteintes à l'état civil des personnes* ».
[668] A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *op. cit.*

l'environnement de l'internet, semble toutefois superflu au regard du caractère général du premier alinéa qui n'excluait pas de son champ d'application les réseaux de communication au public en ligne[669].

218. La notion d'identité. La nouvelle incrimination ne prend pas le soin de définir en son sein la notion d'identité. Par référence à la conception civiliste, l'identité renvoie à l'ensemble des éléments pouvant permettre d'identifier une personne. Elle comprend aussi bien le nom, le prénom, le lieu de naissance, la date de naissance, la situation de famille, le domicile ou encore la profession[670]. Cette conception d'une extrême largesse s'accoutumerait toutefois mal aux exigences du principe de légalité criminelle. L'identité doit alors être entendue sur la base de l'usurpation de nom prévue à l'article 434-23 du Code pénal[671]. En outre, la lecture des travaux préparatoires de la loi LOPPSI II révèle que l'identité dans le domaine numpérique « *doit être considérée comme recouvrant tous les identifiants électroniques de la personne, c'est-à-dire à la fois son nom, mais aussi son surnom ou son pseudonyme utilisé sur internet* »[672]. En définitive, la notion d'identité prévue à l'article 226-4-1 du Code pénal repose principalement sur le nom de la personne mais entendu dans son sens le plus large de manière à intégrer les spécificités des manifestations de l'identité à l'échelle numérique, *« bref, l'identité en ce sens, c'est la façon dont la personne s'appelle ou se fait appeler* »[673].

219. La notion de donnée de toute nature permettant d'identifier un tiers. De la même manière que pour l'identité, le législateur n'a pas défini la notion de « *données de toute nature permettant d'identifier un tiers* ». Le texte faisait à l'origine référence aux « *données personnelles* » définies comme « *toute information se rapportant à une personne physique identifiée ou identifiable* » sachant qu' « *est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son*

669 V. en ce sens : N. RIAS, « Usurpation d'identité ou usage de données permettant d'identifier un tiers », *J.-Cl.* Pénal Code, fasc. 20, mai 2012 (mis à jour septembre 2018), n° 2 ; E. VERNY, « Usurpation d'identité », *J.-Cl.* Comm., fasc. 58, juillet 2015 (mis à jour janvier 2018), n° 12 ; A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *op. cit.*
670 V. *supra* n° 189.
671 A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *op. cit.*
672 E. CIOTTI, Rapp. AN. n° 2271, 1ère lecture. 27 janvier 2010 sur le projet de loi, d'orientation et de programmation pour la performance de la sécurité intérieure, p. 112.
673 A. LEPAGE, « Le délit d'usurpation d'identité : questions d'interprétation », *op. cit.*

identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[674]. Au vu de cette définition, la notion de donnée personnelle recouvre un champ plus large que l'identité qui renvoie principalement au nom sous lequel une personne est reconnaissable. Le législateur a toutefois remplacé l'expression « *données personnelles* » par « *données de toute nature permettant d'identifier un tiers* » ayant pour effet d'étendre encore un peu plus le champ d'application du texte. La formulation retenue permet d'accorder une protection accrue à l'internaute au regard des nombreux éléments pouvant permettre de l'identifier sur internet[675]. L'infraction vise : le pseudonyme, le numéro de sécurité sociale, le numéro de compte bancaire, le numéro de téléphone, l'adresse électronique[676] mais aussi, l'image, le logo, le dessin, le sigle ou encore l'avatar[677]. L'adresse IP, les codes d'accès, les login et mots de passe semblent aussi concernés par le texte d'infraction[678]. L'intégration de la notion de donnée dans le texte d'incrimination permet pour ce dernier de se saisir de toute la complexité inhérente au caractère protéiforme des éléments relevant de l'identité, particulièrement dans le domaine numérique. Cependant, la même interrogation demeure : la rédaction du délit n'offre-t-elle pas un champ d'application trop étendu à l'identité numérique ? Le législateur semble distinguer d'une part l'identité de la personne et d'autre part les données permettant de l'identifier, ces dernières revêtant un champ d'application encore plus large. Cependant, le texte l'incrimination sanctionne de manière égale l'usurpation d'identité ou l'usage de données identifiantes révélant ainsi un champ d'application extrêmement large.

220. En définitive, l'incrimination de l'article 226-4-1 du Code pénal propose une rédaction permettant d'englober l'ensemble des manifestations de l'identité numérique y compris, celles observées sur les réseaux sociaux en ligne. Il est cependant impératif de trouver la juste mesure dans l'appréhension des comportements pour que cette nouvelle incrimination ne soit pas sanctionnée pour sa trop grande largesse. Pour ce faire, la sanction de l'usurpation d'identité numérique doit intervenir lorsque l'atteinte porte, au moins en partie, sur le nom de la personne entendu dans son sens large. Dans cette hypothèse les autres

[674] Cette définition autrefois prévue à l'article 2 de la directive 95/46/CE sur la protection des données à caractère personnel du 24 octobre 1995 se retrouve désormais à l'article 4 (1) du Règlement (UE) 2016/679 sur la protection des données (RGPD) du 27 avril 2016.
[675] I. SOSKIN, « Les nouvelles formes d'atteintes à la "réputation" et à "l'image" de la personne dans l'environnement numérique », *Légipresse*, n° 336, mars 2016, p. 145.
[676] Circ. n° JUSD1121169C, 28 juillet 2011, relative à la présentation des dispositions de droit pénal général et de procédure pénale de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure : BO min. Just. 31 août 2011.
[677] I. SOSKIN, « Les nouvelles formes d'atteintes à la "réputation" et à "l'image" de la personne dans l'environnement numérique », *op. cit.*, p. 145.
[678] N. RIAS, « Usurpation d'identité ou usage de données permettant d'identifier un tiers », *J.-Cl.* Pénal Code, fasc. 20, mai 2012 (mis à jour septembre 2018), n° 9.

éléments composant l'identité numérique peuvent également être pris en compte dans la démonstration des éléments constitutifs de l'infraction mais la présence d'une atteinte, directe ou indirecte, au nom demeure nécessaire pour parvenir à la conclusion de l'atteinte pénale à l'identité numérique.

§2. Une large protection contre les atteintes à l'identité

221. Le délit de l'article 226-4-1 du Code pénal offre par ailleurs une protection large des atteintes à l'identité. D'une part la rédaction de l'incrimination permet de protéger l'identité contre diverses formes d'atteintes (A), d'autre part, le législateur n'est pas venu exiger la réalisation d'un résultat matériel faisant de cette infraction un délit formel (B).

A. La protection de l'identité contre diverses formes d'atteintes

222. La diversité des atteintes à l'identité numérique. Le droit pénal vient avant tout sanctionner une atteinte à l'identité numérique. Au travers de cette sanction plusieurs formes d'identités entrent sous sa protection. Sur les réseaux sociaux, si l'identité numérique peut être copiée, créée ou usurpée, elle peut en outre concerner l'identité d'une personne morale. La sanction de ces comportements par la jurisprudence permet de développer en parallèle la notion pénale d'identité numérique. Les actes incriminés par le texte d'infraction (1) seront confrontés aux actes sanctionnés par la jurisprudence (2).

1) Les actes incriminés par le texte d'infraction

223. Usurper l'identité d'un tiers. À l'origine l'identité était couplée avec le terme utiliser. Le législateur a cependant choisi de modifier la rédaction en associant l'identité avec le verbe usurper renvoyant au fait de s'attribuer sans droit, donc de manière illégitime, l'identité d'un tiers dans le but de se faire passer pour lui[679]. Cette rédaction permet ainsi d'éviter que le simple fait de citer le nom d'un tiers dans une publication puisse entraîner la qualification de l'infraction d'usurpation d'identité numérique[680]. La définition de l'infraction se trouve alors plus proche du comportement visé.

[679] N. RIAS, « Usurpation d'identité ou usage de données permettant d'identifier un tiers », *J.-Cl.* Pénal Code, fasc. 20, mai 2012 (mis à jour septembre 2018), n° 6.
[680] Rapport AN n° 2271, sur le projet de loi n° 1697 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2), *op. cit.* ; D. BOURGAULT-COUDEVYLLE, « La protection pénale de

224. Faire usage de données permettant l'identification d'une personne. Le texte conserve toutefois le terme « *utiliser* » qui demeure lié aux données d'identification. Plus précisémenent, l'élément incriminé concerne l' « *usage* » de données permettant l'identification d'une personne. L'usage concerne dans ce cas la simple utilisation de l'objet (les données) indépendamment d'une volonté de se faire passer pour autrui. Les données peuvent ainsi être utilisées pour satisfaire un unique besoin matériel[681] alors que l'identité nécessite l'intention de s'accaparer la personnalité de la personne visée. Cette distinction opérée au sein de l'article 226-4-1 du Code pénal traduit la volonté de ne pas élever au rang de l'identité d'une personne des données qui permettent certes de l'identifier, mais qui ne symbolisent pas pour autant sa personnalité.

2) Les actes sanctionnés par la jurisprudence

225. L'identité copiée. Le délit d'usurpation d'identité peut concerner dans un premier temps le fait de reproduire une identité numérique préexistante à l'image d'un faux site internet adoptant la même apparence que le site d'origine. Sur ce point, la Cour de cassation a confirmé le 16 novembre 2016 la condamnation pour usurpation d'identité numérique d'un ingénieur informaticien qui avait créé un faux site de la maire d'un arrondissement de Paris[682]. L'individu avait en l'espèce exploité une faille de sécurité liant le faux site avec le site officiel de la maire[683]. Selon l'enquête, la fausse interface permettait à des internautes de mettre en ligne des messages sous forme de communiqués de presse qui paraissaient rédigés par l'élue elle-même. Le prévenu fut poursuivi pour introduction frauduleuse de données dans un système informatisé et pour usurpation d'identité numérique et condamné à 3000 euros d'amende en première instance[684]. En appel, les juges du fond confirmèrent la condamnation mais sous le seul fondement unique du délit d'usurpation d'identité numérique[685]. Pour justifier la condamnation, les juges du fond ont expliqué que même si la page d'accueil du

---

l'identité », *in* V. MUTELET et F. VASSEUR-LAMBRY (dir.), *Qui suis-je, dis-moi qui tu es. L'identification des différents aspects juridiques de l'identité*, Artois Presses-Université, 2015, p. 258.

[681] Par exemple, se servir des identifiants de la personne dans le but de bénéficier des services qu'ils permettent d'obtenir.

[682] Crim., 16 novembre 2016, nº 16-80.207 : *CCE* n° 1, janvier 2017, comm. 6, A. LEPAGE ; *RLDI*, 2017, n° 133, obs. L. COSTES.

[683] Le prévenu avait habilement exploité cette faille en créant une sorte de tunnel afin d'y injecter du code indirect ce qui entrainait la modification du comportement du site (il s'agit d'une opération dite « *XSS* » ou *cross-site scripting*) ; V. J. FRANCILLON, « Piratage informatique. Usurpation d'identité numérique. L'affaire du « faux site officiel » de Rachia Dati : une étape dans la lutte contre la cyberdélinquance », *RSC*, janvier-mars 2015, p. 101.

[684] TGI Paris, 13ème ch. corr., 18 décembre 2014, n° 12010064012 : *RLDI*, 2015, n° 111, Obs. J. de ROMANET ; *RSC*, janvier-mars 2015, p. 101, chron. J. FRANCILLON.

[685] Paris, chambre 2-7, 13 novembre 2015.

faux site n'était pas exactement similaire à celle du site de la plaignante, le délit d'usurpation d'identité se trouvait quand même constitué. La reproduction d'une photographie de l'élue ainsi que les éléments principaux de la charte graphique de son site officiel ont en l'occurrence suffi à retenir que le délit de l'article 226-4-1 du Code pénal était constitué. En confirmant sans réserve l'arrêt de la Cour d'appel de Paris, la Cour de cassation reconnaît dès lors que l'usurpation est admise lorsque le doute est permis dans l'esprit du public. En conséquence, nul besoin que l'identité soit une reproduction fidèle d'une interface préexistante, il suffit qu'elle soit dotée d'une crédibilité suffisante pour que le public, voire les proches de la victime, puissent être trompés. À l'inverse, la parodie grossière ou clairement exprimée d'un individu, ne peut fonder le délit d'usurpation d'identité. Cette interprétation jurisprudentielle traduit une conception large de l'identité sous forme numérique, cette dernière s'émancipe des éléments techniques classiques de l'identité numérique tels que l'adresse IP, le nom de domaine ou la messagerie. L'identité repose en définitive davantage sur sa crédibilité que sur sa véracité.

226. L'identité créée. Sur les réseaux sociaux en ligne, le comportement le plus fréquent revient à créer de toutes pièces un faux profil d'une personne existante afin de troubler le public, l'entourage de la victime ainsi qu'elle-même. À cet égard, les exemples se multiplient, l'article 226-4-1 du Code pénal étant devenu en la matière un outil de répression. Par exemple, un individu fut condamné sur ce fondement à un an d'emprisonnement assorti du sursis avec mise à l'épreuve d'une durée de trois ans et sur le plan civil, à 40 000 € de dommages et intérêts au titre du préjudice matériel et 20 000 € au titre du préjudice moral[686]. Cette condamnation empreinte de sévérité fut prononcée à la suite d'un différend commercial entre le prévenu et son associé. En l'espèce, l'individu avait modifié les paramètres d'accès de la messagerie électronique de son associé afin de créer à partir de ses coordonnées de fausses adresses de messagerie électronique ainsi que des faux profils Facebook sur lesquels il avait publié des propos diffamatoires et insultants. Il avait également passé de fausses annonces sur des sites de rencontres et des sites de vente entre particuliers. Dans une autre affaire, le tribunal de grande instance de Paris[687] fut à nouveau saisi d'un cas d'usurpation d'identité numérique sur un site de réseau social. En l'espèce, après avoir entretenu une liaison avec un collègue à laquelle ce dernier avait mis fin, une femme décida pour se venger de créer un faux compte Facebook sous le nom et le prénom de ce collègue. Elle y avait notamment publié des photos de lui et de sa compagne et tenu des propos injurieux en son nom. L'enquête révéla

[686] Paris, 10 Octobre 2014, n° 13/7387 : *CCE*, n° 1, décembre 2015, comm. 9, É. A. CAPRIOLI.
[687] TGI Paris, 17ème ch. corr., 24 mars 2015 : *CCE* n° 10, Octobre 2015, comm. 86, É. A. CAPRIOLI.

que le compte litigieux avait été ouvert à partir d'une adresse de courriel dont le titulaire était un ami de cette femme. Les deux prévenus ayant reconnu les faits, le tribunal a considéré que les éléments caractérisant l'usurpation d'identité étaient caractérisés et condamna respectivement les deux individus à des peines de 4 000 € et 3 000 € d'amende et à un total de 5 000 € de dommages et intérêts en réparation du préjudice moral. Ces différents exemples jurisprudentiels[688] permettent d'éclairer l'interprétation donnée aux élements constitutifs de l'infraction. En l'occurrence, la sanction de l'usurpation d'identité repose sur une pluralité d'éléments incluant la création de faux profils sur les sites de réseaux sociaux mais également le fait d'alimenter ces profils par des commentaires, statuts ou photos. Les éléments de l'identité numérique sociale sont ainsi pleinement pris en considération par le juge dans l'application de l'article 226-4-1 du Code pénal.

227. L'identité usurpée. Le présent délit d'usurpation d'identité numérique concerne en outre l'hypothèse d'un « *vol* » d'identité à savoir le cas où un individu s'empare du compte ou profil numérique déjà existant d'une tierce personne. Bien que ce type d'agissement puisse être sanctionné sous d'autres fondements[689], le délit de l'article 226-4-1 du Code pénal vient également appréhender ce type de comportement. La présente situation amène à un concours de qualifications où une activité matérielle unique est susceptible de tomber sous le coup de plusieurs incriminations. Le concours de qualifications se résout en principe par une unité de qualification[690] auquel cas le fait unique doit être réprimé « *sous sa plus haute expression pénale* »[691]. Il est cependant des exceptions où les différentes qualifications sont retenues

[688] D'autres exemples peuvent encore être cités tels que : TGI Paris, 24ème ch. corr. 1, 21 nov. 2014, n° 10183000010 et n° 13311000700 : *CCE* 2015, comm. 85, É. CAPRIOLI – TGI Paris, réf., 12 août 2016 : *CCE* 2016, comm. 105, É. CAPRIOLI – Paris, pôle 3, ch. 5, 13 avril 2016 : *Dr. pén.* 2016, chron. 11, A. LEPAGE.

[689] V. *supra* n° 207.

[690] Selon la jurisprudence, le principe de solution du concours idéal de qualifications est l'unité de qualification. Les fondements juridiques de cette solution diffèrent cependant. Certaines décisions utilisent la règle *non bis in idem*, en considérant qu'un même fait autrement qualifié ne peut entraîner une double déclaration de culpabilité. Crim., 25 février 1921 : *S.* 1923, 1, 89, note J.-A. ROUX – Crim., 28 janvier 1969 : *Bull. crim.* n° 51 – Crim., 26 mars 1974 : *Bull. crim.* n° 129 – Crim., 22 novembre 1983 : *Bull. crim.* n° 308 – V. aussi CEDH, *Oliveira c/ Suisse*, 30 juillet 1998, n° 25711/94, § 22 – CEDH, *Fischer c/ Autriche*, 29 mai 2001, n° 37950/97, § 25 – CEDH, *Garetta c/ France*, 4 mars 2008, n° 2529/04, § 78. *Adde* : P. BONFILS et E. GALLARDO, Rép. pén., Dalloz, *V°* Concours d'infractions, n° 30.

[691] Principe rappelé de manière constante par la Cour de cassation : Crim. 26 juin 1930 : *Bull. crim.* n° 190 – Crim. 29 novembre 1956, *JCP* 1957. II. 9727, note M. de CHAMBON – Crim. 20 novembre 1978 : *Bull. crim.* n° 323 – Crim. 15 décembre 1993, n° 93-84.515 : *Bull. crim.* n° 389 – Crim. 16 mai 2006, n° 05-86.860 : inédit ; *Dr. pén.* 2006, comm. 121, J.-H. ROBERT. Ce principe a été validé par le Conseil constitutionnel qui selon lui : « *en vertu de l'article 8 de la Déclaration de 1789, la loi ne doit établir que des peines strictement et évidemment nécessaires [et] que le principe de proportionnalité qui en découle implique que, lorsque plusieurs dispositions pénales sont susceptibles de fonder la condamnation d'un seul et même fait, les sanctions subies ne peuvent excéder le maximum légal le plus élevé* ». Cons. const., 12 janvier 2002, DC n° 2001-455 : *RSC* 2002, p. 674, obs. V. BÜCK. Enfin, rappelons que lorsque les deux qualifications en concours idéal ont une sévérité identique, la jurisprudence fait alors primer « l'infraction-fin » sur « l'infraction-moyen » : J. PRADEL, *Droit pénal*

cumulativement. C'est le cas lorsqu'une seule et unique activité matérielle tombe sous le coup de plusieurs qualifications et révèle une atteinte à plusieurs valeurs sociales protégées différentes[692]. Or, l'introduction sur le profil numérique d'un individu peut révéler à la fois une volonté de porter atteinte à un bien, en l'occurrence le STAD, mais également une volonté de porter une atteinte à la personne, précisément à son identité numérique. Le juge peut donc retenir cumulativement le délit de l'article 226-4-1 du Code pénal et un des délits prévus aux articles 323-1 et suivants, réprimant les atteintes aux STAD. Par contre, si l'usurpation d'identité ne constitue qu'un élément d'un comportement infractionnel plus large il faut privilégier la qualification qui permet d'englober l'ensemble des faits. En d'autres termes, la qualification la plus large sera retenue au détriment de celle qui n'est que partielle[693]. Il en est ainsi si le comportement d'usurpation d'identité sert en réalité à réaliser une escroquerie. Dans ce cas, le juge doit retenir la qualification du délit d'escroquerie prévu à l'article 313-1 du Code pénal.

228. L'identité de la personne morale. L'une des critiques adressées à l'encontre du délit d'usurpation d'identité numérique était que son application aux personnes morales semblait difficile en raison de la place de l'infraction au sein du Code pénal[694], plus particulièrement dans le titre relatif aux atteintes à la personne humaine[695]. Le rapport sur la cybercriminalité de février 2014 avait toutefois précisé que l'article 226-4-1 du Code pénal « *est suffisamment large pour réprimer toute usurpation d'identité numérique, y compris au préjudice des personnes morales et donc des entreprises* »[696]. Certaines propositions de loi ont voulu prévoir de manière spécifique l'application du délit d'usurpation d'identité numérique aux entreprises mais n'ont cependant pas été suivies d'effets[697]. L'absence de disposition explicite permettant l'application du texte aux personnes morales ayant la qualité de victimes doit être

général, 19ème éd., 2012, Cujas, nº 297, p. 270. *Adde* : P. BONFILS et E. GALLARDO, Rép. pén., Dalloz, *V°* Concours d'infractions, n° 31.

[692] L'exemple le plus célèbre est celui du jet d'une grenade à l'intérieur d'un café à des fins terroristes, qui peut à la fois relever d'une tentative de destruction d'édifice et d'une tentative d'homicide volontaire avec préméditation. Crim. 3 mars 1960 : *Bull. crim.* nº 138 ; *RSC* 1961. 105, obs. Legal. ; J. PRADEL et A. VARINARD, *Les grands arrêts du droit pénal général*, 8e éd., 2013, Dalloz, nº 49, p. 266 – Crim., 8 novembre 1977 : *Bull. crim.* nº 339. – Crim., 21 septembre 1999, nº 97-85.551 : *Bull. crim.* nº 191 ; *D.* 2000. Somm. 383, obs. M.-C. AMAUGER-LATTES ; *RSC* 2000, p. 200, obs. Y. MAYAUD.

[693] Par exemple, la Cour de cassation a retenu l'homicide involontaire causé par une conduite en état d'ivresse et non la conduite sous l'influence de l'alcool : Crim. 3 octobre 1984, Bull. crim. nº 285.

[694] É. CAPRIOLI, « Usurpation d'identité par création d'adresses mails et de faux profils Facebook », *CCE* n°1, janvier 2015 comm. 9.

[695] C. pén., Livre II, Titre II : « *Des atteintes à la personne humaine* ».

[696] Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes. Rapport sur la cybercriminalité*. Février 2014. p. 153.

[697] Sénat, prop. de loi n° 452, 4 juillet 2005 tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques ; Sénat, prop. de loi n° 86, 6 novembre 2008 relative à la pénalisation de l'usurpation d'identité numérique.

cependant nuancée. D'une part l'article 2 du Code de procédure pénale ne restreint pas l'action civile aux seules personnes physiques. L'action en réparation du dommage causé par un crime, un délit ou une contravention « *appartient à tous ceux qui ont personnellement souffert du dommage directement causé par l'infraction* ». Ainsi, il est reconnu que la qualité de victime et la capacité à agir concernent tout aussi bien les personnes physiques que les personnes morales[698]. De manière large, la victime est considérée comme toute personne en souffrance, cette dernière pouvant être directe ou indirecte, individuelle ou collective ou enfin, qu'elle atteigne une personne physique ou morale[699]. Il doit alors être rappelé que les personnes morales constituent une réalité et non une fiction[700] et deviennent un sujet de droit susceptible d'engager leur responsabilité mais également de subir des infractions[701]. Les personnes morales sont dotées de la personnalité juridique et bénéficient de tous les attributs extrapatrimoniaux qui ne sont pas exclusivement attachés à la personne humaine[702]. Dans un premier temps, la jurisprudence est venue reconnaître une usurpation d'identité numérique d'une entreprise mais par l'intermédiaire de son dirigeant. À ce titre, l'arrêt de la Cour d'appel de Paris du 10 octobre 2014[703] envisage pour la première fois une condamnation d'une personne ayant usurpé l'identité d'un dirigeant d'entreprise. Cette jurisprudence admet le droit pour une entreprise à agir sur le fondement de l'article 226-4-1 du Code pénal au travers de son dirigeant social en cas d'atteinte à son e-réputation[704]. Pour que l'action civile soit exercée par l'entreprise elle-même victime d'une usurpation encore faut-il qu'elle justifie d'un préjudice personnel et direct[705]. Dans un jugement postérieur du 21 novembre 2014, les juges du fond allèrent dans ce sens en indiquant que le prévenu avait créé des profils en utilisant le nom d'une société et que cette dernière « *a été victime de la part de Mme L. A. d'une usurpation d'identité en vue de porter atteinte à son honneur ou à sa considération en utilisant un réseau de communication au public en ligne* ». Le jugement précisa que cette infraction « *cause un préjudice particulièrement grave à cette société, les termes utilisés*

[698] B. LAPÉROU-SCHENEIDER, « Action publique et action civile », *J.-Cl.* proc. pén., art. 2 à 3, mars 2008 (mis à jour mai 2019), fasc. 20, n° 11.
[699] R. CARIO, Rép. pén. Dalloz, juin 2018, *V°* Victimes d'infractions, n° 8.
[700] « *Les personnes morales n'ont ni chair, ni sang ; pourtant, elles ont des organes. Elles n'ont pas de sentiments ; pourtant, elles ont une volonté. Elles sont invisibles ; pourtant elles agissent et peuvent même se voir reprocher leur inaction. Elles n'ont pas de domicile ; pourtant elles ont un siège, etc* ». E. DREYER, *Droit pénal général*, LexisNexis, 5ème éd., 2019, p. 879, n° 1139.
[701] Civ., 28 janvier 1954 : jurispr. p. 217, note G. LEVASSEUR.
[702] J.-C. SAINT-PAU, « Droit au respect de la vie privée et droit pénal », *Dr. pén.* 2011, n° 9, étude 20.
[703] Paris, 10 octobre 2014, n° 13/7387 : *CCE* n° 1, décembre 2015, É. A. CAPRIOLI, comm. 9.
[704] L'entreprise, en tant que marque et bénéficiaire d'un droit de propriété intellectuelle, peut également engager une action en contrefaçon (art. L335-3 CPI) pour se protéger à l'égard d'une usurpation d'identité numérique.
[705] B. LAPÉROU-SCHENEIDER, « Action publique et action civile », *op. cit.*, n° 26.

mettant en cause son sérieux et sa probité »[706]. Suite à une usurpation d'identité, la société subit alors un préjudice moral justifiant sa qualité autonome de victime[707].

229. En conclusion, une appréhension large de la protection de l'identité. Les comportements d'usurpation d'identité concernent une multitude de possibilités dans le domaine numérique : l'identité peut être copiée à partir d'une préexistante, elle peut être créée de toute pièce, l'usurpation peut consister en l'intrusion ou le détournement frauduleux d'un profil numérique auquel cas le juge aura le choix entre plusieurs qualifications pénales et enfin le délit concerne également l'identité d'une personne morale. Pour sanctionner ces comportements divers et variés, le juge pénal peut dorénavant se fonder sur les prévisions de l'article 226-4-1 du Code pénal qui permet de saisir les différentes facettes de l'identité des individus y compris leur identité numérique sociale. À ce titre, autant l'identité numérique « *déclarative* » que l'identité numérique « *agissante* » servent d'éléments au juge pour venir prouver l'usurpation. Ceci est permis par la formulation large utilisée par le législateur et notamment par l'emploi du terme « *usage d'une ou plusieurs données de toute nature permettant de l'identifier* » qui permet d'englober l'identité numérique dans toutes ses manifestations. Toutefois, dans l'ensemble des comportements sanctionnés l'usurpation d'identité s'est accompagnée de l'usage du nom, entendu au sens large, de la victime. L'usage d'une seule photographie ne peut constituer en soi une usurpation d'identité, celle-ci doit être associée à la création d'un faux profil reprenant le nom de la personne ciblée. Dans toutes ces hypothèses, l'acte d'usurpation d'identité doit être commis dans l'intention de nuire à la tranquillité ou à l'honneur et à la considération de la personne. La jurisprudence a eu l'occasion de venir préciser les contours de cette condition.

B. Un délit formel

230. La protection large de l'identité numérique se déduit en outre du fait que l'article 226-4-1 du Code pénal est un délit formel n'exigeant pas la présence d'un résultat matériel (1) et bénéficiant d'une interprétation jurisprudentielle large de l'intentionnalité (2).

[706] TGI Paris, 24ème ch. corr. 1, 21 novembre 2014, n° 10183000010 et n° 13311000700 : *CCE*, n° 10, Octobre 2015, comm. 85, É. CAPRIOLI.
[707] É. CAPRIOLI, « Protection de l'information – atteinte à l'e-réputation de l'entreprise et de ses salariés », *CCE* n° 10, Octobre 2015, comm. 85.

1) L’absence d’exigence d’un résultat matériel

231. Le caractère formel du délit d’usurpation d’identité. L’agent doit commettre l’acte incriminé en vue de troubler la tranquillité de l’usurper ou de celle d’un tiers ou de porter atteinte à son honneur ou à sa considération. Il ne s’agit que d’un résultat redouté, autrement dit, il n’est pas nécessaire que l’individu y parvienne. L’infraction de l’article 226-4-1 du Code pénal est subordonnée à la constitution de ce dol spécial, en revanche elle n’est pas subordonnée à l’atteinte effective voulue par l’agent. L’intentionnalité de l’infraction est plus ample que sa matérialité manifestant son caractère formel[708]. Ainsi, le trouble à la tranquillité ou l’atteinte à l’honneur et à la considération fait partie de l’élément moral de l’infraction. L’article 226-4-1 exige alors un double niveau d’intentionnalité se retrouvant dans un dol général et un dol spécial.

232. Dol général. En tant que délit intentionnel, l’agent doit avoir la volonté consciente d’usurper l’identité d’un tiers ou de faire usage de données de toute nature permettant de l’identifier. Ce dol général qui unit la volonté à la matérialité des faits n’est pas suffisant pour saisir l’infraction dans sa globalité. Celle-ci se compose également d’un résultat redouté, élément de la volonté de l’auteur de l’infraction et non de la matérialité des faits.

233. Dol spécial. Les mots choisis par le législateur pour définir le but recherché par le délinquant renvoient à d’autres notions familières du droit pénal. La volonté de nuire à la tranquillité fait ainsi penser à l’infraction d’appels téléphoniques malveillants de l’article 222-16 du Code pénal. La jurisprudence relative à ce délit est particulièrement exigeante dans la preuve de l’atteinte à la tranquillité. Celle-ci se déduit de la réitération outrancière des appels mais également de la nuisance sonore qui accompagne ces derniers[709]. Le trouble de la tranquillité d’autrui au sens de l’article 222-16 du Code pénal s’observe matériellement. Il en est autrement pour le nouveau délit d’usurpation d’identité numérique. Le texte d’infraction semble distinguer l’acte d’usurpation d’identité et la volonté spéciale qui accompagne l’auteur de l’infraction. Le trouble à la tranquillité peut cependant se déduire du fait pour la victime d’être dépossédée de son identité et donc de la seule matérialité des faits.

234. En revanche, il en est autrement concernant le second résultat redouté : l’atteinte à l’honneur et à la considération de la victime. Ce dernier fait écho au délit de diffamation prévu à l’article 29 de la loi du 29 juillet 1881. La volonté de se comporter comme autrui doit

[708] À la différence d’une infraction matérielle qui suppose que le résultat soit effectivement atteint.
[709] Crim., 17 septembre 2014, n° 13-85637 : inédit.

alors s'accompagner de la volonté de porter atteinte à la réputation de l'individu visé. C'est sur ce point que l'article 226-4-1 du Code pénal dispose d'une force particulière au regard des nouveaux comportements rencontrés sur les sites de réseaux sociaux. L'infraction est à la fois assez englobante pour protéger les éléments de l'identité numérique de l'individu et elle prend en exigence, sans non plus l'élever au rang d'élément matériel, la volonté du délinquant de porter atteinte à la réputation de la personne dont il aurait usurpé l'identité. L'existence de ce dol spécial permet de préciser un peu plus le contour pénal de l'infraction et d'encadrer ainsi son champ d'application. Le juge pénal dispose donc d'un outil efficace lui permettant de sanctionner ce type de comportement qui n'entrait auparavant sous aucune qualification spécifique.

2) Une interprétation jurisprudentielle large de l'intentionnalité

235. Une intention et non une matérialité. Pour que le délit d'usurpation d'identité soit constitué l'auteur des faits doit avoir agi avec une intention malveillante dépassant le simple dol général. La jurisprudence est alors venue apporter des précisions quant à l'interprétation de ce dol spécial animant l'auteur de l'acte délictueux. En l'occurrence, dans l'affaire du faux site de la personnalité politique les juges du fond avaient démontré l'existence du trouble à la tranquillité de la victime[710]. Selon les juges, le fait de créer un site fictif et d'encourager de nombreuses personnes au moyen de sites de réseaux sociaux à rédiger des messages soit obscènes soit contenant des affirmations politiques contraires aux opinions de la personne ciblée est de nature à troubler la tranquillité de cette dernière, voire de porter atteinte à son honneur et à sa considération. La subtilité du présent cas réside dans le fait que la personne poursuivie n'avait pas elle-même écrit les communiqués de presse diffamatoires à l'encontre de l'élue mais avait simplement fourni les outils permettant à d'autres internautes de le faire. Le prévenu n'avait alors pas lui-même porté atteinte à l'honneur ou à la considération de la victime. Les juges du fond ont pourtant retenu que l'intention de nuire était caractérisée dès lors que le prévenu a mis en œuvre des moyens permettant aux internautes de publier des faux communiqués diffamatoires, d'autant plus que l'individu avait la possibilité en sa qualité de modérateur du site de supprimer ou, *a minima*, désapprouver le caractère diffamatoire ou injurieux des propos. Les enseignements tirés de cette jurisprudence sont nombreux. Premièrement, les prévenus ne pouvaient justifier leurs actes du fait que l'usurpation reprochée était seulement destinée à faire rire et que le caractère satirique et parodique du

[710] TGI Paris, 13ème ch. corr., 18 décembre 2014, n°12010064012 : *RLDI*, 2015, n° 111, obs. J. de ROMANET ; *RSC*, janvier-mars 2015, p. 101, chron. J. FRANCILLON.

faux site était exclusif de toute intention de nuire. Les juges leur ont en effet rétorqué que leurs motifs n'étaient ni légitimes, ni honorables. Le dol spécial requis par l'infraction à savoir « *troubler la tranquillité* » de la victime ou d'un tiers, « *ou de porter atteinte à son honneur ou à sa considération* » était caractérisé en l'espèce : « *l'insertion de faux communiqués entraînait à l'évidence des perturbations dans le fonctionnement normal du site officiel* »[711]. Deuxièmement, cette jurisprudence permet de clarifier l'articulation entre le délit d'usurpation d'identité et d'autres qualifications pénales telles que la diffamation.

236. La diffamation et l'usurpation d'identité, deux fondements différents. Si les délits d'usurpation d'identité et de diffamation se recoupent dans leur volonté de protéger l'honneur et la considération de la victime, la matérialité de ces deux incriminations est toutefois différente. Le délit d'usurpation d'identité numérique n'élève pas au rang d'élément matériel l'atteinte à la réputation de la victime mais exige seulement, au travers d'un dol spécial, que l'auteur du délit ait eu l'intention de le faire. Le délit de l'article 226-4-1 du Code pénal semblerait donc admettre la répression de ce qui relèverait d'une tentative de diffamation, chose que la loi de 1881 ne prend pas en considération[712]. La jurisprudence est venue confirmer cette analyse en affirmant que « *concernant le trouble à la tranquillité, à l'atteinte à l'honneur et à la considération, il convient de rappeler qu'au regard des dispositions de l'article 226-4-1 du Code pénal, les faits visés doivent être commis en vue de commettre un tel trouble ou une atteinte, l'intention suffisant dès lors seule à caractériser l'infraction* »[713]. Suivant ce constat, les magistrats amenés à statuer sur le délit d'usurpation d'identité numérique ne prêtent pas particulièrement attention au fait que les propos incriminés constituent effectivement une diffamation. Les juges déduisent le plus souvent l'atteinte de la matérialité des faits : « *la matérialité des faits n'est pas contestée par les deux prévenus, qui ont non seulement usurpé l'identité de FZ, mais ont aussi mis en ligne des photographies de celui-ci et de VP, le tout accompagné de termes vulgaires en vue de troubler leur tranquillité et de leur nuire* »[714]. Il en résulte que le délit d'usurpation d'identité numérique bien que voulant protéger une atteinte à l'honneur ou à la considération n'épouse pas les spécificités

[711] J. FRANCILLON, « Piratage informatique. Usurpation d'identité numérique. L'affaire du "faux site officiel" de Rachia Dati : une étape dans la lutte contre la cyberdélinquance », *RSC*, janvier-mars 2015, p. 105.
[712] I. SOSKIN, « Les nouvelles formes d'atteintes à la "réputation" et à "l'image" de la personne dans l'environnement numérique », *Légipresse*, n° 336, mars 2016, p. 146.
[713] TGI Paris, 13ème ch. corr., 18 décembre 2014, n° 12010064012 : *RLDI*, 2015, n° 111, Obs. J. de ROMANET ; *RSC*, janvier-mars 2015, p. 101, chron. J. FRANCILLON.
[714] TGI Paris, 17ème ch. corr., 28 mai 2015 : *Légipresse* n° 336, mars 2016, p. 146, chron. I. SOSKIN.

procédurales du droit de la presse[715]. En conséquence, les victimes d'une diffamation pourront faire le choix de poursuites sous le fondement d'une usurpation d'identité numérique dans l'hypothèse où les éléments constitutifs de ce dernier délit seraient également réunis. Cela lui permettrait de bénéficier de conditions procédurales plus souples. Cette situation ne doit cependant pas permettre de sanctionner des propos par le biais du délit de l'article 226-4-1 du Code pénal, auquel cas, le juge pourrait appliquer la loi sur la liberté de la presse. Ainsi, pour engager des poursuites sur le fondement de l'article 226-4-1 du Code pénal, le comportement d'usurpation d'identité doit être avéré et constituer le fondement de la répression[716]. Au final, si les délits d'usurpation d'identité et de diffamation peuvent être invoqués de manière concurrentes car les deux révèlent une atteinte à la réputation de la victime, leurs finalités sont cependant différentes. Le délit de l'article 226-4-1 du Code pénal instaure une protection spécifique de l'identité, l'atteinte à la réputation de la victime n'étant que la conséquence voire l'intention cachée du comportement d'usurpation. Il ne s'agit donc pas de sanctionner la parole mais le comportement d'usurpation dans son entier. Le délit d'usurpation d'identité protège donc au final davantage la personnalité numérique que la réputation numérique.

237. Conclusion de la Section 2. Le délit de l'article 226-4-1 du Code pénal a réalisé un apport nécessaire au Code pénal. Désormais, l'identité bénéficie d'une protection autonome du droit pénal. La répression des comportements lui portant atteinte ne se fait alors plus au travers d'autres infractions non spécifiques et souvent incomplètes. L'identité est désormais reconnue au niveau pénal comme un élément à part entière de la personnalité, défendue au titre du droit au respect de la vie privée. De plus, cette nouvelle infraction propose une définition qui appréhende de façon englobante l'identité des individus y compris ces manifestations contemporaines dans le domaine numérique. Ainsi, l'identité numérique est protégée au travers des identités « *déclaratives* » et « *agissantes* » des individus et donc sous l'ensemble du prisme permis par les sites de réseaux sociaux. Il est toutefois nécessaire que cette notion soit circonscrite dans une définition précise pour qu'elle ne s'affranchisse pas des exigences du principe de légalité. À ce titre, l'usurpation d'identité implique la réunion de

[715] Principe rappelé par le jugement du TGI Paris, 17ème ch. corr., ordonnance de référé, 4 avril 2013. En l'espèce, la société Twitter invoquait l'irrégularité de la procédure « *en ce que l'action, qui viserait à faire sanctionner un fait portant atteinte à l'honneur et à la réputation de Mathieu S., ne respect(ait) pas les dispositions impératives de l'article 53 de la loi du 29 juillet 1881 et (était) donc nulle ; mais attendu que l'examen des demandes formulées dans l'assignation démontre que celles-ci ne visent pas à faire cesser des propos injurieux ou diffamatoires, mais le fait qu'une personne, non identifiée usurpe l'identité de Mathieu S. sur Twitter, peu important le contenu des propos qu'il tient en son nom* ». V. I. SOSKIN, « Les nouvelles formes d'atteintes à la "réputation" et à "l'image" de la personne dans l'environnement numérique », *op. cit.*, p. 146.

[716] I. SOSKIN, « Les nouvelles formes d'atteintes à la "réputation" et à "l'image" de la personne dans l'environnement numérique », *op. cit.*, p. 146.

deux principaux critères : premièrement, l'usage du nom de la victime et deuxièmmement, une confusion dans l'esprit du public. L'exigence du dol spécial permet pour sa part d'encadrer un peu plus le champ d'application de ce délit sans pour autant remettre en cause la *ratio legis* de ce présent délit qui vise à protéger avant tout la vie privée des individus contre les formes d'atteintes à leur identité.

Conclusion du Chapitre 1

238. Le développement des réseaux sociaux en ligne a fait émerger la notion d'identité numérique sociale qui est venue étendre de manière considérable la représentation numérique de l'individu au point d'en faire une représentation d'égale importance à son identité réelle. L'identité à l'ère numérique est aujourd'hui le fruit d'une multitude de facteurs issus de l'activité de l'individu lui-même mais également de l'action d'autres personnes. C'est précisément ce dernier point qui a révélé une insuffisance de la protection offerte par le droit pénal. Ce dernier se devait donc d'adapter son système répressif afin de combler cette carence structurelle qui traduit en réalité une évolution profonde des formes de représentation de l'individu et partant, de son identité. Les sites de réseaux sociaux ont ainsi eu un impact sociétal suffisamment important pour justifier l'adoption d'une nouvelle incrimination qui ne peut être assimilée à une simple politique répressive adoptée en réaction à quelques faits divers. Le délit prévu à l'article 226-4-1 du Code pénal reconnaît une nouvelle dimension à l'identité individuelle en étendant la protection pénale à l'identité numérique des individus. Mais surtout, cette nouvelle incrimination fait de l'usurpation d'identité une forme d'atteinte à la vie privée des individus permettant dès lors une répression pénale complète des diverses formes d'atteintes à l'identité y compris celles rencontrées dans le domaine numérique.

Chapitre 2 – L'extension pénale de la protection de l'intimité

239. La divulgation de l'intimité sur les réseaux sociaux. Les sites de réseaux sociaux font partie des catalyseurs les plus efficients du phénomène de mise en visibilité de soi. Ce désir « *d'extimité* » décrit par Monsieur Serge Tisseron[717] favorise l'exposition d'éléments de la personnalité particulièrement variés. Ces sites enregistrent ainsi certaines caractéristiques stables et durables de l'individu mais aussi, des informations plus diffuses, mouvantes et multiples révélées par l'activité sociale de partage[718]. En l'occurrence, la divulgation d'informations personnelles est dans son ensemble le fait de l'individu lui-même, cependant ce dernier peut également devenir victime d'une divulgation non consentie d'informations représentant son intimité sur les sites de réseaux sociaux. Au *summum* de cette atteinte se trouve la pratique du *revenge porn* appelée également vengeance pornographique qui consiste dans le fait de publier à l'insu de la personne des photos la représentant dans son intimité sexuelle. Cette divulgation est souvent le fait d'un(e) ex-conjoint(e) ou partenaire ou amant(e).

240. L'évolution de la protection pénale de l'intimité. Si le droit pénal ne s'occupe *a priori* pas du désir d' « *extimité* » des individus sur les réseaux sociaux en ligne, il redevient légitime à intervenir lorsque la mise en avant de soi concerne des images à caractère sexuel et davantage lorsque la diffusion de telles images n'est pas consentie. Cependant, la protection pénale préexistante de l'intimité de la vie privée prévue aux articles 226-1 et 226-2 du Code pénal ne permettait pas de sanctionner la seule diffusion non consentie de l'intimité. Cette carence révélée par une combinaison stricte de ces deux textes a alors poussé le législateur à adapter le droit pénal par la création d'un nouveau délit sanctionnant de manière autonome la diffusion non consentie de l'intimité. Ce nouveau délit motivé par certains comportements déviants rencontrés sur les sites de réseaux sociaux consacre en réalité une évolution profonde dans la protection pénale de la vie privée. Ainsi, les carences de la protection préexistante de l'intimité (**Section 1**) ont justifié une extension de la protection de l'intimité (**Section 2**).

---

[717] S. TISSERON, *L'intimité surexposée*, Hachette littérature, 2001, p. 52. V. *supra* n° 20.

[718] D. CARDON, « Le design de la visibilité. Un essai de cartographie du web 2.0 », *Réseaux*, vol. 26, n° 152,2008, p. 99.

Section 1 : Les carences de la protection préexistante de l'intimité

241. La protection pénale de l'intimité. La loi n° 70-643 du 17 juillet 1970[719] est venue consacrer une protection pénale de la vie privée. Cette protection a ensuite été reprise aux articles 226-1 et suivants du Code pénal de 1994. L'article 226-1 vient précisément sanctionner le fait de porter atteinte à « *l'intimité de la vie privée d'autrui* » contre les atteintes qui lui sont portées au moyen de procédés acoustiques et optiques. L'article 226-2 constitue quant à lui un délit de conséquence venant protéger la vie privée contre la divulgation des actes réprimés à l'article précédent. La *ratio legis* de ces incriminations vient spécifiquement protéger « *l'intimité de la vie privée* » de la personne. Cependant, à l'origine, les incriminations venaient davantage sanctionner une captation non consentie d'un moment d'intimité plutôt que la diffusion non consentie d'un tel moment. La large capacité de diffusion offerte par les sites de réseaux sociaux est alors venue mettre en exergue les limites des incriminations préexistantes. Le droit pénal a ainsi révélé de véritables carences dans son dispositif traditionnel de protection de la vie privée (**§1**) pouvant néanmoins être prise en compte de manière incidente par d'autres incriminations (**§2**).

§1. Les carences du dispositif traditionnel de protection de la vie privée

242. Les limites de la protection offerte par les articles 226-1 et 226-2 du Code pénal. Avant l'entrée en vigueur du délit de l'article 226-2-1 du Code pénal, la protection pénale de l'intimité de la personne résultait des articles 226-1 et 226-2 du Code pénal. Le premier texte vient incriminer une atteinte primaire à l'intimité de la vie privée résultant de l'appropriation de l'image ou de la parole intime d'autrui sans son consentement. À l'inverse, la deuxième incrimination vient davantage appréhender une atteinte dérivée à l'intimité de la privée issue de la diffusion de l'image intime de la personne. Ces textes se sont montrés toutefois inadaptés aux nouvelles pratiques issues des sites de réseaux sociaux consistant à divulguer l'intimité sexuelle de personnes sans leur consentement. Cette inadaptation résulte du système de renvoi opéré par ces deux textes d'infraction. La rédaction de ces textes fait de l'atteinte primaire à la vie privée un élément préalable à la constitution du délit de l'article 226-2 du Code pénal. En conséquence, la diffusion d'une image de l'intimité d'autrui ne peut être sanctionnée que lorsqu'elle constitue au préalable le délit prévu à l'article 226-1 du Code

[719] L. n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, *JORF* 19 juillet 1970, p. 6751.

pénal. La répression concerne alors les seuls cas où l'image aurait été saisie initialement sans le consentement de la personne, restreignant considérablement le champ d'application de ces incriminations.

Les limites de ces incriminations proviennent du système de renvoie opéré entre l'article 226-1 et l'article 226-2 du Code pénal, ainsi, l'exigence initiale d'une captation non consentie de l'intimité de la personne (A) aboutit à une protection insuffisante de la diffusion de son intimité (B).

A. Initialement, une captation non consentie de l'intimité de la personne

243. L'atteinte primaire à l'intimité de la vie privée. L'article 226-1 du Code pénal incrimine « *le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui* ». Ce texte définit l'atteinte primaire à l'intimité de la vie privée et constitue l'élément préalable de l'incrimination de l'article 226-2. Cette atteinte sanctionne en l'occurrence l'appropriation non consentie (2) de l'intimité de la victime (1).

1) Une appropriation de l'intimité de la victime

244. Les moyens d'atteinte à l'intimité. L'atteinte primaire à l'intimité de la vie privée se déduit de la réalisation des moyens décrits au sein du texte d'infraction. Ainsi, l'article 226-1 du Code pénal prévoit deux procédés permettant de déduire une atteinte à l'intimité. Premièrement, l'atteinte à l'intimité de la vie privée peut résulter d'une appropriation de l'image d'autrui se trouvant dans un lieu privé (a). Deuxièmement, une telle atteinte s'observe suite à une appropriation de la parole d'autrui prononcée à titre privé ou confidentiel (b).

a- Une appropriation de l'image d'autrui se trouvant dans un lieu privé

245. L'image d'autrui. L'image fait référence à l'apparence visible d'un individu, à son aspect physique et constitue pour la personne, une partie de sa personnalité[720]. La lecture de l'article 226-1 du Code pénal impose de ne prendre en considération que « *l'image d'une personne* ». En conséquence, la protection pénale de l'image ne prend pas en compte la représentation d'un animal ou d'une chose, seule l'image de la personne est visée par la loi[721].

[720] Association H. CAPITANT, *Vocabulaire juridique*, G. CORNU (dir.), PUF, 12ème éd., 2018, *V°* Image.
[721] Cette condition stricte ne permet pas d'envisager toutes les situations pouvant menacer la vie privée d'une personne. La présence d'un animal sur une photographie peut par exemple révéler un état de solitude de son

De même, la seule reproduction graphique d'une scène d'intimité échappe à l'incrimination en ce qu'elle n'utilise pas l'un des moyens énoncés à savoir, une fixation, un enregistrement ou une transmission de l'image. Seules les images purement représentatives de la réalité à savoir la photographie ou la vidéo d'une personne sont visées par l'article 226-1 2° du Code pénal.

246. La prise en compte spécifique de l'image truquée. La deuxième Section du Chapitre du Code pénal consacrée aux atteintes à la personnalité[722] prend en considération le montage réalisé à partir de l'image d'une personne. L'article 226-8 du Code pénal dispose : « *Est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec des paroles ou l'image d'une personne sans son consentement s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en a pas expressément fait mention* ». Deux conditions transparaissent du texte d'infraction : d'une part qu'il y ait un montage et d'autre part qu'il n'apparaisse pas à l'évidence qu'il s'agit d'un montage. La doctrine a donné de multiples définitions au mot montage. On peut le définir ainsi comme « *la manipulation ou le truquage d'un ou plusieurs films, photographies ou enregistrements* »[723], ou encore comme la « *manipulation d'images ou de sons, tout truquage ayant pour but de présenter au public une idée mensongère ou dénaturée de ce qui a été dit, fait ou vu en réalité* »[724] ou plus généralement comme un « *truquage photographique* »[725]. Cette infraction qui n'est pas fréquemment utilisée par le juge pénal[726] peut cependant trouver un regain d'utilité avec le développement des technologies de l'information et de la communication. De nouvelles applications pour smartphone[727] permettent en effet de réaliser soi-même des trucages photos. Certains truquages réalisés sans le consentement de la personne et publiés à

---

propriétaire, de même l'image d'une maison peut dévoiler l'adresse de son occupant ou sa situation sociale. I. LOLIES, *La protection pénale de la vie privée*, PUF Aix-Marseille, 1999, p. 105.

[722] C. pén., Livre deuxième, Titre 2, chapitre 6 « *des atteintes à la personnalité* ».

[723] J. PRADEL, « Les dispositions de la loi du 17 juillet 1970 sur la protection de la vie privée », *D.* 1971, chron. p. 115.

[724] R. MERLE et A. VITU, *Traité de droit criminel, Droit pénal spécial*, Cujas, 1982, p. 1652, n° 2034.

[725] R. LINDON, « Les dispositions de la loi du 17 juillet 1970 relative à la protection de la vie privée », *JCP* G 1970, I, 2357, n° 19.

[726] Hervé PELLETIER rappelle que l'une des rares décisions pénales en matière de montage avait été rendue, sous l'empire de l'ancien article 370 : Toulouse, 26 février 1974 : *JCP* G 1975, II, 17903, note R. LINDON ; *D.* 1974, jurispr. p. 736 ; *RSC* 1976, p. 119, obs. G. LEVASSEUR. En l'occurrence, la photographie d'un couple de personnes avait été utilisée pour illustrer l'affiche électorale d'un parti politique. Selon la chambre d'accusation, le montage ne constituait pas nécessairement une manipulation ou un truquage de la photographie mais était toutefois réalisé dès lors que l'insertion de cette photographie dans un contexte d'images, de dessins ou de légendes, en modifiait la valeur artistique, la portée ou la signification. Le montage était démontré dès lors que la présentation et la typographie de l'affiche avaient modifié sa signification authentique qui était celle de deux promeneurs et avaient fait d'eux, au moyen de la légende, l'image type d'un couple de jeunes français recherchant un logement. V. H. PELLETIER, « Atteinte à la représentation de la personne », *J.-Cl.* Pénal Code, fasc. 20, septembre 2016, n° 10.

[727] Par exemple les applications *Face It*, *Warp my face* ou encore *Ifun face*.

son insu sur des sites de réseaux sociaux pourraient alors revêtir cette qualification pénale à défaut d'entrer dans le champ qualificatif de l'article 226-1 2° du Code pénal.

247. Un procédé quelconque. Selon l'article 226-1 2° du Code pénal, l'appropriation de l'image d'autrui peut se réaliser au moyen de plusieurs procédés que ce soit une fixation, un enregistrement ou une transmission de l'image d'une personne. La fixation de l'image peut s'interpréter comme le fait de figer de façon instantanée la représentation d'une personne. De plus, l'atteinte ne peut résulter que d'un « *procédé* », ce qui suppose l'utilisation d'un moyen technologique pour fixer l'image[728]. Le simple regard indiscret porté sur autrui ne peut, en soi, constituer une infraction. Plus généralement, le danger apparaît dès lors que la trace d'un instant d'intimité volé peut être conservée[729]. L'infraction prévoit par ailleurs dans son champ d'application, non seulement la fixation mais aussi l'enregistrement de l'image d'autrui. Cette occurrence permet de rattacher au champ d'application de l'article 226-1 du Code pénal la vidéo prise d'une personne. Le droit pénal protège en conséquence autant la représentation mobile d'une personne que la photographie statique de celle-ci. Enfin, le procédé peut également résulter de la transmission de l'image supposant l'utilisation d'un procédé d'espionnage à distance[730].

248. Exigence d'un lieu privé. L'article 226-1 2° du Code pénal précise que l'appropriation de l'image d'autrui doit être effectuée dans des circonstances particulières pour faire l'objet de la protection pénale. L'atteinte à la vie privée implique nécessairement que l'image de la personne résulte d'un lieu privé. Par opposition, la protection pénale de l'image ne s'appliquerait pas aux lieux publics tels que les parcs ou voiries. Le domicile apparaît alors comme l'exemple le plus évident de lieu privé[731]. Sur le sujet, la doctrine se divise en deux points de vue. Selon une conception subjective, le critère de définition du lieu privé serait le consentement de la personne. Ce dernier distinguerait donc si la personne se trouve dans un lieu public ou un lieu privé. Sous cet angle d'analyse, le lieu privé se définit comme comme « *tout endroit clos, inaccessible aux regards de l'extérieur et où l'entrée dépend de l'autorisation donnée de celui-là seul qui a la propriété, l'utilisation ou la jouissance, à un cercle limité* »[732]. Dans une formulation plus générale le Professeur Jacques Ravanas considère qu'un lieu est privé « *dès lors que son accès dépend du consentement de*

[728] I. LOLIES, *La protection pénale de la vie privée*, *op. cit.*, p. 104.
[729] E. DREYER, *Droit pénal spécial*, Ellipses, 3ème éd., 2016, p. 208, n° 433.
[730] *Ibid.*
[731] R. BADINTER, « La protection de la vie privée contre l'écoute électronique clandestine », *JCP*, 1971, I, octobre n° 2435, § 19.
[732] D. BÉCOURT, « réflexion sur le projet de loi relatif à la vie privée », *Gaz. Pal.* 1970, I, octobre, p. 202.

celui qui l'occupe »[733]. La nécessité d'un lieu clos pour conceptualiser la notion de lieu privé, n'est plus mentionnée ; la seule exigence serait ici l'accès par le consentement de l'intéressé. La conception objective est quant à elle plus restrictive. Elle définit le lieu privé par opposition à la liste de lieux publics énumérés par la loi tels que les rues, parcs, stades[734]. Cette divergence doctrinale se retrouve dans l'interprétation du juge de l'article 226-1 2° du Code pénal. Dans une décision du 16 octobre 1973 le tribunal correctionnel d'Aix-en-Provence a adopté une conception objective du lieu privé en se référant à la simple énumération de lieux publics par nature. En l'espèce, les juges ont considéré qu'il manquait un élément constitutif du délit de l'ancien article 368 du Code pénal, en observant que la photographie litigieuse avait été prise dans la rue devant l'immeuble où la personne habitait et qu'il n'y avait pas violation de l'intimité de la vie privée du fait que l'image résultait d'un lieu public par nature[735]. Cependant, force est de constater que la jurisprudence dominante privilégie la conception subjective s'adonnant par là même à une interprétation plus large de la loi[736]. La Cour de cassation est venue asseoir l'interprétation subjective en érigeant le critère du consentement comme élément de distinction entre lieu privé et lieu public. Ainsi le juge de cassation désigne un lieu privé comme « *un endroit qui n'est ouvert à personne, sauf autorisation de celui qui l'occupe* »[737].

b- Une appropriation de la parole d'autrui prononcée à titre privé ou confidentiel

249. La notion de parole. Par le terme parole il faut comprendre l'expression d'un langage articulé émanant d'une personne humaine, qu'il soit verbal ou gestuel[738]. En conséquence la

[733] J. RAVANAS, *La protection des personnes contre la réalisation et la publication de leur image,* coll. Solus, LGDJ, 1978, p. 514.
[734] « *L'espace public est constitué traditionnellement des voies publiques ainsi que des lieux ouverts au public ou affectés à un service public* ». L. n° 2010-1192 du 11 octobre 2010 interdisant la dissimulation du visage dans l'espace public, *JORF* n° 0237, 12 octobre 2010, p. 18344, texte n° 1, Art. 2, al. 1.
[735] TC Aix-en Provence, 16 octobre 1973 : *JCP*, 1974, II, n° 17623, note R. LINDON ; *RSC* 1976, obs. G. LEVASSEUR, p. 119.
[736] Par exemple les juges du fond ont suivi cette conception à propos d'une photographie d'une femme aux seins dénudés se trouvant sur une plage. Le délit n'était en l'occurrence pas constitué aux motifs que « *le lieu était accessible à tous les estivants* », les juges ont également pris en compte un faisceau d'indices tel que le nombre de personne pratiquant le nudisme et si les pratiquants se souciaient du regard d'autrui. Le tribunal a donc réalisé une appréciation *in concreto* pour évaluer la nature du lieu et non une simple appréciation au regard d'une liste énumérative de lieux classés publics. TC Paris, 18 mars 1971 : *D.*, 1971, J. p. 447, note J. FOULON PIGANIOL ; *Gaz. Pal.*, 1972, I, 59, note P. FREMOND ; *JCP*, 19712, II, 16875 ; *RSC* 1972, p. 118, n° 6.
[737] Crim., 28 novembre 2006, n° 06-81.200 : *CCE* n° 3, Mars 2007, comm. 45, A. LEPAGE.
[738] R. MERLE et A. VITU, *Traité de droit criminel, Droit pénal spécial*, Cujas, 1982, p. 1648, n° 2031.

protection ne porte pas sur la voix mais davantage sur la teneur des propos tenus, peu importe la langue utilisée, il suffit que le message soit compréhensible[739].

250. Une appropriation mécanique de la parole. L'appropriation se réalise par la captation, l'enregistrement ou la transmission de la parole d'autrui au moyen d' « *un procédé quelconque* ». L'article 226-15 du Code pénal venant incriminer de manière spécifique l'interception de conversations téléphoniques, le champ d'application de cette infraction à portée générale concerne alors l'appropriation de la parole d'autrui par tout procédé d'espionnage autre que la captation illicite d'une conversation téléphonique[740].

251. Des propos prononcés à titre privé ou confidentiel. Enfin, les paroles appréhendées doivent avoir été prononcées « *à titre privé ou confidentiel* ». En conséquence, toutes les paroles prononcées dans un lieu privé semblent concernées par le texte, mais également les paroles prononcées dans des lieux publics ou ouverts au public[741]. La protection de la parole est alors plus étendue que la protection de l'image restreinte au seul lieu privé. Cependant, l'appropriation de l'image ou de la parole d'autrui dans un lieu privé ne suffit pas à démontrer l'atteinte pénale, il est également nécessaire de rapporter l'absence de consentement de la victime.

2) Une appropriation non consentie

252. L'absence de consentement de la victime, élément constitutif de l'infraction. L'article 226-1 érige en élément légal de l'infraction l'absence de consentement de la victime. L'infraction suppose alors qu'il y ait eu fixation de l'image d'autrui dans un lieu privé sans son consentement. En outre, le dernier alinéa de l'article 226-1 du Code pénal prévoit que lorsque l'enregistrement des paroles ou des images est effectué avec l'accord de la personne concernée, l'acte perd son caractère délictueux. Cet alinéa pose une présomption d'accord de la victime lorsque les actes sont accomplis « *au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire* ». Cette présomption est *de facto* écartée lorsque le moyen de fixation de l'image était dissimulé[742].

[739] E. DREYER, *Droit pénal spécial*, *op. cit.*, p. 210, n° 435.
[740] Paris, 19 mars 2002, n° 00/02830 : *JCP* G 2002, IV, 2620.
[741] E. DREYER, *Droit pénal spécial*, *op. cit.*, p. 211, n° 437.
[742] Paris, 24 avril 2007 : *CCE* 2007, n° 156, obs. A. LEPAGE.

B. Une protection insuffisante de la diffusion de l'intimité d'autrui

253. L'atteinte dérivée à l'intimité de la vie privée. L'article 226-2 du Code pénal incrimine : « *le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus à l'article 226-1* ». Ainsi, tant la conservation[743] que la diffusion d'une atteinte primaire à l'intimité de la vie privée constituent un acte pénalement répréhensible. De plus, en sanctionnant le fait « *de porter à la connaissance du public ou d'un tiers* » le produit de l'infraction de l'article 226-1 du Code pénal, la présente incrimination permet d'entendre de manière large la notion de diffusion. L'absence de toute référence à l'utilisation d'un moyen technique ou le fait que la seule prise de connaissance par un tiers suffise à caractériser l'infraction, indique que le champ d'application de celle-ci dépasse largement la notion de publication au sens de la loi sur la liberté de la presse du 29 juillet 1881[744]. Cependant, le champ d'application de l'infraction est considérablement restreint par son lien indissociable avec l'infraction prévue à l'article 226-1 du Code pénal. Ce renvoie empêche l'incrimination de l'article 226-2 de venir sanctionner de manière autonome la diffusion non consentie de l'intimité d'une personne. Le consentement initial de la victime constitue dès lors une limite à la protection pénale de la diffusion de l'image intime (1), cette limite étant confirmée par le principe d'interprétation stricte de la loi pénale (2).

1) Le consentement initial de la victime, limite à la protection pénale de la diffusion de l'image

254. Une répression cantonnée à une prise d'image initiale non consentie. Avec l'instauration en 1992 du nouveau Code pénal, le terme « *actes* » a été substitué à celui de « *faits* » dans le texte d'infraction de l'article 226-2. Il est donc désormais clair que l'article 226-2 renvoie à l'ensemble des actes énoncés à l'article 226-1 et non plus à l'ensemble des faits, ce qui a pour conséquence que le renvoi ne concerne plus seulement les faits matériels énoncés à l'article 226-1 du Code pénal, mais l'incrimination dans son ensemble. Dans ce cas, le délit de l'article 226-2 du Code pénal vient sanctionner la diffusion d'une image prise en violation de l'intimité de la vie privée et se heurte à un problème de renvoi : l'existence de

[743] En prévoyant le fait de conserver le législateur a érigé en infraction autonome un acte qui aurait pu relever d'un simple recel. La conservation doit néanmoins être entendue moins comme la conséquence des actes décrits à l'article 226-1 que comme le préalable de ceux qui suivent. Elle peut alors s'interpréter comme un acte préparatoire érigé en infraction obstacle. E. DREYER, *Droit pénal spécial*, *op. cit.*, p. 214, n° 447.
[744] V. s*upra* n° 50 et suiv.

l'infraction de l'article 226-2 se trouve subordonnée à la condition que le délit de l'article 226-1 du Code pénal soit préalablement constitué[745]. Ainsi, ne sont visés que les cas de la diffusion d'une image prise sans le consentement de la personne. C'est le cas par exemple des publications de photographies d'une personne non consentante à travers la fenêtre fermée de son appartement depuis l'extérieur[746], mais aussi de la communication à des tiers d'une vidéocassette mettant en scène les ébats amoureux du prévenu avec une personne non consentante[747] ou encore de la diffusion sur internet des photographies d'une personne, à l'insu de celle-ci, la représentant dans un lieu privé et dans son intimité[748]. Il est cependant évident qu'une personne puisse donner son consentement à être prise en photo sans pour autant accepter la publication de ce document. Les articles 226-1 et 226-2 du Code pénal se contentent de protéger contre l'espionnage mais sont indifférents à la publication non consentie de l'image d'une personne prise dans son intimité. L'individu ne peut invoquer ni l'article 226-1 du fait de son consentement initial à la prise de l'image, ni l'article 226-2 du fait de la licéité de la prise d'image initiale. La diffusion de l'image n'est donc pas en soi, dans cette hypothèse, un moyen d'atteinte à la vie privée.

255. Une répression circonscrite à une prise initiale d'image dans un lieu privé. Le mécanisme de renvoi de l'article 226-2 du Code pénal impose non seulement l'absence de consentement de la victime dans la prise d'image initiale mais également que la représentation de la victime résulte d'un lieu privé. Cette condition sera souvent remplie compte tenu du fait que les images intimes sont, dans la grande majorité des cas, captées dans un cercle privé. Il n'est cependant pas impossible que les photographies ou enregistrements compromettants aient été captés dans des lieux publics[749]. Plus généralement, un lieu privé étant défini comme « *un endroit qui n'est ouvert à personne, sauf autorisation de celui qui l'occupe* »[750], tout endroit ouvert est *de facto* exclu du champ d'application de l'article 226-1 du Code pénal. Toute image issue d'un espace naturel est en conséquence insusceptible de bénéficier d'une protection pénale. L'élément constitutif du lieu privé cantonne l'intimité à un espace fermé,

[745] I. LOLIES, *La protection pénale de la vie privée*, *op. cit.*, p. 115.
[746] Crim., 25 avril 1989 : *Bull. crim.* n° 165 ; *RSC* 1990, 78, obs. G. LEVASSEUR.
[747] Paris, ch. corr. 11, 23 juin 2004, n° 04/00485.
[748] Paris, ch. corr. 11, 22 mars 2005, n° 04/06467.
[749] Un homme a par exemple été poursuivi pour avoir publié sur le réseau social Facebook une vidéo de son ex-femme lui pratiquant une fellation dans un bar. L'individu a cependant été relaxé au motif que les éléments constitutifs du délit d'atteinte à l'intimité de la vie privée par la captation, l'enregistrement ou la transmission de l'image d'une personne se trouvant dans un lieu privé sans son consentement n'était pas réunis.
<http://www.leprogres.fr/jura/2013/06/08/doubs-il-balance-une-video-porno-de-son-ex-sur-facebook> (dernière consultation le 9 octobre 2019).
[750] Crim., 28 novembre 2006, n° 06-81.200 : *CCE* n° 3, mars 2007, comm. 45, A. LEPAGE.

cela peut paraître réducteur dans la mesure où des scènes relevant de l'intimité peuvent également se retrouver en dehors d'espaces clos.

256. Une incohérence relevée très tôt. Cette incohérence dans la voie répressive n'a pas manqué d'être soulevée dès les débats devant l'Assemblée nationale sur la loi de 1970 portant réforme de la vie privée[751]. Les députés Grailly, Mazeaud et Bozzi présentèrent un amendement (n° 77) qui proposait d'ajouter à l'article 369[752] un nouvel alinéa : « *Sera puni des mêmes peines quiconque aura utilisé à des fins lucratives directes ou indirectes, l'image ou l'enregistrement des paroles d'une personne sans son consentement* »[753]. Cette rédaction permettrait de réprimer à la fois l'utilisation d'images obtenues en violation de l'article 226-1 du Code pénal mais également l'utilisation d'images prises à l'origine régulièrement. Plus généralement, cette solution ne cantonnerait plus l'article 226-2 à un simple délit de conséquence mais en ferait une infraction autonome, du moins pour partie. La présence de la condition préalable est vivement critiquée par la doctrine, selon Georges Levasseur il est « *regrettable que l'article 369 sur la publication et la divulgation ne soit pas applicable lorsque le document n'a pas été obtenu dans les conditions incriminées par l'article 368 du Code pénal. Il est fâcheux que la personne qui a donné son consentement à son établissement n'impliquait pas le consentement à sa publication* »[754]. Dans le même sens, le Professeur Jacques Ravanas, expose que « *le délit n'est pas réalisé si l'image a été fixée avec le consentement du modèle. Cette conséquence à laquelle il est difficile d'échapper est cependant critiquable* […] *elle conduit à penser que le consentement à la captation d'une scène intime emporte le consentement à la divulgation* […] *la victime ne pourra pas obtenir gain de cause devant le Tribunal correctionnel, le délit de l'article 368 n'étant pas constitué* »[755].

2) Une limite confirmée par le principe d'interprétation stricte de la loi pénale

257. Une nécessaire interprétation stricte de la loi pénale. Les juges ont dans un premier temps choisi d'opérer une interprétation souple de la loi pénale de manière à sanctionner les vengeances pornographiques diffusées sur les sites de réseaux sociaux (a). Cependant, dans

[751] L. n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, *JORF*, 19 juillet 1970, p. 6751.
[752] C. pén., ancien art. 226-2.
[753] I. LOLIES, *La protection pénale de la vie privée*, *op. cit.*, p. 117.
[754] G. LEVASSEUR, *La protection pénale de la vie privée*, *in* Études offertes à Pierre Kayser, Aix-en-Provence, PUF d'Aix-Marseille, 1979, tome 2, p. 127.
[755] J. RAVANAS, *La protection des personnes contre la réalisation et la publication de leur image*, coll. Solus, LGDJ, 1978, p. 527.

un second temps, la Cour de cassation est venue rappeler la nécessaire interprétation stricte de la loi pénale faisant alors obstacle à d'éventuelles poursuites sur ce fondement (b).

a- Une tentative d'interprétation souple de la loi pénale

258. La condamnation sur le fondement de l'article 226-1 du Code pénal. Bien que la rédaction des infractions des articles 226-1 et 226-2 démontre une carence dans la prise en compte du consentement de la victime à la diffusion de son image, le juge n'hésite pas à prendre ce consentement en considération dans les motifs de sa décision. La Cour d'appel de Toulouse dans son arrêt du 27 février 2012[756] a ainsi confirmé le jugement de première instance qui avait condamné le prévenu, du chef d'utilisation d'un document ou d'un enregistrement obtenu par une atteinte à la vie privée. Le prévenu avait diffusé sur deux profils Facebook des photos à caractère pornographique de la partie civile, prises dans un lieu privé et à sa seule intention dans le cadre d'une relation amoureuse. Cependant, le juge ne s'est pas contenté de rapporter l'ensemble des éléments constitutifs du délit, y compris l'absence de consentement initial de la partie civile. Ce dernier a également constaté dans ses motifs les menaces de diffusion des photos par le prévenu, ainsi que l'absence d'autorisation univoque de la victime de voir ses images mises en ligne. La motivation de l'arrêt dépasse la simple qualification des éléments constitutifs de l'infraction de l'article 226-2 du Code pénal. Cela démontre une volonté de prendre en considération le consentement de la victime à la diffusion de son image et donc de dépasser le seul consentement initial. La présence de ce type d'argumentation dans la motivation d'arrêts ne permet pas pour autant de conclure à un changement de structure de l'infraction, cela ne relevant que de la prise de position d'un magistrat ou de sa volonté d'étayer au maximum sa décision. Cependant il ressort de certaines décisions une véritable prise en compte de l'absence de consentement de la victime dans la démonstration de l'infraction.

259. Certaines juridictions du fond ont déjà conclu à des condamnations sur le fondement de l'article 226-1 du Code pénal. C'est le cas notamment de décisions de juridictions du premier degré[757] et du second degré[758]. Dans ces décisions, les juges ont retenu la

[756] Toulouse, Ch. appl. corr. 3, 27 février 2012, Jurisdata n° 2012-012168.

[757] Par exemple : TC Metz, 3 avril 2014, n° 812/2014. Dans la présente décision le juge a prononcé une peine de douze mois d'emprisonnement assortis d'un sursis avec mise à l'épreuve à l'encontre d'un individu qui avait publié des photos de son ex-compagne dénudée ou pratiquant un acte sexuel sur la page Facebook du lycée dans lequel elle enseignait. V. aussi TC Metz, jugement du 8 septembre 2015, n° 1654/2015. Dans la présente décision le juge a prononcé un an d'emprisonnement ferme à l'égard du même individu qui continuait de publier des photographies de son ex-conjointe dénudée, y compris sur des sites échangistes sous forme de faux profils d'annonce.

qualification de l'article 226-1 du Code pénal. Selon eux, le prévenu avait volontairement fixé, enregistré ou transmis, sans son consentement, l'image de la victime se trouvant dans un lieu privé. Cependant dans ces différentes hypothèses, l'absence de consentement de la victime provient non pas de la prise d'image initiale mais de la publication de ces images sur internet. Le champ d'application de l'infraction de l'article 226-1 du Code pénal viserait-il autant la captation de l'image que sa publication sans le consentement de la victime ? Les juges ont assurément adopté en l'espèce une vision extensive de cette infraction. Cette position peut être défendue en séparant d'un côté les termes « *fixé, enregistré* » et d'un autre le terme « *transmis* ». Ce dernier pourrait viser les cas de transmission au public d'images prises dans un lieu privé et portant atteinte à l'intimité de la vie privée sans le consentement de la personne. De cette interprétation naîtrait toutefois une ambiguïté : quelle serait l'utilité de l'article 226-2 du Code pénal qui vient sanctionner la *diffusion* du produit de l'infraction de l'article 226-1 ? La locution « *transmis* » doit en réalité s'interpréter comme un relais entre la captation et la réception de l'image dans l'hypothèse où l'appareil qui capte celle-ci est différent de celui qui la reçoit[759]. Par exemple, la transmission, telle qu'énoncée à l'article 226-1 du Code pénal, pourrait s'appliquer dans la situation où une personne placerait une webcam dans un lieu privé à l'insu de ses occupants et transmettrait cette image en direct sur un écran situé dans un autre lieu. *In fine*, selon une interprétation stricte, la publication d'une image postérieurement à sa captation ne peut relever de l'infraction de l'article 226-1 du Code pénal mais uniquement de l'article 226-2 du même Code. En conséquence, l'application de l'article 226-1 du Code pénal pour la répression de la publication sans le consentement de la personne d'images relevant de son intimité entre en contradiction avec la lecture stricte du texte et par là même le principe de légalité criminelle.

---

[758] Par exemple : Paris, Chambre correctionnelle 11 section A, 22 Mars 2005, Numéro JurisData : 2005-277904, résumé jurisdata : « *Constitue une atteinte à la vie privée le fait de diffuser sur un site internet des photos d'une personne la représentant dans des lieux privés et touchant à son intimité, notamment celles-là montrant au lit et dans la salle de bain. Le consentement n'avait été donné que pour une première photo, alors qu'une cinquantaine ont été ainsi accessibles aisément à tout internaute. Le fait que le prévenu ait supprimé les photographies après son audition par la police ne saurait effacer la commission de l'infraction. Il ne s'agit en effet que d'un simple repentir actif mais tardif* », *CCE* n° 11, novembre 2005, comm. 176, A. LEPAGE ; V. aussi Paris, Ch. corr. 11 section B, 23 Juin 2004, n° JurisData : 2004-258413, Résumé jurisdata : « *Doit être reconnue coupable d'atteinte à l'intimité de la vie privée d'autrui la personne qui communique à des tiers des copies d'une cassette vidéo mettant en scène les ébats amoureux du prévenu et de la victime, la communication pouvant être qualifiée de diffusion au sens du texte* ».

[759] H. PELLETIER, « Atteinte à la vie privée – enregistrement de la parole ou de l'image – fabrication, détention, location ou vente d'appareils d'enregistrement », *J.-Cl.* Pénal Code, fasc. 20, juin 2017, n° 23.

260. La condamnation sur le fondement des articles 226-1 et 226-2 du Code pénal. En outre, dans des affaires similaires[760] les juges du fond ont parfois choisi de se référer indistinctement aux articles 226-1 et 226-2 du Code pénal sans entrer dans les détails techniques de la combinaison de ces deux articles et concluant en une atteinte à la vie privée. Cette interprétation est toutefois imparfaite puisque aucun de ces deux textes ne vient prendre en compte le consentement de la victime au moment de la diffusion de son image, l'infraction de l'article 226-2 du Code pénal n'étant qu'une infraction de conséquence vis-à-vis de l'article 226-1, se bornant à réprimer la diffusion du produit de la première infraction.

261. La validation de cette interprétation par la Cour de cassation. Enfin, aussi contestables soient-elles, ces analyses ont reçu l'approbation de la Cour de cassation[761] alors même que l'auteur du pourvoi, en la personne du prévenu, soulevait la carences des textes répressifs[762]. La Cour de cassation justifie la décision de condamnation des juges du fond sans entrer dans l'analyse technique de l'interprétation des incriminations des articles 226-1 et 226-2 du Code pénal. La haute juridiction se contente de reprendre dans les solutions citées l'attendu suivant : « *Attendu que les énonciations de l'arrêt attaqué mettent la Cour de Cassation en mesure de s'assurer que la cour d'appel a, sans insuffisance ni contradiction, caractérisé en tous ses éléments, tant matériels qu'intentionnel, le délit dont elle a déclaré le prévenu coupable* »[763]. La Cour de cassation choisit de ne pas relever d'incohérence allant même affirmer que la diffusion sur internet sans le consentement de l'image d'une personne permet « *sans insuffisance, ni contradiction* » de caractériser « *en tous ses éléments matériels* » le délit de l'article 226-1 du Code pénal. Sans doute que les magistrats du quai de l'horloge ont voulu assurer la punition d'un comportement objectivement répréhensible mais

[760] Par exemple : Amiens, Ch. corr., 15 Avril 2009, n° 08/01374, résumé Jurisdata : « *Doit être condamné pour utilisation d'un document ou enregistrement obtenu par une atteinte à la vie privée d'autrui, le prévenu qui a diffusé des photos intimes de son ancienne compagne. Le prévenu et la victime se sont rencontrés via internet. Un enfant est né de leur union. Des photos intimes de la victime ont été prises avec son accord par le prévenu. Dans un contexte de séparation difficile, le prévenu a menacé de diffuser ces photos. Plusieurs personnes de l'entourage de la victime ont reçu sur leur ordinateur les photos litigieuses. Le prévenu nie vainement toute participation à la diffusion des images intimes. En effet, les photos n'ont pu être diffusées que par une personne les détenant, possédant un minimum de compétences informatiques et voulant se venger ou porter atteinte à la réputation de la victime. Le témoignage des parents de la victime et la transcription de conversations téléphoniques confirment le faisceau de présomptions et d'indices qui établissent la culpabilité du prévenu* », Dans la présente affaire la Cour a déclaré l'individu coupable « *d'utilisation d'un document ou enregistrement obtenu par une atteinte a la vie privée d'autrui, (…), infraction prévue par les articles 226-2 alinéa 1, 226-1 du code pénal et réprimée par les articles 226-2 alinéa 1, 226-1 alinéa 1, 226-31 du code pénal* ».

[761] Par exemple : Crim, 31 Octobre 2001, n° 01-80.282 – Crim, 26 Avril 2000, n° 99-85.951.

[762] Arguments du pourvoi : « *ne caractérise pas, en ses éléments matériels, le délit prévu et réprimé par l'article 226-1 du Code pénal, le fait d'avoir porté à la connaissance de tiers des photographies prises, avec le consentement des intéressés, de personnes se trouvant dans un lieu privé au moyen de la réalisation et de l'envoi de photocopies de ces photographies ; qu'en décidant le contraire, la cour d'appel a violé par fausse application les dispositions de l'article susvisé* ». Crim., 31 Octobre 2001, n° 01-80.282.

[763] Crim., 31 Octobre 2001, n° 01-80.282 – Crim., 26 Avril 2000, n° 99-85.951.

au détriment d'une de leur fonction essentielle : assurer un contrôle de légalité et en conséquence le respect du principe d'interprétation stricte de la loi pénale. Cette position jurisprudentielle n'est cependant pas devenue constante, la Cour de cassation s'étant résolue à adopter une interprétation stricte des textes.

b- Une nécessaire interprétation stricte de la loi pénale

262. La combinaison stricte des articles 226-1 et 226-2 du Code pénal. La chambre criminelle de la Cour de cassation rappelait déjà dans un arrêt du 25 avril 1989[764] la grille de lecture de ces deux infractions. La haute juridiction précisait d'une part, que constituait l'infraction prévue par l'article 368 du Code pénal (nouvel art. 226-1) le fait de photographier un tiers, sans son consentement, de l'extérieur à travers la fenêtre fermée de son appartement, d'autre part que la publication d'une telle photographie prise sans le consentement de l'intéressé, caractérisait le délit prévu par l'article 369 du même code (nouvel art. 226-2)[765]. Le délit de l'article 226-1 impose donc la démonstration de l'absence de consentement de la victime de l'atteinte à la vie privée et le délit de conséquence qui le suit exige également cette absence de consentement initial. Les juridictions du fond ont rappelé cette condition nécessaire à la qualification de ces infractions : « *les photographies conservées puis divulguées par le prévenu ont été prises avec l'accord de son ex-femme. Les faits déférés ne constituent donc pas une infraction pénale* »[766]. Cette interprétation stricte des textes par les juges du fond est d'ailleurs validée par la Cour de cassation de la manière suivante : « *Attendu que les énonciations de l'arrêt attaqué et du jugement qu'il confirme permettent à la Cour de cassation de s'assurer que la cour d'appel a, sans insuffisance ni contradiction, et en répondant aux chefs péremptoires des conclusions dont elle était saisie, exposé les motifs*

[764] Crim., 25 avril 1989, n° 86-93.632 : *Bull. crim.* 1989, n° 165 ; *RSC* 1990. 78, obs. G. LEVASSEUR.
[765] Dans les faits, un hebdomadaire très répandu avait publié un article montrant un individu derrière une fenêtre fermée de son appartement. La photographie avait été prise au téléobjectif à partir d'une position surélevée face à l'immeuble habité par la victime. V. A. LEPAGE, « Images intimes sur Internet », *CCE* n° 11, novembre 2005, comm. 176.
[766] Montpellier, Ch. corr. 3, 2 février 2006, n° Jurisdata : 2006-301727, résumé Jurisdata : « *Le prévenu est poursuivi pour avoir envoyé à l'employeur de son ex-femme des photocopies de photographies la représentant nue. Cependant, l'application des dispositions de l'article 226-2 du Code pénal sanctionnant la conservation et la diffusion d'images implique que soient réunies les conditions de l'incrimination prévues par les dispositions de l'article 226-1 du même Code qui exigent que les images soient obtenues sans le consentement de la personne photographiée. Or en l'espèce, les photographies conservées puis divulguées par le prévenu ont été prises avec l'accord de son ex-femme. Les faits déférés ne constituent donc pas une infraction pénale* ». Autre exemple, Saint-Denis (Réunion), 14 Décembre 2011 : « *l'ensemble des incriminations prévues par les articles 226-1 et suivants du code pénal témoigne de la volonté du législateur pénal de sanctionner les atteintes à l'intimité de la vie privée (…) réalisées de façon clandestine ; (…) ; (…) ; que de même, la transmission ou la divulgation au public d'une photographie à laquelle la personne avait consenti n'entre pas dans le champ d'application des articles 226-1 et 226-2 du code pénal* ».

pour lesquels elle a estimé que les faits d'atteinte à l'intimité de la vie privée (…) n'étaient pas établis, et ainsi justifié sa décision déboutant les parties civiles de leurs prétentions »[767]. Selon ces jurisprudences, la protection du consentement à la diffusion de l'image relève donc de la seule compétence du juge civil au titre de l'article 9 du Code civil.

263. La consécration de cette interprétation stricte par la Cour de cassation. De manière à mettre fin aux fluctuations jurisprudentielles, la chambre criminelle de la Cour de cassation a rendu un arrêt de principe le 16 mars 2016[768]. La haute juridiction rappelle aux visas des articles 111-4, 226-1 et 226-2 du Code pénal que « *la loi pénale est d'interprétation stricte* » et en déduit sur le fondement des deux derniers textes que « *le fait de porter à la connaissance du public ou d'un tiers, soit des paroles prononcées à titre privé ou confidentiel, soit l'image d'une personne se trouvant dans un lieu privé, n'est punissable que si l'enregistrement ou le document qui les contient a été réalisé sans le consentement de la personne concernée* ». Avec cet attendu de principe, le présent arrêt dépasse le cadre du simple arrêt d'espèce et donne une portée maximum à cette interprétation. Cette jurisprudence donne son plein sens au principe d'interprétation stricte de la loi pénale et de ce fait a été très largement saluée par la doctrine[769]. Certaines critiques[770] ont toutefois été formulées à la suite de cette décision, les auteurs reprochant à la Cour de cassation de ne pas assurer correctement la protection de la vie privée des individus qui est une obligation positive issue de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales[771]. Cependant, élargir l'interprétation du texte à une hypothèse qu'il apparaît souhaitable de réprimer s'apparente à une interprétation par analogie[772] qui est proscrite en droit pénal d'autant plus qu'il ne s'agit pas d'une analogie favorable[773].

---

[767] Crim., 28 janvier 2014, n° 12-80.157 : inédit.

[768] Crim., 16 mars 2016 , n° 15-82.676 : *Bull. crim.* n° 86 ; *JCP* G 2016, 658, note J.-C. SAINT-PAU ; *Dr. pén.* 2016, comm. 73, obs. P. CONTE ; *CCE* n° 5, mai 2016, comm. 42, A. LEPAGE ; *D.* 2016. p. 935, note A. SERINET ; *RSC* 2016, p. 96, obs. J. FRANCILLON ; *AJ Pénal* 2016, p. 268 note J.-B. THIERRY ; *Dalloz IP/IT* 2016, p. 321. Obs. G. DESGENS-PASANAU.

[769] V. en ce sens : J.-B. THIERRY, « Diffusion sur internet de la photographie d'une femme nue », *AJ Pénal* 2016, p. 268 ; A. LEPAGE, « Précision bienvenue au sujet de l'article 226-2 du Code pénal », *CCE* n° 5, mai 2016, comm. 42 ; G. DESGENS-PASANAU, « Le "*revenge porn*" n'est pas (toujours) une infraction pénale », *Dalloz IP/IT* 2016, Obs., p. 321. ; C. AIGOUY, « Le revenge porn ou la revanche du principe d'interprétation stricte de la loi pénale », *LPA*, 21 avril 2016, n° 80, p. 13.

[770] V. en ce sens P. CONTE, « Diffusion d'une photographie sans le consentement de l'intéressé », *Dr. pén.* 2016, n° 5, comm. 73 ; P. Le MAIGAT, « Revenge porn et cyber-harcèlement. Schizophrénie ou déconnexion du juge pénal ? », *Gaz. Pal.* 19 avril 2016, n° 15, p. 12 ; J.-C. SAINT-PAU, « Vie privée : du lien entre délit principal et délit de conséquence », *JCP* G n° 23, 6 juin 2016, 658.

[771] Principe notamment rappelé par CEDH, *Von Hannover c/ Allemagne*, 24 juin 2004, n° 59320/00, § 57.

[772] « *Cette manière de concevoir le rôle du juge renvoie directement à une approche anglaise dans laquelle la jurisprudence est la source principales du droit, y compris pénal, que le juge fait évoluer par le recours à la technique du* distinguishing*. L'interprétation analogique est alors de l'essence même du processus de création judiciaire du droit : le juge se doit d'appliquer la solution dégagée à propos d'une espèce donnée à toutes les*

264. L'analyse de l'inadaptation du dispositif pénal aux pratiques de vengeance pornographique rencontrées sur les réseaux sociaux en ligne doit cependant, pour être complète, être étendue à l'ensemble des incriminations prévues par le Code pénal et non pas seulement aux incriminations relevant de la vie privée. À ce titre, plusieurs qualifications pénales peuvent recouvrir le comportement en cause.

§2. Une protection incidente de l'intimité par d'autres incriminations

265. Un comportement saisi en tout ou partie. Parmi le *corpus* des infractions existantes, les divulgations non consenties d'images à caractère sexuel sur les sites de réseaux sociaux peuvent entrer dans le champ d'application de certaines d'entre elles et être sanctionnées sous ces fondements. La vengeance pornographique n'est alors plu sanctionnée au titre d'une atteinte à l'intimité de la vie privée mais en raison d'une atteinte à d'autres valeurs sociales protégées. Les incriminations ne proposent cependant le plus souvent qu'une protection partielle à l'égard de ce type de comportement (A) à l'exception du délit d'usurpation d'identité numérique qui offre pour sa part une protection englobante en la matière (B).

A. Une protection partielle offerte par certaines incriminations

266. Une appréhension pas assez spécifique ou trop spécifique. Si certaines incriminations préexistantes permettent d'envisager l'hypothèse du *revenge porn*, leurs définitions légales présentent toutefois des limites à l'égard de ce type particulier de comportement. Dans un premier temps, des incriminations démontrent leur incapacité à appréhender un tel comportement de manière autonome, la pratique du *revenge porn* ne constitue alors qu'un élément entrant dans un champ répressif plus large. C'est le cas des incriminations de harcèlement qui n'offrent qu'une protection partielle à l'égard de ce type de comportement (1). Dans un second temps, L'incrimination de l'article 227-23 du Code pénal

---

*situations similaires (*precedent*), et il est au contraire autorisé à appliquer une solution différente lorsqu'il relève l'existence d'un élément de différenciation* ». D. DECHENAUD, « Interprétation, téléologique ou interprétation par analogie ? », *in Histoire et méthodes d'interprétation en droit criminel*, Dalloz, Thèmes Commentaires, 2015, p. 137.

[773] « *La technique de l'analogie évoque l'idée de glissement. Si une loi est imparfaite, au sens où elle ne prévoit pas de répression dans une hypothèse où il paraîtrait souhaitable qu'il y en ait, il est tentant de raisonner par une sorte d'assimilation. L'omission du législateur doit être palliée par une extension de ce qu'il a prévu à ce qu'il a omis ; ce qui n'est même plus vraiment de l'interprétation. (…) Cette analogie légale n'est admissible que si elle joue en faveur du prévenu, du moins selon l'opinion courante (analogie in favorem ou bonam partem) (…) Intrinsèquement pourtant, le procédé n'est pas moins condamnable. Le droit pénal est le droit de la rigueur textuelle. Un laxisme unilatéral altère son office* », W. JEANDIDIER, « Principe de légalité criminelle », *J.-Cl.* Pénal Code, fasc. 20, août 2011 (mis à jour juin 2019), n° 11.

envisage une protection spécifique de la diffusion d'images pornographiques se restreignant toutefois aux seuls mineurs (2).

1) Une protection partielle offerte par les incriminations de harcèlements

267. La vengeance pornographique, une hypothèse de cyberharcèlement. Selon le Professeur Patrick Mistretta, les infractions de harcèlement ont en commun de protéger la liberté de chacun de consentir à un acte sexuel ou, plus largement, de ne pas subir d'agression morale, la *ratio legis* de ce texte se situe dès lors au-delà des simples agressions pour emprunter ce qui relève en réalité de la dignité des personnes[774]. Bien que la notion de dignité soit floue et insaisissable, particulièrement en droit pénal[775], la diffusion non consentie de l'image intime d'une personne dans le but de lui nuire peut parfaitement entrer dans le champ d'application des incriminations de harcèlement, plus particulièrement, du harcèlement moral général et du harcèlement sexuel. La vengeance pornographique devient alors une forme de cyberharcèlement[776]. Ce comportement peut d'abord relever d'un harcèlement moral général défini à l'article 222-33-2-2 du Code pénal. Cette incrimination permet d'éviter d'affilier ce comportement à une relation de travail mais également à une situation de couple qui est le plus souvent déjà révolue au moment des faits. Le harcèlement se déduirait soit de la diffusion répétée d'images de l'intimité de la victime, soit de la diffusion d'une seule image de ce type mais accompagnée d'autres actes ou comportements ayant également pour effet d'entraîner une dégradation de la santé physique ou mentale de la victime. Ensuite, un acte de *revenge porn* peut, de manière encore plus spécifique, être sanctionné dans le cadre d'un harcèlement sexuel prévu à l'alinéa 1er de l'article 222-33 du Code pénal. La diffusion d'une image à caractère sexuel d'une personne pourrait constituer un comportement à connotation sexuelle constitutif d'un acte de harcèlement sexuel.

268. Un harcèlement aggravé. Par ailleurs, tant à l'égard du harcèlement moral général, qu'à l'égard du harcèlement sexuel, l'utilisation d'un moyen de communication au public en ligne est source d'aggravation des pénalités encourues. En conséquence, dès lors que la pratique du *revenge porn* entre dans le cadre d'un harcèlement, les pénalités encourues sont alors portées à deux ans d'emprisonnement et 30 000 euros d'amende pour le harcèlement

[774] P. MISTRETTA, Rép. pén., Dalloz, mai 2019, *V°* Harcèlement, n° 7.
[775] V. en ce sens : P. MISTRETTA, « La protection de la dignité de la personne et les vicissitudes du droit pénal », *JCP* G n° 1, 12 janvier 2005, doctr. 100 ; P. CASSIA, *Dignité(s) : une notion juridique insaisissable ?*, Dalloz, 2016.
[776] V. en ce sens : J. FRANCILLON, « Cyberharcèlement et interprétation stricte des textes en matière pénale, *RSC* 2016 », p. 96.

moral général[777], et à trois ans d'emprisonnement et 45 000 euros d'amende pour le harcèlement sexuel[778].

269. Limite : l'impossible répression sous ces fondements d'un acte unique de *revenge porn*. Cependant, les délits de harcèlement sont par définition des infractions d'habitude[779] et exigent de manière constante la présence de « *propos ou comportements répétés* ». L'exigence de répétition constitue alors la principale limite à l'appréhension pénale de la diffusion d'une image à caractère sexuelle, un acte unique de diffusion ne pouvant constituer de manière autonome un délit de harcèlement. Les juges du fond[780] ont ainsi retenu une hypothèse de cyberharcèlement après avoir constaté la diffusion répétée sur internet de 34 articles nuisant à la réputation d'un couple et caractérisant le délit d'harcèlement moral général de l'article 222-33-2-2 du Code pénal.

2) Une protection spécifique de l'image pornographique du mineur

270. La sanction en toute circonstance de la diffusion de l'image à caractère sexuel d'un mineur. L'infraction prévue à l'article 227-23 du Code pénal sanctionne la prise d'une image à caractère pornographique d'un mineur ainsi que sa diffusion indépendamment d'un éventuel consentement de ce dernier à la prise d'image initiale. En l'espèce, la jurisprudence déduit le caractère pornographique de l'image dès le moment où elle met en scène le mineur de façon dénudée invoquant pour ce faire « *une position pornographique* »[781], « *une position équivoque* »[782], « *des positions suggestives ou ambigües* »[783], ou encore « *des attitudes ou postures dégradantes* »[784]. La prise d'image à caractère sexuel d'un mineur ainsi que sa diffusion sont en conséquence incriminées par l'article 222-33 du Code pénal indépendamment de tout consentement du mineur[785].

---

[777] C. pén., art. 222-33-2-2, al. 3, 4°.
[778] C. pén., art. 222-33, III, 6°.
[779] V. s*upra* n° 175.
[780] TGI Paris, ord. réf., 29 mars 2016, *Nathalie X. et Philippe Y.c / Emeric Z.*, Legalis.net, 1er avril 2016.
[781] Nimes, 3ème ch. corr., 22 mai 2001, n° JurisData : 2001-157851 : « *un album de photographies, dont une bonne partie pornographiques mettant en scène des jeunes filles posant nues et adoptant des positions pornographiques* ».
[782] Grenoble, 1ère ch. corr., 21 juin 2006, n° JurisData : 2006-314267 : « *des jeunes filles de moins de quinze ans dénudées dans positions équivoques, voire obscènes* ».
[783] Paris, 3ème Pôle, 5è ch., 9 décembre 2009, n° JurisData : 2009-019596 : « (…) *un disque CD-ROM contenant 74 images de jeunes filles mineures nues ou dénudées dans des positions suggestives ou ambiguës* ».
[784] Aix-en-Provence, 19ème ch. corr., 7 mars 2006, n° JurisData : 2006-312418 : l'expertise met en évidence « *des images de mineures nues dans des attitudes et postures* (…) *dégradantes* ».
[785] Pour une critique de cette conception trop large du terme « pornographique » V. J. LEONHARD, *Étude sur la pornographie pénalement prohibée*, Thèse Université Nancy 2, 2011, n° 252 et suiv.

271. Limite : un champ d'application restreint aux seuls mineurs. Cette qualification pénale est toutefois restreinte aux seuls mineurs. Cette restriction se justifie au regard de la *ratio legis* de la présente incrimination qui protège la vulnérabilité du mineur et son éventuelle mise en péril, davantage que l'intimité de sa vie privée. En conséquence, la principale limite de ce texte concerne la limite d'âge, inhérente à la valeur sociale protégée par l'incrimination. Les diffusions d'images intimes sur les réseaux sociaux ne pourront alors entrer dans cette qualification que lorsqu'elles concernent des mineurs. En excluant les majeurs de son champ d'application, la présente incrimination ne constitue donc pas un outil permettant d'appréhender de manière englobante l'ensemble des hypothèses de *revenge porn*, notamment lorsqu'elles concernent des majeurs.

B. Une protection englobante offerte par le délit d'usurpation d'identité

272. Le *revenge porn* saisit par le délit d'usurpation d'identité. À l'inverse des incriminations susmentionnées, le délit d'usurpation d'identité numérique prévu à l'article 226-4-1 du Code pénal semble pouvoir appréhender les vengeances pornographiques diffusées sur les sites de réseaux sociaux de manière autonome et sans exiger une qualité spécifique pour l'auteur ou la victime. Ce délit est en effet rédigé dans des termes suffisamment larges pour recouvrir la pratique de *revenge porn* dans sa globalité. Si cette pratique diverge avec l'action d'usurpation d'identité (1), elle converge toutefois dans une certaine mesure avec l'action d'usage de données identifiantes également prévue par le texte d'infraction (2).

1) La divergence avec l'action d'usurpation d'identité

273. Une action supposant le fait de se faire passer pour la victime. L'incrimination de l'article 226-4-1 du Code pénal concerne en premier lieu « *le fait d'usurper l'identité d'un tiers* ». Cette action correspond au fait de s'attribuer sans droit, et donc de manière illégitime, l'identité d'un tiers, dans le but de se faire passer pour lui[786]. Ceci vient répondre aux insuffisances des infractions préexistantes face aux pratiques de *phishing*, de création de faux sites web, de faux profils sur les sites de réseaux sociaux. Plus généralement, « *cette loi répondait, à l'origine, à l'utilisation croissante des éléments permettant l'identification*

[786] N. RIAS, « Usurpation d'identité ou usage de données permettant d'identifier un tiers », *J.-Cl.* Pénal Code, fasc. 20, mai 2012 (mis à jour septembre 2018), n° 6.

d'autrui sur internet et notamment sur les réseaux sociaux »[787]. La présente infraction vient ainsi protéger l'usage frauduleux du nom d'un tiers et spécifiquement de son identité numérique. L'action d'usurpation d'identité consiste alors à se faire passer pour autrui dans le but de nuire à la personne. La vengeance pornographique ne correspond donc à l'action d'usurper l'identité d'un tiers que dans l'hypothèse où l'auteur diffuse d'une part les images de l'intimité sexuelle d'une personne et d'autre part, se fait passer pour cette dernière auprès des internautes.

2) La convergence avec l'action d'usage de données identifiantes

274. La notion de données identifiantes. Si la situation du *revenge porn* est très différente de celle imaginée par le législateur lors du vote de la loi créant le délit d'usurpation d'identité numérique[788], ce comportement spécifique peut toutefois être appréhendé par l'article 226-4-1 du Code pénal du fait qu' il incrimine également le fait « *de faire usage d'une ou plusieurs données de toute nature permettant d'identifier un tiers en vue de troubler sa tranquillité, ou de porter atteinte à son honneur ou à sa considération* ». En l'occurrence, le terme « *donnée de toute nature* » faisait initialement référence à la notion de « *données à caractère personnel* » au sens de la loi informatique et libertés. Cette dernière les définissait comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* »[789]. La différence de formulation retenue suggère d'admettre que le délit vise les identifiants, mot de passe ou encore une adresse IP[790]. Les juges du fond ont considéré dans ce sens qu'une adresse IP était une donnée personnelle identifiante au sens du présent délit « *permettant de retrouver la personne physique ayant mis en ligne le contenu* »[791]. En conséquence, si le terme « *donnée de toute nature* » bénéficie d'une certaine largesse encore suggère-t-il de permettre une identification précise de la victime par référence à son nom ou du moins à un pseudonyme ou une adresse IP. L'image à caractère sexuel d'une personne entre ainsi dans le champ de la protection pénale offerte par l'article 226-4-1 du

[787] C. LACROIX, Rép. pén. Dalloz, Juin 2012, *V°* Usurpation d'identité, n° 49.
[788] L. n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, *JORF* n° 0062, 15 mars 2011, p. 4582, texte n° 2, art. 2.
[789] L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ancien art. 2. Cette définition est désormais reprise à l'article 4 (1) du Règlement (UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (règlement général sur la protection des données dit RGPD).
[790] C. LACROIX, Rép. pén. Dalloz, Juin 2012, *V°* Usurpation d'identité, n° 58.
[791] TGI Paris, 3ème ch., 24 juin 2009, RG nº 08/03317, Jean-Yves Lafesse et a. c/ Google et a.

Code pénal mais seulement lorsque la personne accompagne la diffusion d'un élément d'identification autre qu'une simple image ou vidéo de la victime. Ceci démontre bien que le délit de l'article 226-4-1 du Code pénal concentre sa protection sur l'identité des individus et non spécifiquement sur leur intimité.

275. Un dol spécial correspondant à l'intention animant l'auteur de la vengeance pornographique. En outre, le présent texte d'infraction prévoit un dol spécial chez l'auteur de l'infraction à savoir, l'intention de troubler la tranquillité ou de porter atteinte à l'honneur ou à la considération de la personne. Cette définition de l'intention coupable coïncide en l'occurrence avec celle qui anime l'auteur d'un *revenge porn*, ce dernier étant animé par un esprit de vengeance souhaite *de facto* porter atteinte à la tranquillité de la victime et atteindre par le biais de la diffusion de l'image à caractère sexuel son honneur et sa considération. Certains auteurs s'étonnent alors que le délit de l'article 226-4-1 du Code pénal n'ait pas été retenu dans les cas de *revenge porn* et notamment celui soumis à la Cour de cassation dans son arrêt du 16 mars 2016[792].

276. Conclusion de la Section 1. Le dispositif traditionnel de protection de la vie prive démontre de réelles carences dans la protection de l'intimité de la vie privée provenant majoritairement du fait que le délit de l'article 226-2 du Code pénal est un délit de conséquence ne bénéficiant pas de l'autonomie dont il devrait. Les autres incriminations permettent quant à elles de venir appréhender de manière incidente les actes de diffusion non consentie d'images à caractère sexuel. Sur ce point, c'est l'incrimination d'usurpation d'identité numérique qui permet d'envisager le plus globalement possible un acte de vengeance pornographique. Cependant, même cette incrimination démontre des limites en ce qu'elle protège avant tout l'identité de l'individu par référence à un nom. L'image intime ne bénéficie donc pas d'une protection à part entière dans cette hypothèse. Le législateur s'est alors résolu à engager une réforme nécessaire en instaurant la nouvelle incrimination de l'article 226-2-1 du Code pénal qui sanctionne la diffusion non consentie de l'intimité d'une personne indépendamment de son consentement initial à la prise d'image.

[792] Selon Monsieur Jean-Baptiste Thierry : « *On s'étonnera toutefois que la qualification retenue n'ait pas été celle prévue à l'article 226-4-1 du code pénal qui incrimine, aux côtés de l'usurpation d'identité, le fait de faire usage d'une ou plusieurs données de toute nature permettant d'identifier un tiers en vue de troubler sa tranquillité, ou de porter atteinte à son honneur ou à sa considération. Nul doute que la diffusion en ligne de la photographie d'une femme nue, sans son consentement, entre dans les prévisions de ce texte* ». J.-B. THIERRY, « Diffusion sur internet de la photographie d'une femme nue », *AJ Pénal* 2016, p. 268.

Section 2 : Une extension justifiée de la protection de l'intimité

277. Une pénalisation se retrouvant dans des législations étrangères. De nombreux pays ont consacré ces dernières années dans leurs législations des incriminations venant appréhender de manière spécifique et autonome les cas d'une diffusion non consentie d'images à caractère sexuel. Ainsi, dans sa loi anti-*revenge porn* du 1er octobre 2013, l'État de Californie est venu ajouter à son arsenal répressif une infraction formulée de la manière suivante : « *Toute personne qui photographie ou enregistre par tout moyen l'image d'une ou plusieurs parties intimes d'une personne identifiable alors qu'il était convenu, implicitement ou explicitement, du caractère privé de ces images, et qui par la suite, diffuse ladite image dans l'intention de lui causer une grave détresse émotionnelle et lorsque la personne visée subit effectivement une telle détresse, se rend coupable d'un comportement déviant puni de 6 mois d'emprisonnement et de 1000 dollars d'amende* »[793]. Le législateur californien a opté en l'espèce pour un dol spécial en érigeant en élément constitutif du délit la volonté de causer une grave détresse émotionnelle chez la victime. Par ailleurs, il s'agit d'une infraction matérielle : le résultat redouté doit être atteint pour que l'infraction soit qualifiée. La victime doit donc subir effectivement une telle détresse suite à la publication d'une image à caractère sexuel la concernant. La faiblesse majeure de ce texte réside toutefois dans le fait, pour le législateur californien, d'avoir assimilé l'auteur de la prise d'image initiale avec l'auteur de la diffusion de l'image. Cela exclu de facto toute une multitude d'hypothèses à l'instar de la pratique du « *selfie* » : si la victime prend une image d'elle dénudée et que son compagnon, par vengeance, décide de la publier sur un réseau social, l'infraction telle que prévue par le droit californien ne pourra être constituée car l'image n'a pas été prise par la personne auteur de la diffusion. Plus généralement, le législateur californien a trop détaillé le comportement susceptible de répression, au point de restreindre de manière non pertinente le champ d'application du texte.

278. Le 13 avril 2015 le Royaume-Uni a également étoffé sa législation à ce sujet en affirmant qu' « *est réprimé le fait pour une personne de diffuser des photographies ou*

[793] Le texte dans sa rédaction originale : « *Any person who photographs or records by any means the image of the intimate body part or parts of another identifiable person, under circumstances where the parties agree or understand that the image shall remain private, and the person subsequently distributes the image taken, with the intent to cause serious emotional distress, and the depicted person suffers serious emotional distress, is guilty of disorderly conduct and subject to that same punishment* », Californian Senate Bill N° 255 Disorderly conduct : invasion of privacy.
<http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB255> (dernière consultation le 9 octobre 2019).

enregistrements à caractère sexuel si la diffusion est faite sans le consentement de la personne qui apparaît sur la photographie ou l'enregistrement et lorsque la personne a agi avec l'intention de mettre en détresse »[794]. Concernant l'élément intellectuel, l'infraction Britannique exige également un dol spécial pour l'auteur de l'infraction : à savoir non seulement l'intention de diffuser la photographie ou les enregistrements, mais également l'intention, par cette diffusion, de mettre en détresse la personne concernée. Il s'agit par ailleurs d'une infraction formelle qui se réalise par la seule diffusion de l'image à caractère sexuel. Autrement dit, le résultat escompté par l'auteur ne fait pas parti de l'élément matériel de l'infraction à la différence de son homologue californien. Pour qualifier l'infraction, peu importe la réelle répercussion pour la victime de la diffusion de son image. Enfin, et contrairement au droit californien, la législateur britannique n'a pas pris le soin de préciser qui était l'auteur de la prise d'image initiale. Cela permet d'ouvrir un plus large champ répressif et de ne pas s'enfermer dans une rédaction trop étroite. Ce choix répressif paraît préférable partant du fait qu'il s'agit de sanctionner la diffusion d'une image à caractère sexuel et non la prise de cette image. Seul importe donc dans la répression la diffusion.

279. La nouvelle incrimination de l'article 226-2-1 du Code pénal. Si le droit pénal ne constitue assurément pas un droit revendicateur mais à l'inverse, un droit sanctionnateur, l'évolution constatée des atteintes à l'intimité dans le domaine numérique a poussé le législateur à étendre le corps des incriminations protégeant la vie privée. En réaction à la jurisprudence de la chambre criminelle du 16 mars 2016 et aux diverses observations doctrinales[795] formulées à l'encontre des articles 226-1 et 226-2 du Code pénal, l'article 67 de la loi pour la République numérique[796] vient, sans directement modifier ces textes, créer le nouvel article 226-2-1 du Code pénal qui dispose : « *Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende ; Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu,*

[794] Le texte dans sa rédaction originale : « *It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made-(a) without the consent of an individual who appears in the photograph or film, and (b) with the intention of causing that individual distress* », UK ST 2015 c. 2 Pt 1 s. 33, Criminal Justice and Courts Act 2015 c. 2, s. 33: *Disclosing private sexual photographs and films with intent to cause distress*.

[795] V. *supra* n[os] 262 et 263.

[796] L. n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, *JORF*, 19 juillet 1970, p. 6751, art. 67.

avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1 ».

Si l'adoption d'une telle incrimination révèle une évolution profonde de la protection pénale de la vie privée (**§2**), sa rédaction est toutefois entourée d'incertitudes qui justifient sa réécriture (**§1**).

§1. Les incertitudes entourant la rédaction de l'incrimination

280. Le choix rédactionnel entrepris par le législateur pour le nouvel article 226-2-1 du Code pénal met en exergue certaines incertitudes quant à l'interprétation à donner de ce texte. Le premier alinéa organise une rupture avec la protection uniforme de la vie privée (A) et le second alinéa pénalise de manière maladroite la diffusion non consentie de l'intimité sexuelle (B).

A. Une rupture avec la protection uniforme de la vie privée

281. Selon le premier alinéa de la nouvelle incrimination : « *Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende* ». Ainsi, en proposant une protection spécifique des paroles et images à caractère sexuel (1) justifiant une aggravation de la répression (2), cette nouvelle disposition introduit une rupture avec l'ancienne protection uniforme de la vie privée.

1) Une protection spécifique des paroles ou images à caractère sexuel

282. Le nouvel article 226-2-1 du Code pénal « *marque une rupture par rapport aux articles 226-1 et 226-2 du Code pénal qui protègent uniformément la vie privée dans toutes ses manifestations potentielles* »[797]. En l'occurrence, la protection de la vie privée porte spécifiquement sur les images ou paroles à caractère sexuel (a) prises dans un lieu public ou privé (b).

[797] A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *CCE* n° 2, février 2017, étude 3 ; *Dr. pén.* 2017, n° 1, étude 1.

a- La notion d'image ou parole à caractère sexuel

283. L'image à caractère sexuel, définition objective. Selon une approche médicale ou biologique, les caractères sexuels regroupent « *l'ensemble des caractères physiques ou psychologiques dépendant de l'imprégnation en hormones sexuelles, du sexe génétique (XY ou XX), appareil génital, déterminant l'aspect (le phénotype) féminin ou masculin d'un individu. Ils apparaissent progressivement au moment de la puberté, parallèlement à l'augmentation des hormones* »[798]. Il est nécessaire de distinguer les caractères sexuels primaires correspondant aux organes génitaux et formés dès le stade de la vie embryonnaire, et les carctères sexuels secondaires apparraissant quant à eux à la puberté comme la poitrine féminine et la pilosité pubienne[799]. Cependant, cette définition scientifique des caractères sexuels, limitativement énumérés, ne correspond pas à l'identique à l'expression « *un caractère sexuel* » utilisée dans la nouvelle incrimination. La conception juridique du « *caractère sexuel* » est potentiellement plus large en ce qu'elle introduit une dimension subjective dans son appréciation.

284. L'image à caractère sexuel, définition subjective. Ainsi, d'une part, une image peut revêtir ce caractère sexuel parce qu'elle le suggère et donc sans le faire apparaître de manière objective. Le caractère sexuel dépend dès lors de l'interprétation faite de l'image par l'observateur. Le caractère sexuel s'interprète alors dans une position ou une attitude à connotation sexuelle. Par exemple : *Quid* d'une femme (ou d'un homme) mangeant une banane ? L'image peut être à la fois neutre ou peut présenter un caractère sexuel selon la mise en scène[800]. Le contexte peut faire naître une connotation sexuelle mais en matière de pornographie le contexte est insuffisant. D'autre part, une image représentant un organe sexuel présente-t-elle *a fortiori* ce caractère sexuel ? Si l'image ne présente que l'organe sexuel de la personne ou du moins si l'image ne fait pas apparaître le visage de la personne, sa diffusion ne peut entraîner la qualification de l'infraction de l'article 226-2-1 du Code pénal[801]. Par ailleurs, les images de personnes dénudées présentent-elles automatiquement un caractère sexuel ? L'exemple qui revient ici est celui de l'image d'une femme aux seins nus. En l'occurrence, les standards de la communauté Facebook se montrent particulièrement

[798] Larousse, encyclodédie en ligne, *V°* Caractère sexuel.
<https://www.larousse.fr/encyclopedie/divers/caractère_sexuel> (dernière consultation le 9 octobre 2019).
[799] *Ibid.*
[800] Le contexte d'une image peut faire naitre une connotation sexuelle, en matière de pornographie ce contexte est cependant insuffisant. V. J. LEONHARD, *Étude sur la pornographie pénalement prohibée*, Thèse Université Nancy 2, 2011, n° 279 et suiv.
[801] Une réserve peut être toutefois faite dans l'hypothèse où la personne qui diffuserait l'image de l'organe sexuel identifie en même temps la personne sur le réseau social.

stricts en précisant qu'une photo de profil à caractère pornographique ou contenant de la nudité est interdite[802]. Au final, l'interprétation de l'article 226-2-1 du Code pénal relève d'une particulière subjectivité dont les limites sont difficilement prédictibles[803].

285. La parole à caractère sexuel. Le constat est similaire concernant l'appréciation du caractère sexuel des paroles qui peut varier en fonction du contenu et du contexte des mots. Ainsi, une conversation à contenu sexuel peut renvoyer aux détails d'une relation sexuelle ou évoquer des aspects de l'anatomie sexuelle. La parole peut être également prononcée dans un contexte sexuel par exemple lors d'une relation sexuelle[804]. L'hésitation est même permise concernant les propos abordant une maladie affectant un organe sexuel[805], le champ répressif ne devrait cependant pas concerner ce type de propos dès lors qu'ils sont diffusés dans un contexte médical et à visée pédagogique.

286. Interrogation sur la pertinence de la protection spécifique de l'image ou de la parole à caractère sexuel. En accentuant la protection lorsque l'atteinte à la vie privée concerne la diffusion d'une image ou d'une parole à caractère sexuel, le législateur choisit d'orienter sa politique répressive sur un aspect unique de l'intimité. Plusieurs auteurs se sont interrogés sur la pertinence de cette protection spécifique[806], selon eux, d'autres aspects que l'intimité sexuelle auraient pu être saisis par l'article 226-2-1 du Code pénal notamment l'état de santé de l'individu. Le Professeur Agathe Lepage relève ainsi que « *le législateur, les yeux braqués sur les faits divers qui lui ont inspiré ce texte, ne s'est pas demandé si d'autres aspects de l'intimité ne méritaient pas d'accéder à la même protection renforcée. L'image d'une personne sur un lit d'hôpital, par exemple, touche à une autre forme d'intimité que le sexe qui n'en est pas moins digne de considération* »[807].

---

[802] S. ANDRÉ, « Que peut-on montrer sur sa photo de profil Facebook ? », *in* C. MANARA (dir.), *Réseaux sociaux : 101 questions juridiques*, Éd. Diateino, 2013, p. 31. V. *infra* n° 481 à 485.
[803] A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *op. cit.*
[804] *Ibid.*
[805] Le Professeur Agathe Lepage cite en exemple des propos concernant le cancer des testicules ou de l'uterus. V. : A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *op. cit.*
[806] V. S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *RSC* 2016, p. 741 ; A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *op. cit.*
[807] A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *op. cit.*

b- Un lieu public ou privé

287. L'incohérence. Dès lors que le caractère sexuel des paroles ou images est démontré, le comportement infractionnel peut subir l'aggravation de l'article 226-2-1 du Code pénal et ce, peu importe le lieu (public ou privé) de l'atteinte initiale. Telle est la première lecture qui ressort de l'alinéa 1er de l'article 226-2-1 du Code pénal. Cependant, une lecture plus approfondie peut amener à une toute autre compréhension. L'article 226-2-1 alinéa 1er du Code pénal est en effet conçu comme une circonstance aggravante des articles 226-1 et 226-2 du même Code qui définissent le comportement infractionnel originel. Il existe alors une ambiguïté voire, une incohérence entre la définition pénale de l'atteinte à la vie privée et la circonstance aggravante qui en est issue. L'article 226-1 du Code pénal distingue deux objets d'atteinte, à savoir la parole (1°) et l'image (2°) de la personne. Concernant la parole, la nature publique ou privée du lieu où parle la personne est sans incidence sur la constitution du délit car il suffit qu'elle soit prononcée « *à titre privé ou confidentiel* ». À l'inverse, l'image de la personne victime de l'atteinte doit impérativement se trouver « *dans un lieu privé* ». En conséquence, l'article 226-2-1 alinéa 1er du Code pénal entre en contradiction avec l'article 226-1 2° en ce qu'il permet que l'atteinte soit observée également dans un lieu public.

288. La deuxième lecture. Cette incohérence peut toutefois s'expliquer à travers une deuxième lecture de l'article 226-2-1 alinéa 1er. Le critère du lieu public ou privé admis par le nouvel article peut être interprété comme faisant référence tantôt au 1° de l'article 226-1 et tantôt à son 2°, ainsi la circonstance aggravante « *s'accommoderait en réalité du caractère public de l'endroit qu'à la condition que ce caractère soit également admis par le texte d'incrimination* »[808]. La référence au lieu public ne vaudrait alors que pour l'hypothèse des paroles, celle de l'image resterait cantonnée au lieu privé. Vu sous cet angle, le terme « *ou* » ne marquerait pas une indifférence à la nature des lieux mais au contraire une alternative fonction de la première incrimination[809]. Cette deuxième lecture n'est toutefois pas davantage satisfaisante dans la mesure où elle ne reflète pas la volonté du législateur qui souhaitait

[808] S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *op. cit.*

[809] Cette conception partagée par le Professeur Agathe Lepage selon laquelle : « *il conviendrait, à défaut d'une réécriture du texte par le législateur, de déployer une interprétation qui neutralise les termes « prises dans un lieu public ou privé ». Cela reviendrait à considérer qu'ils ne sont que l'expression mutualisée des conditions prévues par l'article 226-1 auxquelles ils n'ajoutent rien, leur fonction consistant juste à rappeler que l'image captée est celle d'une personne dans un lieu privé tandis que les paroles peuvent l'être dans un lieu privé comme dans un lieu public. Ainsi, il faudrait comprendre ces termes à la lumière d'une précision, comme signifiant non pas « prises indifféremment dans un lieu public ou privé » mais « prises, selon les actes considérés, dans un lieu public ou privé* ». A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *op. cit.*

mettre un terme aux faiblesses des incriminations antérieures, notamment quant à leur champ d'application trop restrictif.

2) Une aggravation de la répression

289. Une nature juridique incertaine. De par son mode de rédaction et aux interrogations auxquelles il renvoie, la rédaction du premier aliéna de l'article 226-2-1 du Code pénal est loin de faire l'unanimité. Pis encore, il suscite de profonds questionnements quant à sa véritable nature juridique[810]. Sur ce point, l'article 226-2-1 alinéa 1er du Code pénal constitue une circonstance aggravante *sui generis* (a) qui offre le choix à plusieurs possibilités d'interprétation (b).

a- Une circonstance aggravante *sui generis*

290. Constat. Dans un premier temps, la façon dont est rédigé l'article 226-2-1 alinéa 1er ne laisse pas d'autre choix que de conclure qu'il s'agit d'une circonstance aggravante, en effet ce dernier précise que « *Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende* ». En employant l'expression « *les peines sont portées à* », le législateur renseigne le lecteur sur la nature de ce premier alinéa. Partant, l'article 226-2-1 alinéa 1er ne pourrait être interprété comme une infraction spécifique.

291. Problématique. Avec ce nouvel article 226-2-1 le Code pénal hérite d'une situation pour la moins singulière : en possédant un champ d'application plus étendu, la circonstance aggravante contredit le texte d'incrimination auquel elle s'applique. Plus encore, la caractérisation de cette circonstance aggravante peut se révéler nécessaire à la constitution même de l'infraction.

292. Distinction classique entre infraction et circonstance aggravante. Les prévisions de l'article 226-2-1 du Code pénal obscurcissent la distinction classique entre infraction et circonstance aggravante. De manière générale, les circonstances aggravantes spéciales[811] ne peuvent être retenues que pour les infractions dans le cadre desquelles elles sont

[810] V. sur ce point : S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *op. cit.*

[811] Par opposition aux circonstances aggravantes générales qui n'ont besoin d'aucun texte particulier pour que les peines encourues soient aggravées. On distingue parmi ces circonstances aggravantes générales : la récidive, l'utilisation d'un moyen de cryptologie, le motif raciste ou sexuel des crimes et délits. V. M. DALLOZ, Rép. pén. Dalloz, juin 2017 (mis à jour août 2018), *V°* Circonstances aggravantes, nos 19 et suiv.

spécifiquement prévues[812]. Il est admis qu'il faut refuser la qualité de circonstance aggravante à toutes les conditions tant matérielles que psychologiques, indispensables à l'établissement d'une qualification pénale. Le Professeur Michèle-Laure Rassat observe que : « *du point de vue matériel, les éléments en l'absence desquels il n'existe plus aucune qualification applicable aux faits doivent être considérés comme des éléments constitutifs. En revanche, dès lors qu'un texte pénal décrit toutes les conditions d'existence d'une infraction, chaque élément complémentaire dont la réalisation est envisagée par le législateur et dont l'effet est d'augmenter le quantum des peines encourues doit être analysé comme une circonstance aggravante* »[813]. Or, la présente hypothèse peut amener au constat suivant : dans un premier cas, si les images ne présentent pas un caractère sexuel et que l'individu visé ne se trouvait pas dans un lieu privé, alors la diffusion de ces images n'est pas répréhensible. À l'inverse, si pour la même situation, le caractère sexuel est vérifié les faits deviennent répréhensibles et de surcroît, aggravés. La circonstance aggravante de l'article 226-2-1 du Code pénal se trouve sur un pied d'égalité avec les éléments matériels de l'article 226-1 du Code pénal du fait qu'au-delà de proposer une aggravation des pénalités encourues, elle conditionne l'engagement de la responsabilité de l'auteur de l'infraction. Il s'agirait d'un point de vue pénal d'un outil d'une nature singulière. Différentes interprétations sont possibles.

b- Les différentes possibilités d'interprétation

293. L'alinéa premier de l'article 226-2-1 du Code pénal est à la frontière entre une circonstance aggravante et une infraction autonome. En réalité, deux hypothèses sont à distinguer.

294. Première hypothèse. Dans un premier temps, l'infraction de l'article 226-2-1 du Code pénal est une banale infraction aggravée lorsque les faits reprochés sont déjà punissables au titre des articles 226-1 ou 226-2 du Code pénal, c'est-à-dire dans l'hypothèse où la diffusion de l'image ou de la parole d'autrui résulte d'une atteinte primaire à la vie privée. Le caractère sexuel devient alors une circonstance aggravante ordinaire qui donne aux faits une gravité supplémentaire, mais n'a aucune influence sur le caractère délictueux de l'acte.

295. Seconde hypothèse. Dans un second temps, lorsque les faits reprochés n'entrent pas dans les prévisions des articles 226-1 et 226-2 du Code pénal autrement dit, dans l'hypothèse

[812] M.-L. RASSAT, *Droit pénal général*, Ellipses, 4ème éd., 2017, p. 621, n° 591.
[813] M. DALLOZ, Rép. pén. Dalloz, juin 2017 (mis à jour août 2018), *V°* Circonstances aggravantes, n° 11 et suiv.

où l'image ou la parole résulte d'un lieu public, la nature juridique de l'article 226-2-1 aliéna 1er devient plus incertaine. Le caractère sexuel deviendrait à la fois une circonstance aggravante et un élément constitutif du fait que sa présence devienne nécessaire pour la répression des faits. Il ne peut alors s'agir d'une infraction aggravée dès lors que les infractions simples ne sont même pas constituées. Partant de ce postulat, Monsieur Stéphane Detraz a imaginé plusieurs possibilités d'interprétation[814] :

296. « *Un élément constitutif aggravant* ». Dans cette seconde hypothèse, le caractère sexuel devient un élément constitutif de l'infraction soumis au régime de cette catégorie juridique. En conséquence, l'intention devant être vérifiée à l'égard de l'ensemble des éléments constitutifs, le prévenu devra avoir conscience du caractère sexuel des images et la volonté de les diffuser alors qu'une simple circonstance aggravante n'exige pas en principe cet élément matériel. De même en procédure pénale, le caractère sexuel comptera pour fixer l'étendue de la saisine *in rem* des juridictions, alors qu'une circonstance aggravante peut être librement ajoutée à la cause par les juges. Ce caractère sexuel, un élément constitutif de l'infraction accroît en outre la sévérité des peines, il serait donc un « *élément constitutif aggravant dont la présence entraîne la constitution du délit et, simultanément, le soumet à des peines aussi sévères que celles des infractions aggravées de la même famille* »[815].

297. « *Une circonstance aggravante constitutive* ». Cette réflexion peut être cependant prise à l'opposé en considérant qu'il s'agit d'une circonstance aggravante qui influe sur le caractère délictueux des faits. Il peut dans ce cas s'agir également d'une « *circonstance aggravante constitutive* »[816] : le caractère sexuel aggrave les peines et supprime l'une des exigences matérielles de l'infraction, à savoir celle d'un lieu privé. En parallèle, la condition du lieu privé cherche sa place au sein de ce nouvel ensemble d'infractions, elle est en effet soumise à l'alternative suivante : soit le caractère sexuel de l'image est absent, et la personne doit se trouver dans un tel lieu ; soit il est présent, et la nature du lieu est sans importance.

298. Critique. Le constat qui ressort de cette analyse est que l'article 226-2-1 alinéa 1er du Code pénal instaure « *une chimère juridique* »[817] qui transforme la nature d'un texte au gré des situations d'espèce qui lui sont soumises au point de considérer que « *le bien-fondé*

[814] S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *op. cit.*
[815] *Ibid*.
[816] *Ibid*.
[817] *Ibid*.

criminologique d'un tel assemblage est alors des plus douteux »[818]. Ce doute est également permis quant à la constitutionnalité d'un tel mécanisme. Le Conseil constitutionnel a en effet évoqué à l'occasion de l'examen de l'article 222-22-1 du Code pénal « *qu'il ne résulte pas de ces dispositions qu'un des éléments constitutifs du viol ou de l'agression sexuelle est, dans le même temps, une circonstance aggravante de ces infractions, ces dispositions ne méconnaissent pas le principe de légalité des délits (…) par suite, le grief tiré de l'atteinte au principe de légalité des délits et des peines doit être écarté* »[819]. Par une lecture *a contrario* de cette décision, il semblerait qu'un élément constitutif qui revêtirait également le caractère de circonstance aggravante entre en contrariété avec le principe à valeur constitutionnelle de légalité des délits et des peines.

B. Une pénalisation maladroite de la diffusion non consentie de l'intimité sexuelle

299. Le second alinéa de l'article 226-2-1 du Code pénal créée pour sa part un délit rédigé dans les termes suivants : « *Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1* ». Le principal apport de ce nouveau texte est alors de prévoir une pénalisation de la diffusion[820] non consentie de l'intimité de la victime peut importe son consentement initial à la prise d'image. Toutefois, il apparaît, à la lecture du texte d'incrimination, que ce dernier renvoie encore à l'article 226-1 du Code pénal. Le nouvel article 226-2-1 aliéna 2nd du Code pénal n'en devient pas pour autant une infraction de conséquence du fait que la qualification de cette infraction n'est pas dépendante de la constitution préalable de l'une des deux infractions précédentes. Ainsi, si l'autonomie se fait davantage ressentir dans cette nouvelle incrimination, cette dernière demeure encore

[818] *Ibid.*
[819] Cons. const., 6 février 2015, n° 2014-448 QPC, *D.* 2015 p. 324 ; *RSC* 2015 p. 86, obs. Y. MAYAUD ; *AJ Pénal* 2015 p. 248, note E. DREYER.
[820] Le délit du second alinéa de l'article 226-2-1 du Code pénal emploie le terme « *diffusion* » dans la description du comportement incriminé en l'associant au fait de porter le document litigieux « *à la connaissance du public ou d'un tiers* ». En l'espèce, alors que la notion de publication est propre au droit de la presse et implique une série de conditions particulières à respecter, la notion de diffusion ne fait pour sa part référence à aucun régime particulier. Le terme diffusion représente ainsi un champ d'application plus large que celui de publication. À l'inverse du droit de la presse où c'est la publication qui fait le délit, la diffusion peut être caractérisée alors même d'une seule personne est destinataire de l'image ou de l'enregistrement sonore. La diffusion, contrairement à la publication, ne nécessite donc pas une dimension de publicité. A. SERINET, « L'instauration d'une répression des atteintes à l'intimité sexuelle par la loi pour une république numérique », *D.* 2016, p. 1711.

critiquable en raison de la présence d'un système de renvoie à l'article 226-1. Ce constat d'une rédaction imparfaite (1) suggère alors une nécessaire réécriture de l'infraction (2).

1) Une rédaction imparfaite

300. L'assouplissement du lien de causalité avec l'infraction de l'article 226-1 du Code pénal. La nouvelle infraction fait référence à l'article 226-1 du Code pénal quant aux moyens utilisés pour réaliser l'atteinte à la vie privée. L'alinéa second sanctionne la diffusion d'un enregistrement ou d'un document à caractère sexuel obtenu « *avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1* ». La relation causale de l'article 226-2-1 alinéa 2nd avec l'article 226-1 du Code pénal se trouve cependant davantage distendue en comparaison aux liens étroits unissant les articles 226-1 et 226-2-1 alinéa 1er du Code pénal. Monsieur Stéphane Detraze observe cet « *emprunt relatif* »[821] en plusieurs endroits :

Premièrement, l'article 226-2-1 alinéa 2nd du Code pénal ne fait pas directement référence aux « *paroles* » ou à « *l'image* » prévue à l'article 226-1 du Code pénal mais à « *tout enregistrement ou tout document portant sur des paroles ou des images* ». Cette formulation peut révéler une différence dans la réalisation matérielle de l'infraction. En effet, la rédaction utilisée ne permet pas d'exclure l'hypothèse d'un document écrit faisant état d'une scène intime vue à l'occasion de l'espionnage visuel d'une personne. Cette interprétation peut être validée du fait qu'il suffit que le document ou l'enregistrement « *porte* » sur les paroles et l'image et n'exige en conséquence pas qu'il les « *comporte* »[822].

Deuxièmement, l'article 226-2-1 alinéa 2nd précise que ces documents ou enregistrements soient obtenus « *à l'aide* » des actes incriminés à l'article 226-1 du Code pénal[823]. Il n'est donc pas exigé que les documents ou enregistrements vecteurs de l'atteinte aient été « *fabriqués au moyen de ceux-ci* ». En conséquence, le texte n'impose pas que les paroles ou images objets de l'infraction initiale se retrouvent impérativement à l'identique dans le document ou l'enregistrement diffusé contribuant alors à distendre un peu plus, sans

[821] S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *op. cit.*
[822] *Ibid.*
[823] L'article 226-2-1 du Code pénal reprenant ici une formulation déjà existante à l'article 226-2 du Code pénal.

toutefois le rompre, le lien de causalité entre l'infraction de l'article 226-1 et l'infraction de l'article 226-2-1 du Code pénal[824].

Enfin, le nouveau texte d'incrimination prend également en compte l'hypothèse particulière où l'image initiale résulterait de la victime elle-même. Le texte précise à ce titre que le contenu initial peut être obtenu « *avec le consentement exprès ou présumé de la personne ou par elle-même* ». Cette prise en compte de la part du législateur des modalités particulières de la prise d'image initiale montre l'envie d'adapter le champ répressif aux pratiques rencontrées sur les réseaux sociaux en ligne et notamment à celle très répandue et caractéristique du *Selfie*[825]. Mais surtout, cette précision démontre que la prise d'image initiale peut résulter d'un acte parfaitement licite.

301. Persistance du lien de causalité. Cependant, en employant l'expression de « *tout enregistrement ou tout document* […] *obtenu,* […] *à l'aide des actes incriminés à l'article 226-1 du Code pénal* », la nouvelle infraction demeure toujours liée aux actes matériels définis à l'article 226-1 du Code pénal et fatalement, à l'exigence de l'absence de consentement lors de la captation initiale. Ceci révèle la mauvaise appréhension par le législateur des problématiques juridiques issues de la combinaison des articles 226-1 et 226-2 du Code pénal pourtant mises en exergue par l'arrêt de la Cour de cassation du 16 mars 2016[826]. Ainsi, la réforme n'a non seulement pas porté de modifications à la formule « *obtenu à l'aide de l'un des actes prévus par l'article 226-1 du Code pénal* » présente à l'article 226-2 du Code pénal mais l'a, de surcroît, reproduite au second alinéa du nouvel article 226-2-1 du Code pénal. Pour sortir de cet engrenage, l'interprétation serait alors de considérer que la formule renvoyant aux « *actes incriminés à l'article 226-1 du Code pénal* » ne fait référence qu'aux faits de captation, d'enregistrement, de transmission ou de fixation des paroles ou de l'image de la personne sans prendre en compte la condition de l'absence de consentement de celle-ci.

302. Rejet de la condition de l'absence de consentement initial de la victime. Cette maladresse rédactionnelle est cependant contre balancée par la précision faite que

---

[824] S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *op. cit.*

[825] « *Autoportrait photographique, généralement réalisé avec un téléphone intelligent et destiné à être publié sur les réseaux sociaux* ». Dictionnaire Larousse en ligne, *V°* Selfie.
<http://www.larousse.fr/dictionnaires/francais/selfie> (dernière consultation le 9 octobre 2019).

[826] Crim., 16 mars 2016, n° 15-82.676 : *JCP* G 2016, 658, note J.-C. SAINT-PAU ; *Dr. pén.* 2016, comm. 73, obs. P. CONTE ; *D.* 2016 p. 935, note A. SERINET ; *RSC* 2016, p. 96, obs. J. FRANCILLON ; *AJ Pénal* 2016, p. 268 note J.-B. Thierry ; *Dalloz IP/IT* 2016, p. 321. Obs. G. DESGENS-PASANAU. V. *supra* n° 263.

l'enregistrement ou le document soit obtenu « *avec le consentement exprès ou présumé de la personne ou par elle-même* ». Cette précision au sein du champ de l'incrimination créée alors une différence majeure avec la protection pénale préexistante de la vie privée. La prise en compte du consentement est ici transférée à l'étape de la diffusion de « *tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel* ». La présente infraction admet donc la possibilité du consentement initial de la victime à la prise d'image ou de paroles puis l'absence de consentement à sa diffusion[827]. L'article 226-2-1 alinéa second se présente en rupture avec les infractions précédentes qui exigeaient l'absence de consentement initial de la victime alors que la nouvelle infraction prévoit, à l'inverse, la présence d'un tel consentement. Ce nouveau texte représente dès lors une infraction autonome par rapport au délit de l'article 226-2 du Code pénal. Cette autonomie est cependant restreinte aux paroles et images « *à caractère sexuel* », faisant de cette infraction également une infraction spéciale « *à la fois divergente et plus restreinte que celle qui en est le modèle* »[828].

303. Absence de référence à la nature du lieu. En outre, si le second alinéa de l'article 226-2-1 ne fait pas explicitement référence à la nature du lieu dans lequel est perpétrée l'atteinte initiale on pourrait être incité à conclure que la nature du lieu est indifférente à la réalisation de l'infraction, cette dernière étant absente des éléments constitutifs. Cette déduction serait cependant imparfaite voire, manquerait de rigueur du fait que l'article 226-2-1 alinéa 2nd renvoie « *aux actes prévues à l'article 226-1 du Code pénal* ». Lesdits actes faisant référence d'une part au fait de capter, d'enregistrer ou transmettre les paroles prononcées à titre privé ou confidentiel (Article 226-1, 1°) et d'autre part, au fait d'enregistrer ou transmettre l'image d'une personne se trouvant dans un lieu privé (Article 226-1, 2°). Ainsi en vertu du principe d'interprétation stricte de la loi pénale, l'article 226-2-1 alinéa 2 du Code pénal viserait soit les paroles prononcées à titre privé ou confidentiel soit l'image de la personne prise dans un lieu privé. Partant, la répression de la diffusion de l'image à caractère sexuel d'une personne prise dans un lieu public avec son consentement initial ne pourrait s'envisager que sous l'empire de l'article 226-2-1 alinéa 1er au titre d'une « *circonstance aggravante constitutive* »[829].

[827] La notion de consentement peut en l'occurrence s'analyser à la lumière des prescriptions de l'article 226-1 alinéa 2nd du Code pénal selon lequel : « *lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé* ».
[828] S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *op. cit*.
[829] *Ibid*.

304. L'autonomie de l'élément moral. La distanciation de la nouvelle infraction issue de la loi pour la République numérique par rapport aux articles 226-1 et 226-2 du Code pénal s'observe également concernant l'élément moral. Ce dernier consiste en effet dans la conscience et la volonté pour l'auteur de l'infraction de diffuser l'image ou la parole à caractère sexuel d'autrui. Suivant la structure de la nouvelle infraction, l'élément moral se détache de la prise d'image ou de la captation de parole initiale, l'intention de l'auteur devenant même complètement indifférente à cette dernière. Plus encore, aucune correspondance ne peut être trouvée entre l'élément moral du nouvel article 226-2-1 et l'élément moral de l'article 226-1 dans la mesure où les conditions relatives au consentement initial de la victime sont radicalement opposées. Le législateur a par ailleurs choisi de ne pas préciser dans le texte d'incrimination que la parole ou l'image à caractère sexuel serait diffusée « *dans l'intention de nuire* » ou plus précisément « *dans l'intention de créer une détresse émotionnelle* » chez la victime. Ainsi, pour qualifier l'infraction il n'est pas nécessaire de démontrer l'existence de ce dol spécial. À ce titre, le terme de « *revenge porn* » ne correspond pas entièrement au nouveau délit dans la mesure où aucun mobile spécifique n'est requis. Le mot « *revenge* » ou « *vengeance* » sous-tend l'idée qu'un mobile particulier animerait l'auteur de la diffusion répréhensible. Cependant, à la lecture de la nouvelle infraction, « *peu importent les raisons qui ont animé le prévenu : vengeance, volonté d'humilier, moqueries, chantage... Seuls comptent l'acte de diffusion lui-même et la nature sexuelle de son support* »[830].

305. L'incohérence des régimes de responsabilité au sein de la protection pénale de la vie privée. Enfin, le délit prévu au second alinéa de l'article 226-2-1 du Code pénal s'applique aussi bien aux supports de diffusion au public en ligne (à l'internet) qu'aux supports de communication traditionnels (écriteaux, affiches, …). Cependant aucune précision n'est faite quant aux règles applicables en matière de responsabilité alors que l'article 226-2 du Code pénal précise « *lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables* ». Par cette absence de référence, le législateur créé une différence de régime entre l'article 226-2 et l'article 226-2-1 du Code pénal alors que ces deux textes protègent l'atteinte à l'intimité de la vie privée au moyen d'une diffusion. Il aurait été pourtant judicieux d'appliquer un régime similaire à ces infractions.

[830] A. SERINET, « L'instauration d'une répression des atteintes à l'intimité sexuelle par la loi pour une république numérique », *op. cit*.

Au final, au-delà d'être multiples, les imperfections issues de la rédaction du nouvel article 226-2-1 du Code pénal manifestent une incompréhension des véritables enjeux juridiques intrinsèques à la création d'une telle incrimination et nécessitent dès lors un travail de réécriture de l'infraction.

2) Une nécessaire réécriture de l'infraction

306. Une nécessaire infraction spéciale et autonome. Au vu des précédentes observations, la rédaction actuelle de l'infraction de l'article 226-2-1 du Code pénal est critiquable et sa réécriture nécessaire.

307. Proposition n° 1 : réécriture de l'article 226-2-1. Il apparaît de prime abord envisageable de proposer une réécriture de l'article 226-2-1 du Code tant sa nature juridique et son interprétation sont sources d'interrogations[831]. Dans cette optique le législateur doit proposer une nouvelle infraction spécifique et autonome. L'incrimination pourrait venir sanctionner « *le fait pour une personne de diffuser, sans son consentement, l'image, la parole ou tout contenu à caractère sexuel d'une autre personne portant atteinte à l'intimité de sa vie privée* ». Cette infraction serait autonome par rapport aux articles 226-1 et 226-2 du Code pénal, elle ne souffrirait donc pas des conditions spécifiques à chacune de ces infractions, notamment l'absence de consentement initial de la personne et l'exigence d'un lieu privé. Par ailleurs, le fait de ne pas préciser qui est à l'origine de la photographie ou de l'enregistrement initial présente un certain avantage : l'auteur de la photographie ou de l'enregistrement n'est pas nécessairement l'auteur de l'infraction. Par exemple, l'image peut résulter de la victime elle-même[832]. L'infraction pourrait aussi être retenue à l'encontre d'un hackeur qui choisirait de diffuser des images à caractère sexuel qu'il aurait auparavant usurpé à la victime. Cette solution, en se restreignant à l'intimité sexuelle, n'irait cependant pas au bout de la logique défendue selon laquelle la diffusion de l'intimité de la vie privée doit recevoir une protection

[831] Dans ce sens, Monsieur Stéphane Detraz observe que « *l'article 226-2-1 alinéa 1er, du code pénal devrait* […] *être reformulé. Ou bien la nature privée du lieu (dans lequel se trouve la personne dont l'image est dérobée) est criminologiquement indifférente, et la référence qui y faite à l'article 226-1 doit être éradiquée. Ou bien elle a au contraire son importance, et le caractère sexuel de l'image devrait soit en compenser l'absence, soit en aggraver la présence, mais alors en rendant applicables des peines distinctes suivant l'hypothèse considérée. En posant une circonstance aggravante entraînant des sanctions identiques dans les deux situations, le nouveau texte manque en somme de logique et pervertit le mécanisme de la circonstance aggravante* ». S. DETRAZ, « Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *op. cit.*, n° 19.

[832] Cette hypothèse est loin d'être anodine au regard du phénomène des *selfies* : cette Pratique s'est considérablement développée avec l'usage des réseaux sociaux et consiste à se prendre soi-même en photographie ou vidéo.

pénale égale à la captation de l'intimité de la vie privée. Seule une réécriture des articles 226-1 et 226-2 du Code pénal permettrait de satisfaire cette logique.

308. Proposition n° 2 : abrogation de l'article 226-2-1 et réécriture des articles 226-1 et 226-2 du Code pénal. Pour envisager sous un nouvel angle la protection pénale de la vie privée il paraît indispensable de réécrire les articles qui en constituent sa base à savoir les articles 226-1 et 226-2 du Code pénal. L'objectif étant d'élever à un rang de protection égal l'atteinte à l'intimité de la vie privée issue de la captation sans le consentement de la personne de son image ou de sa parole et l'atteinte à l'intimité de la vie privée issue de la diffusion sans le consentement de la personne de son image ou de sa parole. La solution reviendrait alors à consacrer dans un premier article l'atteinte à l'intimité de la vie privée résultant d'une captation fautive et dans un second article l'atteinte à l'intimité de la vie privée résultant d'une diffusion fautive. Suivant cette observation, l'ajout de la condition du consentement à l'infraction de l'article 226-2 du Code pénal semble à première vue de nature à combler les lacunes des textes répressifs actuels. Cependant, ce simple rajout à l'article 226-2 ne suffirait pas à résoudre la problématique du système de renvoie actuel. C'est pourquoi, il est nécessaire de réécrire dans son entièreté l'infraction de l'article 226-2 du Code pénal.

L'article 226-2 pourrait être rédigé comme tel : « *Est puni des mêmes peines le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :*

1° En diffusant sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En diffusant sans le consentement de la personne, l'image de celle-ci la représentant dans son intimité, et lorsque cette diffusion est de nature à troubler sa tranquillité ou à porter atteinte à son honneur ou à sa considération ».

§2. Une évolution de la protection pénale de la vie privée

309. Bien que sa rédaction demeure imparfaite, la nouvelle incrimination de l'article 226-2-1 du Code pénal traduit une extension de la protection pénale de la vie privée s'observant notamment par une superposition des protections civile et pénale de la vie privée (A). Plus encore, une telle infraction manifeste dans une certaine mesure une réception en matière pénale du droit à l'autodétermination informationnelle (B).

A. Une superposition des protections civile et pénale de la vie privée

310. Une superposition de la protection pénale et civile. La nouvelle incrimination de l'article 226-2-1 du Code pénal marque une revalorisation de la prise en compte du consentement en droit pénal et particulièrement, du consentement à la diffusion d'une image relevant de l'intimité de la personne. L'absence de consentement de la victime est en effet désormais érigée en élément constitutif de l'infraction de diffusion sans lien avec une atteinte préalable à la vie privée par immixtion[833]. En conséquence, ce texte entraîne une extension de la protection pénale de la vie privée et plus encore, démontre un rapprochement de la protection pénale et civile de la vie privée si ce n'est leur superposition.

311. La prise en compte du consentement à la diffusion en droit civil. La jurisprudence civile reconnaît de manière constante sur le fondement de l'article 9 du Code civil que la protection de la vie privée s'étend également à la diffusion d'images relevant du cercle intime. Ainsi, toute diffusion d'une telle image sans le consentement de l'intéressé est sanctionnée civilement. Dans ce sens, la Cour de cassation a précisé que « *toute personne a sur son image un droit exclusif et absolu et peut s'opposer à sa fixation, à sa reproduction, ou à son utilisation sans autorisation préalable* »[834]. En tant qu'élément du droit de la personnalité, l'image d'une personne ne saurait être fixée mais également reproduite sans son accord. En outre, les juges du fond ont précisé que si les circonstances dans lesquelles l'image a été fixée peuvent révéler un accord tacite[835], le consentement donné à la réalisation d'une photographie ne vaut pas nécessairement consentement à son utilisation[836]. Dès lors, la chambre criminelle de la Cour de cassation avait, dans son arrêt du 16 mars 2016[837], clairement marqué la différence d'interprétation en matière pénale en affirmant que « *n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement* ». L'adoption de l'article 226-2-1 marque alors un rapprochement certain entre les protections pénale et civile de la vie privée.

---

833 A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *CCE* n° 2, février 2017, étude 3 ; *Dr. pén.* 2017, n° 1, étude 1.

834 Par exemple, Civ. 2ème, 30 juin 2004, deux arrêts, n° 02-19.599 : *JCP* G 2004, II, 10160, note D. BAKOUCHE. ; V. déjà visant l'article 9 du Code civil – Civ. 1ère, 13 janvier 1998 : *Bull. civ.* 1998, I, n° 14 ; *JCP* G 1998, II, 10082, note G. LOISEAU ; *D.* 1999, p. 120, note J. RAVANAS. – Civ. 1ère, 16 juillet 1998 : *Bull. civ.* 1998, I, n° 259, *D.* 1999, p. 541, note J.-C. SAINT-PAU.

835 Civ 1ère, 4 novembre 2011, n°10-24.761 : *RLDI*, 2011, n° 77.

836 Par exemple, Paris, 1ème ch. B, 29 mai 1998 – TGI Nanterre, 1ère ch., sect. C, 26 octobre 1999.

837 Crim., 16 mars 2016, n° 15-82.676 : *JCP* G 2016, 658, note J.-C. SAINT-PAU ; *Dr. pén.* 2016, comm. 73, obs. P. CONTE ; *CCE* 2016, comm. 42 ; *D.* 2016. 935, note A. SERINET ; *RSC* 2016, p. 96, obs. J. FRANCILLON ; *AJ Pénal* 2016, p. 268, note J.-B. THIERRY ; *Dalloz IP/IT* 2016, p. 321, obs. G. DESGENS-PASANAU.

312. Une protection pénale plus restreinte. Un tel rapprochement ne doit cependant pas être intégral, la protection pénale devant demeurer plus restreinte que son homologue civil. La prise en compte du consentement à la diffusion en matière pénale ne concerne pour l'heure que les images et propos revêtant un caractère sexuel. L'extension pénale observée ne concerne donc qu'une partie limitée de l'intimité des individus à savoir, leur intimité sexuelle. Le législateur a ainsi choisi d'élargir la protection pénale de la vie privée mais uniquement sur un point particulier de l'intimité. Cette infraction marque une rupture en comparaison aux articles 226-1 et 226-2 du Code pénal qui sanctionnent l'atteinte portée à l'intimité de la vie privée sans préciser les éléments compris dans cette intimité. Cette nouvelle infraction étend et restreint donc à la fois la protection de la vie privée en faisant de l'intimité sexuelle une notion soumise à une protection accrue. La justification d'une telle protection se retrouve dans les divers évènements d'actualité qui ont révélé la carence des infractions classiques démontrée plus tôt[838]. Cependant, le législateur aurait dû porter un regard plus global sur la nouvelle relation de notre société avec la notion de vie privée plutôt que de se focaliser sur des faits divers, certes non isolés, mais attirant le regard en raison du caractère sexuel de l'atteinte. Les nouvelles formes de surexposition consentie ou non des individus sur les réseaux sociaux en ligne justifient que le droit pénal soit plus soucieux de la protection de la vie privée de nos jours que dans les années 1970[839]. La diffusion sans le consentement de l'intimité présente aujourd'hui, en raison de la facilité à recueillir une audience massive sur les sites de réseaux sociaux, un degré de gravité similaire voire supérieur à la captation sans le consentement de l'intimité, autrefois unique objet de sanction en matière pénale. Le choix de cantonner l'extension de la protection pénale de la vie privée uniquement aux images ou propos à caractère sexuel paraît alors critiquable. Nombre de contenus diffusés sans le consentement des individus peuvent relever de leur intimité sans pour autant revêtir un caractère sexuel, c'est le cas notamment de l'intimité familiale ou encore de l'intimité du malade[840]. Il n'est pas pour autant question d'élargir le domaine de compétence pénale de manière excessive. Une superposition totale des champs d'application pénal et civil pourrait avoir un effet néfaste notamment sur le caractère dissuasif et sanctionnateur du droit pénal. Ce dernier doit en effet demeurer un droit plus sévère au champ d'application plus restreint que le droit civil. Il est donc de bon sens de préciser que les intérêts privés protégés par le droit civil ne doivent pas correspondre à l'intérêt public protégé par le droit pénal. Il paraît néanmoins

[838] V. *supra* n° 242 et suiv.
[839] A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *op. cit.*
[840] V. *supra* n° 286.

légitime que la protection contre la diffusion non consentie de l'intimité (vue dans son ensemble) soit pénalisée au même titre que l'immixtion non consentie dans la vie privée.

B. Une réception en matière pénale du droit à l'autodétermination informationnelle

313. Au-delà d'une superposition des protections civile et pénale de la vie privée, l'adoption de l'article 226-2-1 du Code pénal marque la volonté du droit pénal de sanctionner une utilisation non consentie d'éléments relevant de la vie privée d'une personne. Cette évolution législative s'inscrit alors dans la lignée du développement d'un droit à l'autodétermination informationnelle. Après avoir mis en évidence l'émergence de ce droit (1), sa réception en droit pénal sera observée (2).

1) L'émergence d'un droit à l'autodétermination informationnelle

314. Une conception revendicatrice du droit au respect de la vie privée. La vie privée s'entend à l'origine comme un concept protecteur assurant un droit au respect de l'autre, mais plus récemment, certains auteurs ont développé une interprétation selon laquelle la vie privée serait un droit également à visée revendicatrice devenant un droit subjectif[841]. La vie privée doit être considérée comme le droit à diriger sa vie comme on l'entend, ce qui implique le droit de disposer de son intimité selon ses propres choix. Le droit au respect de la vie privée se muerait alors en un « *droit à la vie privée* ». Ce « *droit à* » n'aurait plus pour objet de faire respecter son individualité mais de se fonder sur cette dernière pour « *opposer à la société son choix de vie* »[842]. Selon Madame Delphine Chauvet : « *le "droit à" la vie privée se distingue du droit au respect de la vie privée dans la mesure où il ne convient plus de s'ériger contre une atteinte à la vie privée. Il s'agit pour la personne de demander, sur le fondement de sa vie privée, que le droit lui confère un avantage* »[843]. Cette conception dualiste de la vie privée fait écho aux pratiques rencontrées sur les sites de réseaux sociaux et au développement de la personnalité sociale des individus dans le monde numérique. C'est ainsi qu'un pouvoir exclusif de contrôle sur les éléments relevant de sa vie privée, notamment ses données à caractère personnel, est aujourd'hui revendiqué.

315. Le droit à l'autodétermination, élément du « *droit à* » la vie privée. Le droit à l'autodétermination de l'individu s'inscrit dans cette conception revendicatrice du droit au

[841] Se dit d'un droit subjectif, un droit qui « *appartient à une personne* ». Association H. CAPITANT, *Vocabulaire juridique*, G. CORNU (dir.), PUF, 12ème éd., 2018, *V°* Subjectif/ive.
[842] B. BEIGNIER, « Vie privée et vie publique », Arch. phil. droit, 1997, n° 41, p. 163.
[843] D. CHAUVET, *Vie privée, étude de droit privé*, Thèse Université Paris-Sud, 2014, p. 421, n° 548.

respect de la vie privée. Il s'agit d'assurer à l'individu un droit à l'épanouissement personnel lui permettant d'affirmer sa personnalité. La Cour européenne des droits de l'homme se prononce en faveur d'une interprétation large de la notion de vie privée afin d'y inclure son aspect offensif. Selon elle, la vie privée comprend le droit au développement personnel et le droit à l'autodétermination des individus. À ce titre, la Cour affirme de manière récurrente au sein d'une jurisprudence étoffée que la notion de vie privée « *recouvre l'intégrité physique et morale de la personne et englobe parfois des aspects de l'identité physique et sociale d'un individu, dont le droit de nouer et de développer des relations avec ses semblables, le droit au "développement personnel" ou le droit à l'autodétermination en tant que tel* »[844]. Le raisonnement du juge de Strasbourg relie directement l'idée du droit à l'autonomie personnelle à l'article 8 de la convention européenne des droits de l'homme protégeant le « *droit au respect de la vie privée et familiale* »[845]. Le juge français s'est également prononcé en faveur d'une conception plus offensive du concept de vie privée en lui permettant d'en faire un droit source de revendications. Un arrêt de l'assemblée plénière de la Cour de cassation du 11 décembre 1992[846] a ainsi reconnu, aux visas de l'article 9 du Code civil et de l'article 8 de la Convention européenne des droits de l'homme, la possibilité pour les personnes transsexuelles de demander le changement de la mention de leur sexe sur les registres de l'état civil. En outre, le droit à l'autodétermination peut se rencontrer dans la jurisprudence sous diverses formulations telles que « *le droit au développement personnel* », « *le droit à l'autonomie personnelle* », « *le droit à l'épanouissement personnel* ». Ces différentes formulations regroupent cependant toutes une même réalité et doivent s'entendre comme constituant un même principe[847]. L'usage moderne d'internet et des nouveaux moyens de communication que représentent les réseaux sociaux en ligne constituent un nouvel enjeu

---

[844] CEDH, *Obst c. Allemagne*, 23 septembre 2010, n° 425/03, §53 : *RDT* 2011, p. 45, note J. COUARD ; *Légipresse* 2011, n° 279, p. 63, obs. G. LOISEAU ; *RTDH* 2011, p. 375, note G. De BECO –CEDH, *Niemietz c. Allemagne*, 16 décembre 1992, §29 : *D.* 1993, p. 386, obs. J.-F. RENUCCI ; *JCP* G 1993, I, 3654, obs. F. SUDRE – CEDH, *Burghartz c. Suisse*, 22 février 1994, §24 *: RTD Civ.* 1994, p. 563, obs. J. HAUSER ; *JCP* 1995, I, 3823, chron. F. SUDRE ; *D.* 1995, p. 5, note J.-P. MARGUENAUD ; *RTDH* 1995, p. 53, obs. P. GEORGIN – CEDH, *Botta c. Italie*, 24 février 1998, §32 : *RTDH* 1999, p. 600, obs. B. MAURER ; *D.* 1998, p. 371, N. FRICERO – CEDH, *Pretty c. R.-U.*, 29 avril 2002, n° 2346/02, §61 : *RSC* 2002, p. 645, obs. F. MASSIAS ; *RTDH* 2003, p. 71, note O. De SCHUTTER – CEDH, *Polanco Torres et Movilla Polanco c. Espagne*, 21 septembre 2010, n° 34147/06, §40 : *Légipresse* 2011, n° 279, p. 63, obs. G. LOISEAU.

[845] Selon la CEDH : « *l'article 8 de la Convention protège le droit à l'épanouissement personnel, que ce soit sous la forme du développement personnel ou sous l'aspect de l'autonomie personnelle* ». V. CEDH, *Bigaeva c. Grèce*, 28 mai 2009, n° 26713/05 §22 : *JCP* G 2009, 143, n° 16, obs. F. SUDRE.

[846] Cass. ass. plén., 11 décembre 1992, n° 91-11.900 : *JCP* G 1993, II, 21991, concl. M. JEOL et note G. MEMETEAU ; *RTD Civ.* 1993, p. 99, obs. J. HAUSER.

[847] V. en ce sens D. CHAUVET selon laquelle : « *le droit au développement personnel et le droit à l'autodétermination ne constituent pas des droits distincts* », *in* : *Vie privée, étude de droit privé*, Thèse Université Paris-Sud, 2014, p. 292, n° 350 ; V. également F. SUDRE, *Droit européen et international des droits de l'homme*, 10ème éd., PUF, coll. « Droit fondamental », 2011, p. 529, n° 307.

pour le droit à l'autodétermination, celui-ci impliquerait dorénavant la nécessité pour les individus de maîtriser les éléments numériques de leur vie privée représentés par leurs données à caractère personnel.

316. L'apparition de la notion d'autodétermination informationnelle. Le droit à l'autodétermination informationnelle est apparu dans un premier temps au niveau jurisprudentiel. Le tribunal constitutionnel de Karlsruhe fut le premier à identifier cette notion dans un arrêt du 15 décembre 1983. Selon ce dernier : « *la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* »[848]. Dans cet arrêt, le juge constitutionnel allemand a dégagé des principes de dignité de l'homme et de droit au libre développement de sa personnalité un droit à *« l'autodétermination informationnelle* »[849]. Cette décision avant-gardiste consacre le pouvoir de l'individu de décider de lui-même, sur la base du concept d'autodétermination, quand et dans quelle mesure, une information relevant de sa vie privée peut être communiquée à autrui. Avec la nouvelle phase du développement de la société de la communication, ce principe devient aujourd'hui indispensable pour la défense des libertés individuelles. Le juge constitutionnel allemand a formulé un tel principe en constatant que « *si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est limitée* »[850]. La jurisprudence allemande a par la suite réaffirmé cette notion soit de manière implicite[851], soit de manière explicite[852]. Ce principe a également été défendu par la Cour constitutionnelle hongroise qui a reconnu dès 1991 que le droit à la protection des données personnelles englobe « *le contrôle et l'utilisation des données personnelles* »[853].

317. L'affirmation institutionnelle du droit à l'autodétermination informationnelle. Le droit à l'autodétermination informationnelle a été défendu devant plusieurs institutions dans

[848] Tribunal constitutionnel de Karlsruhe, 15 décembre 1983, V. C. GREWE, « Allemagne. Constitution et secret de la vie privée ». AIJC 2000, p. 147.
[849] En allemand : « *Informationnelle Selbstbestimmung* ».
[850] Tribunal constitutionnel de Karlsruhe, 15 décembre 1983 : C. GREWE, « Allemagne. Constitution et secret de la vie privée », AIJC 2000, p. 147.
[851] Cour constitutionnelle fédérale allemande (Bundesverfassungsgerichsthof), 4 avril 2006, BverfGE, 1 BvR 518/02, BverfG, 1BvR 2027/02, 23 octobre 2006 : M. FROMONT, « Jurisprudence constitutionnelle de la République fédérale d'Allemagne (2008) », Chronique de jurisprudence, RDP, 2009, n° 6, pp. 1726-1727.
[852] Cour constitutionnelle fédérale allemande (Bundesverfassungsgerichsthof), 24 avril 2013, JZ 2013, p. 621, V. M. FROMONT, « République fédérale d'Allemagne : la jurisprudence constitutionnelle en 2013 », RDP, 2014, n° 4, pp. 1119-1122.
[853] Cour constitutionnelle hongroise, 9 avril 1991, Décision n° 15/1991, IV. 13, AB, Recueil ABH 1991, 40, *in* P. BON et D. MAUS, *Les grandes décisions des cours constitutionnelles européennes*, Dalloz, 2008, pp. 269-270.

divers rapports. Le Conseil de l'Europe a consacré en 2004 un rapport spécifique à la question dans lequel il identifiait ce droit comme un nouvel enjeu issu du développement technologique des réseaux et services de communication électronique[854]. En France, plusieurs rapports ont prôné l'existence d'un tel droit. C'est le cas du rapport « *Le numérique et les droits fondamentaux* » du Conseil d'État qui définit le droit à l'autodétermination informationnelle comme « *le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel* »[855]. Il s'agit également du rapport « *Numérique et libertés : un nouvel âge démocratique* » remis à l'assemblée nationale en octobre 2015 et prônant la consécration d'un « *droit à l'autodétermination informationnelle des individus à l'ère numérique* »[856].

318. L'affirmation doctrinale du droit à l'autodétermination informationnelle. Dans la continuité des institutions, la doctrine affirme également sa volonté de voir reconnaître un tel principe. Certains auteurs emploient le terme « *droit à conserver la maîtrise de ses données personnelles* » qu'ils définissent comme « *l'aptitude de la personne fichée à maîtriser, dans une certaine mesure, les informations personnelles la concernant* »[857]. Selon Monsieur Philip E. Agre, la protection de la vie privée et la protection des données personnelles suggèrent respectivement un contrôle de l'individu de l'ampleur et de la manière dont certains aspects de son intimité sont exposés au public, mais aussi, la possibilité pour l'individu de construire sa propre personnalité à l'abri de contraintes excessives[858]. Le droit à l'autodétermination informationnelle permettrait à l'individu de demeurer libre de conduire son existence alors même qu'internet incite l'individu à laisser de plus en plus de traces numériques. Deux versants peuvent être distingués dans ce droit : le premier renvoie à la possibilité pour l'individu de maîtriser les informations (ou données) divulguées à son encontre ; le second, plus en amont, impliquerait l'exigence du consentement de l'individu avant tout usage d'une donnée à caractère personnel, surtout lorsque cette dernière relèverait de son intimité. Une fois ce droit énoncé il faut alors s'attacher à en préciser sa valeur.

---

[854] Conseil de l'Europe, *rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications - L'autodétermination informationnelle à l'ère de l'Internet*, Éléments de réflexion sur la Convention n° 108 destinés au travail futur du Comité consultatif (T-PD), Strasbourg, le 18 novembre 2004.
[855] Rapport Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 269.
[856] C. PAUL et C. FERAL-SCHUHL, *Numérique et libertés : un nouvel âge démocratique*, Rapport n° 3119, déposé le 9 octobre 2015, mis en ligne le 13 octobre 2015, p. 133.
[857] N. OCHOA, *Le droit des données personnelles, une police administrative spéciale*, Thèse Univ., Paris 1 Panthéon-Sorbonne, 2014, p. 474.
[858] P. E. AGRE, M. ROTENBERG, « technology and privacy. The New Landsacpe », *MIT Press*, 1998, p. 3.

319. Un principe directeur. La seule affirmation d'un tel droit n'a pas pour conséquence de le rendre effectif. Le droit à l'autodétermination informationnelle ne se suffit pas à lui-même au risque de devenir un instrument de protection inefficace. Il doit en réalité servir de pilote à des outils de protection déterminés dans la mesure où il donnerait sens à ces droits. Ce droit à l'autodétermination ne doit donc pas être saisi comme un simple droit supplémentaire s'ajoutant à des droits préexistants mais davantage « *comme un principe donnant sens à tous ces droits, ceux-ci tendant à le garantir et devant être interprétés et mis en œuvre à la lumière de cette formalité* »[859]. Un rapport a ainsi préconisé de consacrer le droit à l'autodétermination informationnelle comme principe directeur des autres droits reconnus par la loi « *informatique et liberté* »[860]. En écho à cette proposition, la loi n° 2016-1321 du 7 octobre 2016[861] est venue insérer un nouvel alinéa à l'article 1er de la loi « *informatique et liberté* » selon lequel : « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ». Sans le mentionner directement, cet ajout conforte le principe d'autodétermination informationnelle en le plaçant en tête de la loi informatique et liberté tel un principe directeur. Sa portée doit être cependant nuancée dans la mesure où le droit de tout individu à maîtriser ses données demeure soumis aux « *conditions fixées par la présente loi* », ce qui restreint automatiquement l'autonomie du principe énoncé. Dans cette même dynamique, le règlement général sur la protection des données du 27 avril 2016[862] a mentionné dans son premier considérant que : « *toute personne a droit à la protection des données à caractère personnel la concernant* ». Cette précision n'est toutefois pas de nature à ériger au rang de principe défendu le droit à l'autodétermination informationnelle. Plus encore, la doctrine a relevé « *un silence assourdissant du règlement sur l'autodétermination informationnelle* »[863].

320. Un principe fondamental attaché à la personnalité. Outre son caractère directeur, le principe d'autodétermination informationnelle sous-tend un rattachement aux droits de la personnalité et non au droit de propriété. Consacrer un tel principe en lien étroit avec les

[859] Rapport Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 26, proposition n° 1.
[860] C. PAUL et C. FERAL-SCHUHL, *Numérique et libertés : un nouvel âge démocratique*, Rapport n° 3119, déposé le 9 octobre 2015, mis en ligne le 13 octobre 2015, p. 134.
[861] L. n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n° 0235, 8 octobre 2016, texte n° 1.
[862] Règl. (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la dir. 95/46/CE (règlement général sur la protection des données dit RGPD).
[863] N. MARTIAL-BRAZ, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017 p. 253.

données à caractère personnel traduit la volonté de détacher ces dernières de la notion de propriété. La donnée, même si elle est une chose, ne serait alors pas un élément du patrimoine de l'individu mais un élément relevant de sa personnalité. Ce raisonnement a déjà été admis en doctrine notamment selon le Professeur Judith Rochfeld qui observe que : « *des évolutions contemporaines poussent à relativiser cette distinction* [la distinction chose-personne] *et à réfléchir aux frontières de la notion de personne* […]. *C'est ce qui explique qu'aujourd'hui des revendications visant à ce que certains éléments qualifiés de choses soient élevés au rang de personne* »[864]. Le Conseil d'État a d'ailleurs recommandé que la protection des données soit envisagée comme un droit à l'autodétermination, et donc comme un droit de la personnalité, plutôt qu'un droit de propriété[865]. Cette solution est la manière la plus efficace d'assurer à l'individu un droit intangible sur ses données : « *un droit de propriété implique un droit d'être dépossédé, alors qu'un droit de la personnalité est inaliénable* »[866]. Allant au bout de cette logique, certains auteurs proposent d'ériger le principe d'autodétermination informationnelle, et plus largement le principe d'autodétermination comme principe fondamental à valeur constitutionnelle, gouvernant l'ensemble des droits de la personnalité et permettant de raviver l'autonomie délibérative et réflective des individus[867]. Dans cette logique le règlement européen sur la protection des données du 27 avril 2016 vient préciser dans son premier considérant que : « *la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental* »[868]. Ce nouveau règlement confirme alors la conception « *personnaliste* » de la notion de donnée à caractère personnel et ainsi son rattachement aux droits de la personnalité plutôt qu'au droit de propriété[869].

---

[864] J. ROCHFELD, *Les grandes notions du droit privé*, PUF, 2013, p. 34.

[865] Rapport Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 26, proposition n° 1.

[866] CNIL, *Vie privée à l'horizon 2020*, Cahier IP, innovation et prospective, n° 1, p. 55.

[867] Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. », *in* K. BENYEKHLEF & P. TRUDEL (dir.), *État de droit et virtualité*, Montréal, Thémis, 2009, p. 161.

[868] Règl. (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la dir. 95/46/CE (règlement général sur la protection des données).

[869] Dans un commentaire du nouveau règlement européen sur la protection des données, Frédérique Lesaulnier observait que : « *Les données personnelles sont des attributs de la personnes humaine, des émanations de celle-ci dont elles portent l'empreinte, des " choses personnalisées" en quelque sorte qui participent de son rayonnement. Sans contenir toute sa personne, le corpus des données à caractère personnel qui la concernent participe à la plénitude de son animus. C'est pourquoi elles doivent être soumises à un régime protecteur* ». F. LESAULNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz, IP/IT* 2016, p. 573.

2) Une réception d'un tel droit en matière pénale

321. Selon le Professeur Agathe Lepage, la pénalisation de l'absence de consentement à la diffusion d'images à caractère sexuel s'inscrit dans la montée en puissance contemporaine du principe « *d'autodétermination informationnelle* »[870]. Au plan pénal, cela se manifeste par la sanction de la diffusion d'informations relevant de l'intimité sans le consentement de la personne concernée. Il ne s'agit pas d'une maîtrise en amont de ses données, c'est-à-dire avant leur diffusion, mais d'une maîtrise en aval, après leur diffusion. Ceci s'explique par le caractère sanctionnateur et non préventif du droit pénal. Cette nouvelle infraction reconnaît ainsi une meilleure maîtrise pour l'individu de ses données, ou plus précisément, sanctionne l'absence de prise en compte du consentement de l'individu dans l'utilisation de ses données. Ce nouveau délit traduit alors dans une certaine mesure, la réception en matière pénale du droit à l'autodétermination informationnelle. En l'occurrence, le droit pénal choisit de protéger la divulgation non consentie d'éléments de la vie privée dès lors qu'ils présentent la victime dans son intimité sexuelle. Le Professeur Agathe Lepage remaque à ce titre qu'en incriminant la diffusion *per se* le nouvel article 226-2-1 marque un changement de paradigme dans l'appréhension pénale de la vie privée[871]. On constate alors un élargissement de la protection de la valeur sociale protégée d'intimité qui concerne également la diffusion de cette dernière.

322. Conclusion de la Section 2. Du point de vue de la technique juridique, la nouvelle incrimination prévue à l'article 226-2-1 du Code pénal doit faire l'objet de vives critiques. Ce nouveau texte rompt en effet avec la protection pénale uniforme de la vie privée, mais surtout, il introduit en raison de sa maladresse rédactionnelle de nombreuses incertitudes quant à son interprétation. Il est dès lors proposé d'abroger ce nouvel article et de réécrire les incriminations des articles 226-1 et 226-2 du Code pénal afin de rétablir une plus grande clarté dans la protection pénale de l'intimité. Toutefois, considération faite de ces critiques, il convient par ailleurs de souligner la légitimité de cette nouvelle incrimination au vu des nouvelles formes d'atteinte à l'intimité permises par les sites de réseaux sociaux. Cette nouvelle incrimination matérialise alors une évolution de la protection pénale de la vie privée qui vient un peu plus se rapprocher de la protection consacrée par le droit civil. Cette évolution législative intervient également dans le contexte de l'essor du principe

[870] A. LEPAGE, « L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *CCE* n° 2, février 2017, étude 3 ; *Dr. pén.* 2017, n° 1, étude 1.
[871] *Ibid.*

d’autodétermination informationnelle qui justifie une plus grande prise en considération du consentement de l’individu dans la diffusion des données à caractère personnel le concernant. Partant, ce nouveau délit peut être observé comme une forme de réception en droit pénal du droit à l’autodétermination informationnelle.

Conclusion du Chapitre 2

323. En matière pénale, l'intimité a toujours été l'élément central définissant la vie privée, cependant à l'heure des sites de réseaux sociaux cette intimité subit de profonds changements. Il n'est plus uniquement question de protéger contre une immixtion dans l'intimité mais davantage de maîtriser la divulgation de l'intimité qui est devenue une pratique sociale courante. Sur ce point, le principe d'autodétermination informationnelle répond aux nouveaux enjeux de protection de la vie privée et notamment de la défense de la conception offensive de « *droit à* » la vie privée. Ce mouvement juridique qui dépasse le simple cadre du droit pénal investit davantage le registre des droits fondamentaux. Le délit de l'article 226-2-1 du Code pénal traduit en l'occurrence de manière indirecte une certaine réception du droit à l'autodétermination informationnelle au sein du droit pénal. Le législateur n'a cependant pas su prendre la mesure véritable de l'enjeu juridique sous-jacent au délit de l'article 226-2-1 du Code pénal. Il en résulte une incrimination insatisfaisante et floue qui doit être revue, sinon abrogée. Il est ainsi suggéré de créer une infraction entièrement autonome d'atteinte à la vie privée par la diffusion non consentie d'éléments relevant de l'intimité. Le juge pénal devra alors bien circonscrire la notion d'intimité et en faire une notion pénale distincte de la notion civile et respectueuse du principe de légalité.

Conclusion du Titre 2

324. L'usage massif des sites de réseaux sociaux a initié une évolution de la protection pénale de la vie privée allant dans le sens général d'une extension de son champ d'application. Les carences mises en évidence par le principe d'interprétation stricte de la loi pénale sont la conséquence de la numérisation de la société et notamment de l'explosion des échanges intra personnels sur les sites de réseaux sociaux. Ces transformations sont de surcroît solidement ancrées dans les usages et suffisamment durables pour impacter en profondeur le droit et particulièrement le droit au respect de la vie privée. Ce dernier a dû en conséquence s'adapter à l'environnement des réseaux sociaux en ligne y compris sur le plan pénal. La création des nouvelles infractions des articles 226-4-1 et 226-2-1 du Code pénal vient concrétiser les évolutions constatées. Cependant, ces incriminations donnent différents niveaux de satisfaction. Le délit d'usurpation d'identité numérique de l'article 226-4-1 réalise un apport nécessaire à la protection de l'identité en l'érigeant de manière autonome en tant que droit de la personnalité. Le risque provient en réalité de la définition trop large de l'identité numérique suggérée par le texte. Le travail consiste alors pour le juge à circonscrire cette notion dans un cadre pénal strict de manière à ce que l'identité, y compris dans ces manifestations à l'échelle numérique, soit une valeur sociale protégée à part entière du droit pénal. De la même manière, le délit de l'article 226-2-1 semble établir un apport essentiel à la protection pénale de la vie privée, et particulièrement de l'intimité, mais les imperfections dans sa rédaction et sa limitation à l'intimité sexuelle de la victime en font un délit incomplet qui ne prend pas la mesure de ses propres enjeux. Il est en conséquence nécessaire d'abroger le délit de l'article 226-2-1 du Code pénal et d'envisager la réécriture de l'article 226-2 pour arriver à un système de protection satisfaisant de l'intimité c'est-à-dire, un système de protection mettant sur un même niveau d'égalité la captation non consentie de l'intimité et la diffusion non consentie de cette dernière.

Conclusion de la Partie 1

325. Des incriminations préexistantes adéquates. Les réseaux sociaux constituent un nouvel espace d'atteinte dont le droit pénal a su se saisir à des degrés diverses. Les incriminations se sont montrées dans certains cas parfaitement adaptées aux comportements permis par ces sites à l'image des délits de presse et des nombreuses incriminations classiques qui peuvent parfaitement s'appliquer dans cet environnement numérique en raison de leur neutralité sur le plan technologique. Les sites de réseaux sociaux constituent en outre un bien, objet d'une protection spécifique par les articles 323-1 et suivants du Code pénal en tant que système de traitement automatisé de données. Il peut alors être conclu que les spécificités techniques de ces sites s'accordent de manière générale aux définitions pénales préexistantes. Certaines adaptations ont davantage révélé une volonté de la part du législateur d'intensifier la répression de certains comportements plutôt que de combler un véritable vide juridique. La réaction à ces carences conjoncturelles a dans certains cas généré des incriminations redondantes au regard de celles préexistantes ou, plus grave encore, des textes entrant en contradiction avec certains droits et libertés fondamentales encadrant la répression. Ainsi, le délit de consultation habituelle de sites terroristes s'est vu censurer à deux reprises par le Conseil constitutionnel en raison notamment du non-respect du principe de nécessité des délits et des peines.

326. Un mouvement d'adaptation justifié. Toutefois, les comportements rencontrés sur les sites de réseaux sociaux ont mis en évidence des carences structurelles au sein des incriminations préexistantes justifiant une adaptation du dispositif pénal. Plus précisément, les sites de réseaux sociaux ont révélé au moyen du principe d'interprétation stricte de la loi pénale deux carences dans le corpus des incriminations du droit pénal ayant abouti à l'adoption de nouvelles incriminations. L'article 226-4-1 vient protéger de manière autonome l'identité des individus, y compris à l'échelle numérique, alors que les incriminations préexistantes restreignaient la protection pénale à la seule identité civile de l'individu ou ne permettait qu'une protection de l'usage frauduleux de l'identité. De même, l'article 226-2-1 du Code pénal marque une profonde mutation de la protection pénale de la vie privée en sanctionnant de manière autonome la diffusion non consentie de l'intimité d'une personne s'apparentant alors à une réception en matière pénale du droit à l'autodétermination informationnelle.

Partie 2 – L’adaptation de la répression aux réseaux sociaux en ligne

327. L’effectivité de répression pénale. Les sites de réseaux sociaux ne se limitent pas à générer de nouveaux comportements qui suscitent une adaptation, voire la création de nouvelles incriminations, leur usage engendre également de nouvelles problématiques concernant la répression des atteintes observées. En l’occurrence, les sites de réseaux sociaux agissent sur les voies répressives traditionnelles qui doivent s’adapter à l’influence de ces nouveaux moyens de communication. Cette affirmation s’observe particulièrement à l’égard des systèmes de responsabilité pénale applicables aux différents acteurs des réseaux sociaux en ligne à savoir d’un côté les opérateurs des réseaux sociaux et de l’autre leurs utilisateurs. Ainsi, tant le régime de responsabilité pénale de droit commun que celui applicable aux hébergeurs ou aux éditeurs de services révèlent un manque d’adaptation des règles juridiques aux nouveaux environnements créés par les sites de réseaux sociaux. Ces carences conduisent à un manque d’effectivité de la loi pénale en particulier concernant la répression des infractions de presse. Le développement s’attachera alors à démontrer dans un premier temps l’inadéquation des règles de responsabilité pénale aux acteurs des réseaux sociaux en ligne (**Titre 1**).

328. La régulation en complément de la répression. L’inadéquation du système répressif qui résulte de son incapacité à assurer une sanction effective des comportements commis sur les réseaux sociaux en ligne, amène à repenser les moyens de réponses aux infractions à l’aune de ces nouveaux moyens de communication. En l’occurrence, le recours à la voie judiciaire ne doit plus être pensé comme l’unique moyen de réponse aux infractions commises sur les sites de réseaux sociaux. Une régulation des contenus diffusés sous le contrôle d’une autorité administrative permet d’apporter un traitement complémentaire aux comportements délictueux, en particulier à l’égard des abus de la liberté d’expression. Il faut dès lors distinguer les rôles respectifs de la répression et de la régulation, l’une venant sanctionner l’auteur d’une infraction, l’autre faisant cesser le trouble à l’ordre public résultant de la publication de propos délictueux. Sur ce point, le droit pénal doit s’adapter par la création

d’un nouveau cadre juridique applicable aux opérateurs des réseaux sociaux. Le mouvement d’adaptation revient donc en l’occurrence à une évolution de la réponse aux infractions (**titre 2**).

Titre 1 – L'inadéquation des règles de responsabilité pénale aux acteurs des réseaux sociaux en ligne

329. Les règles de responsabilité applicables aux différents acteurs des réseaux sociaux. L'ensemble des acteurs des réseaux sociaux en ligne ont vocation à engager leur responsabilité pénale et à devenir sujets de la répression. Cela concerne autant leurs utilisateurs que leurs dirigeants qui exploitent ces réseaux de communication et qui seront qualifiés à ce titre d'opérateurs[872]. Sur ce point, le développement de l'outil internet dans la réalisation de nombreuses infractions a contraint le législateur à mettre en place des régimes de responsabilité pénale spécifiques à ces derniers. À ce titre, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[873] prévoit des règles de responsabilité spécifiques qui se conjuguent avec les mécanismes de responsabilité déjà existants à savoir, les règles de responsabilité pénale de droit commun et de droit pénal spécial de la presse[874]. En conséquence, sur les sites de réseaux sociaux, une multitude d'acteurs peut engager sa responsabilité pénale sous divers fondements. Par ailleurs, la mise en œuvre de la responsabilité pénale est différente en fonction du statut juridique propre à chaque acteur du réseau social. Ainsi, il est nécessaire en premier lieu de déterminer le statut juridique de ces différents acteurs allant des simples utilisateurs aux opérateurs du réseau social. En l'occurrence, internet se divise en deux principales catégories : d'un côté les prestataires techniques (fournisseurs d'accès à internet et hébergeurs), de l'autre, les éditeurs de services. Les prestataires techniques n'influent pas dans les différents contenus publiés sur internet, ils mettent à disposition des internautes soit un accès à internet, ce sont les fournisseurs d'accès à internet (FAI), soit une plateforme de stockage de divers contenus, ce sont les hébergeurs[875]. Les éditeurs de services sont quant à eux « *les personnes dont l'activité*

[872] Selon l'article L. 32, 15° du Code des postes et des communications électroniques, l'opérateur est défini comme *« toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques* ».
[873] L. n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), *JORF* n° 0143, 22 juin 2004, p. 11168.
[874] F. CHOPIN, Rép. pén. Dalloz, juillet 2013 (actualisation : avril 2018), *V°* Cybercriminalité, n° 326.
[875] LCEN, art. 6, I, 2 définit les prestataires techniques comme : « *2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en*

est d'éditer un service de communication au public en ligne »[876]. À la différence des prestataires techniques, ces derniers ont le choix et la maîtrise des contenus diffusés. Il s'agit alors de déterminer dans quelles catégories peuvent s'inscrire les différents acteurs des réseaux sociaux, ou plus précisément si l'opérateur du réseau social entre sous la qualification actuelle d'hébergeur et si les utilisateurs des réseaux sociaux sont assimilables à des éditeurs de services.

330. L'inadéquation des règles de responsabilité aux acteurs des réseaux sociaux. Cette analyse amènera surtout à déterminer si les règles de responsabilité de droit commun et celles propres à internet permettent une répression satisfaisante des comportements issus des sites de réseaux sociaux. En effet, les spécificités de ces sites incitent à nuancer la pertinence des règles de responsabilité particulières qui leur sont applicables. Ces règles de responsabilité imaginées avant l'émergence des réseaux sociaux en ligne ne se trouvent plus forcément adaptées à l'environnement numérique actuel. D'un côté leurs opérateurs, en tant que prestataires techniques jouissent d'une responsabilité pénale modérée, de l'autre, leurs utilisateurs, en tant qu'éditeurs de services, se retrouvent liés à un système de responsabilité les séparant dans diverses catégories et faisant d'eux les responsables à titre principal des contenus publiés. Toutefois, les frontières entre ces différentes catégories d'acteurs se trouvent parfois injustifiées, en particulier depuis l'apparition et le développement du web interactif. Il s'agit alors d'opposer les règles déterminant la responsabilité pénale des opérateurs de réseaux sociaux aux règles déterminant la responsabilité pénale des utilisateurs de réseaux sociaux afin de révéler les limites des régimes de responsabilité qui leur sont applicables. Plus généralement, ces systèmes de responsabilité démontrent leur inadéquation aux nouvelles formes de communication permises par les sites de réseaux sociaux en raison du manque d'effectivité des poursuites et sanctions de leurs différents acteurs qui se rendent auteurs d'infractions.

Le régime de responsabilité pénale modéré des opérateurs des réseaux sociaux (**Chapitre 1**) sera ainsi opposé à la sévérité de la responsabilité pénale des utilisateurs des réseaux sociaux (**Chapitre 2**).

---

ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ».

[876] LCEN, art. 6, III, 1.

Chapitre 1 – La responsabilité pénale modérée des opérateurs des réseaux sociaux

331. La responsabilité des opérateurs des réseaux sociaux[877]. Les opérateurs des réseaux sociaux peuvent devenir sujets de la justice pénale de deux manières différentes. En vertu du droit commun, il peuvent devenir responsables à titre principal d'une infraction en leur qualité de responsable d'un traitement de données personnelles. Leur responsabilité pénale peut également être engagée selon la loi n° 2004-575 pour la confiance en l'économie numérique (LCEN) en leur qualité de fournisseur d'hébergement du fait des contenus mis en ligne par leurs utilisateurs, il s'agit toutefois d'une responsabilité modérée. En toute hypothèse, les mécanismes de responsabilité actuels applicables aux opérateurs des réseaux sociaux leurs sont avantageux soit en raison de la faible effectivité de la responsabilité pénale de droit commun (**Section 1**), soit compte tenu du régime juridique favorable mis en place par la LCEN (**Section 2**).

[877] V. sur la question : E. DERIEUX, « Réseaux sociaux et responsabilité des atteintes aux droits de la personnalité », *RLDI*, 2014, n° 100.

Section 1 : Une responsabilité pénale de droit commun peu effective

332. Une responsabilité pénale des opérateurs de réseaux sociaux de leur propre fait. La responsabilité pénale des opérateurs de réseaux sociaux peut s'envisager dans un premier temps par leur propre activité. En effet, les sites de réseaux sociaux mettent en œuvre un traitement massif de données à caratère personnel pouvant être de nature à engager leur responsabilité pénale. Plus précisément, la loi n° 78-17 dite « *informatique et libertés* »[878] a instauré divers devoirs, obligations et interdictions à la charge du responsable d'un traitement de données. Le non-respect de ces dispositions caractérise les infractions prévues aux articles 226-16 et suivants du Code pénal, sanctionnées d'une peine de 300 000 euros d'amende et de cinq ans d'emprisonnement. Ces dispositions sont par ailleurs intimement liées au droit européen sur la protection des données. La directive 95/46/CE[879] constituait à l'origine le texte de référence européen, poursuivant le but d'établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne. Plus récemment, le nouveau règlement européen sur la protection des données (RGPD)[880] est venu réformer le droit européen en poursuivant la volonté d'adapter le système juridique européen aux évolutions majeures vécues par internet et notamment d'offrir un niveau de protection adéquat face aux nouveaux enjeux soulevés par les géants du web. Les dispositions de ce nouveau règlement ont été transposées en droit français le 20 juin 2018[881] et impactent directement les définitions pénales des infractions prévues aux articles 226-16 et suivants du Code pénal.

Les pratiques des opérateurs des réseaux sociaux à l'égard des données de leurs utilisateurs révélées notamment par les affaires *PRISM* et *Cambridge Analytica*[882] sont de nature à entrer sous les qualifications pénales des articles 226-16 et suivants du Code pénal et *in fine,* amener l'engagement de leur responsabilité pénale. Cependant, si les opérateurs des sites de réseaux sociaux peuvent se voir reconnaître aisément la qualité de responsable d'un

[878] L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, 7 janvier 1978 p. 227.
[879] Directive 95/46/CE du Parlement européen et du Conseil, 4 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[880] Règlement (UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (règlement général sur la protection des données dit RGPD).
[881] L. n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* n° 0141, 21 juin 2018.
[882] V. *supra* n° 23.

traitement de données à caractère personnel (**§1**), la sanction pénale de ces derniers se révèle difficile à mettre en œuvre (**§2**).

§1. Les opérateurs de réseaux sociaux, responsables d'un traitement de données à caractère personnel

333. S'il a déjà été démontré que les sites de réseaux sociaux organisaient un traitement automatisé de données[883], les incriminations des articles 226-16 et suivants du Code pénal visent particulièrement à protéger les traitements de données à caractère personnel. Les articles 226-16 et suivants du Code pénal viennent ainsi sanctionner de manière spécifique les atteintes qui peuvent être portées à ces données indépendamment de la protection de la vie privée. En l'occurrence, au vu du traitement de données à caractère personnel réalisé par les opérateurs des réseaux sociaux (A), ces derniers peuvent engager leur responsabilité pénale en leur qualité de responsables d'un tel traitement (B).

A. Le traitement de données à caractère personnel organisé par les opérateurs des réseaux sociaux

334. La notion de données à caractère personnel. À l'origine, la loi n° 78-17 du 6 janvier 1978 faisait référence aux « *informations nominatives* ». Cependant, depuis la loi n° 2004-801 du 6 août 2004 la loi informatique et libertés ainsi que le Code pénal utilisent désormais la notion de « *données à caractère personnel* ». Cette notion était définie par l'article 2 de la loi informatique et libertés comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». Le texte précisait également que « *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* »[884]. Le nouveau règlement européen sur la protection des données est venu reprendre cette définition en la précisant dans son article 4 (1) selon lequel les données personnelles comprennent désormais « *toute information se rapportant à une personne physique identifiée ou identifiable* », sachant qu'est réputée identifiable « *une personne physique qui peut être identifiée, directement ou*

[883] V. *supra* n° 124.
[884] L. n° 78-17, 6 janvier 1978, art. 2, al. 2, mod. L. n° 2004-801, 6 août 2004.

indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Ainsi, de manière constante, les données sont considérées comme à caractère personnel dès lors qu'elles concernent des personnes physiques identifiées directement ou indirectement. Ce type particulier de données concerne alors une grande variété d'éléments comprenant des données d'identification directes (nom, prénom, domicile, numéro d'identification au répertoire national d'identification des personnes physiques, empreintes digitales et autres données biométriques), mais également des informations permettant une identification plus indirecte (notamment l'adresse IP ou encore l'image ou la vidéo d'une personne)[885].

335. La notion de traitement de données à caractère personnel. La loi n° 2004-801 du 6 août 2004 est venue définir la notion de traitement de données à caractère personnel comme « *toute opération ou ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* »[886]. Cette définition est aujourd'hui reprise peu ou prou à l'article 4 (2) du RGPD définissant pour sa part la notion de « *traitement* ». Il est alors permis de déduire de ces éléments que les opérateurs des réseaux sociaux organisent un traitement de données à caractère personnel. En effet, ces sites génèrent en raison de l'activité de leurs utilisateurs une grande diversité d'informations permettant une identification et même un profilage complet de ces derniers. À partir de ces informations, leurs opérateurs organisent une collecte et une conservation de ces données aboutissant à un traitement de données à caractère personnel. À ce titre, le réseau social Facebook explique dans sa politique d'utilisation des données : « *pour fournir les Produits Facebook, nous devons traiter des informations vous concernant* »[887].

Le traitement de données à caractère personnel effectué par les opérateurs des réseaux sociaux s'observe en conséquence par la collecte de données identifiantes soit de nature technique (1) soit relatives à l'activité des internautes (2).

---

[885] F. CHOPIN, Rép. pén. Dalloz, juillet 2013 (actualisation : avril 2018), *V°* Cybercriminalité.
[886] L. n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n° 182, 7 août 2004, p. 14063.
[887] <https://www.facebook.com/privacy/explanation> (dernière consultation le 9 octobre 2019).

1) La collecte de données techniques identifiantes

336. Une multitude de données techniques. Les sites de réseaux sociaux recueillent d'abord des données techniques à savoir, des informations sur les ordinateurs, téléphones ou autres appareils utilisés par leurs abonnés. Ces données révèlent une grande diversité d'informations telles que le système d'exploitation, la version du matériel, les paramètres de l'appareil, les noms et les types de fichier et de logiciel, le niveau de la batterie et l'intensité du signal, ainsi que les numéros d'identification de l'appareil. Mais également les données d'emplacement de l'appareil, notamment les données d'emplacement géographique précises recueillies à travers les signaux GPS, Bluetooth ou Wi-Fi. Les sites de réseaux sociaux recueillent ensuite des informations de connexion telles que le nom de l'opérateur mobile ou du fournisseur d'accès à internet de l'utilisateur ou encore le type de navigateur utilisé par ce dernier. Enfin, les sites de réseaux sociaux recueillent les cookies[888] présents sur l'ordinateur de ses utilisateurs dès lors qu'ils utilisent des sites web et des applications de tiers qui ont recours aux services du réseau social.

337. L'adresse IP, une donnée identifiante. Parmi ces données techniques certaines d'entre elles constituent des données identifiantes revêtant le statut de données à caractère personnel, c'est le cas notamment de l'adresse IP[889]. Dans sa décision du 10 juin 2009 le Conseil constitutionnel a ainsi reconnu ce statut spécifique aux adresses IP[890]. La Cour de justice de l'Union européenne lui reconnaît également ce statut sous certaines conditions[891]. Sur le plan national, la Cour de cassation a reconnu le 3 novembre 2016[892] que les adresses IP peuvent être assimilées au sens de l'article 2 de la loi « *informatique et libertés* » à des données à caractère personnel du fait qu'elles permettent d'identifier indirectement une personne physique. Les juges en ont déduit que la collecte des adresses IP constitue un traitement de données à caractère personnel. Selon Monsieur Alexis Mihman, il peut alors en

[888] Les cookies sont de petits fichiers textes stockés par le navigateur web sur le disque dur du visiteur d'un site web et qui servent (entre autres) à enregistrer des informations sur le visiteur ou encore sur son parcours dans le site. Le webmestre peut ainsi reconnaître les habitudes d'un visiteur et personnaliser la présentation de son site pour chaque visiteur.

[889] Une adresse IP (internet protocol) se définit comme une suite de chiffres binaires attribuée de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique.

[890] Cons. const., 10 juin 2009, DC n° 2009-580 : *RLDI*, 2009, n° 51, p. 114, obs. C. SIMON.

[891] CJUE, *Scarlet c/ SABAM*, 24 novembre 2011, aff. C-70/10 : *RSC* 2012, p. 163, obs. J. FRANCILLON ; *CCE* 2012, comm. 63, obs. A. DEBET ; *CCE* 2012, étude 3, obs. A. NERI – CJUE, *Breyer, B. Pautrot*, 19 octobre 2016, aff. C-582/14 : *RLDI*, 2017, n° 134, p. 23 ; *CCE* 2016, comm. 104, obs. N. METALLINOS ; Rev. int. Compliance 2016, comm. 130, obs. M. GRIGUER et J. SCHWARTZ.

[892] Civ. 1ère, 3 novembre 2016, n° 15-22.595 : *Légipresse* 2017, n° 345, obs. N. BOTCHORICHVILI, p. 27 ; *JCP* G 2016, 1310, obs. R. PERRAY ; *Dalloz IP/IT* 2017, obs. G. PERONNE et E. DAOUD, p. 120 ; *Dr. pén.* 2015, n° 12, chron. 11, obs. A. LEPAGE ; *Gaz. Pal.* 15 novembre 2016, n° 40, p. 24, obs. P. INGALL-MONTAGNIER.

être raisonnablement déduit que la même position soit adoptée par la chambre criminelle[893]. Mais surtout, le RGPD assimile dans son considérant n° 30 les adresses IP mais également les cookies à des identifiants en ligne « *qui peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes* ».

2) La collecte de données identifiantes relative à l'activité des internautes

338. Captation de l'activité de l'utilisateur sur son compte. Au moment de son inscription sur un réseau social, l'utilisateur produit lui-même des données en renseignant des informations comme son nom ou pseudonyme, sa date de naissance, son lieu de résidence, ses centre d'intérêts, etc. Or, de la création d'un album photo au like d'une publication, toutes les actions de l'utilisateur sur son compte sont captées par le réseau social. La politique Facebook d'utilisation des données le mentionne très clairement à son premier alinéa : « *nous recueillons le contenu ainsi que d'autres types d'informations que vous fournissez lorsque vous avez recours à nos services, notamment lorsque vous créez un compte, créez ou partagez du contenu ou encore lorsque vous communiquez avec d'autres utilisateurs. Ceci peut comprendre des informations concernant le contenu que vous partagez, telles que le lieu d'une photo ou encore la date à laquelle un fichier a été créé. Nous recueillons également des informations concernant la manière dont vous utilisez nos services, telles que les types de contenu que vous consultez ou avec lesquels vous interagissez, ou encore la fréquence et la durée de vos activités* »[894].

339. Captation de l'activité des autres utilisateurs. Les sites de réseaux sociaux captent non seulement l'activité de l'utilisateur au sein de son propre compte mais également l'activité des autres internautes sur ce dernier. Les données des utilisateurs sont en effet également produites par d'autres utilisateurs par le fait de messages ou commentaires publiés sur le compte d'un utilisateur, ou encore de photos ou vidéos qui identifient des abonnés. Le réseau social Facebook explique en ce sens : « *Nous recueillons également les contenus et informations que les autres utilisateurs fournissent lorsqu'ils ont recours à nos services, notamment des informations sur vous, par exemple lorsqu'ils partagent une photo de vous,*

[893] L'auteur observe que jusqu'à maintenant, elle s'était bornée à retenir l'absence de traitement de données, compte tenu des conditions dans lesquelles la collecte de l'adresse IP avait été effectuée, sans se prononcer sur l'éventuelle qualification de l'adresse IP en données à caractère personnel (v. par exemple : Crim., 13 janvier 2009, n° 08-84.088 : *Dr. pén.* 2009, comm. 66, obs. J.-H. ROBERT ; Crim., 16 juin 2009, n° 08-88.560 ; Crim., 23 mars 2010, n° 09-80.787). A. MIHMAN, « Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques », *J.-Cl.* Pénal Code, art. 226-16 à 226-24, fasc. 20, janvier 2018, n° 9.
[894] <https://www.facebook.com/privacy/explanation> (dernière consultation le 9 octobre 2019).

vous envoient un message ou encore lorsqu'ils téléchargent, synchronisent ou importent vos coordonnées »[895]. Plus encore, ne pas être abonné sur un réseau social ne garantit pas que ce dernier ne dispose pas d'informations nous concernant. Il suffit pour cela qu'un abonné du réseau social fournisse des informations à propos d'une personne n'y étant pas inscrite en publiant des contenus à son sujet tels que des images, vidéos ou commentaires. En définitive, sur les sites de réseaux sociaux, ce sont les utilisateurs eux-mêmes qui génèrent le plus d'informations en dévoilant des éléments relevant de leur personnalité ou quotidien mais également celui des autres. Les opérateurs des réseaux sociaux sont de ce fait en mesure de dresser une grille d'information détaillée de leurs utilisateurs, voire de personnes n'ayant pas recours à leurs services.

B. La qualité de responsable d'un tel traitement

340. L'organisation du traitement de données à caractère personnel observable sur les principaux réseaux sociaux en ligne permet de déduire pour leurs opérateurs la qualité de responsable d'un tel traitement. Cependant, la dimension internationale des entreprises organisant des sites de réseau social peut s'avérer être un frein à l'application du droit à la protection des données en particulier lorsque la société mère est basée hors de l'Union européenne. Toutefois, l'élargissement récent de la notion de responsable d'un traitement de données par le droit européen (1) permet de rendre applicable aux opérateurs des réseaux sociaux les exigences européennes en matière de protection des données (2).

1) L'élargissement récent de la notion de responsable d'un traitement de données

341. Définition du responsable d'un traitement de données. L'art. 4 (7) du RGPD désigne le responsable du traitement comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ». Autrement dit, ce qui caractérise le responsable du traitement est le fait qu'il décide d'un traitement de données personnelles et qu'il en définisse les caractéristiques, objectifs et moyens[896]. C'est le responsable du traitement de données qui supporte les devoirs et obligations définis par le RGPD et donc les éventuelles sanctions en cas de manquement à ces derniers[897].

[895] *Ibid.*
[896] F. DONNAT, *Droit européen de l'internet. Réseaux, données et services*, Systèmes, LGDJ, 2018, p. 72.
[897] F. MATTATIA, *RGPD et droit des données personnelles*, Eyrolles, 2018, p. 54.

342. Élargissement de la qualité de responsable au sous-traitant. Le règlement européen marque par ailleurs une évolution significative de la protection des données au regard de la précédente directive européenne en attribuant un niveau d'exigence similaire au responsable du traitement de données et à son sous-traitant. Pour ce faire, le présent règlement s'applique aux responsables du traitement mais également aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques[898]. Aux termes de l'article 4 (8) du RGPD, le sous-traitant est défini comme la « *personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* »[899]. L'article 28 du présent règlement précise en outre que le sous-traitant est soumis aux mêmes obligations concernant le recueil et le traitement des données que le responsable lui-même.

343. Champ d'application territorial du règlement. Une autre évolution déterminante du droit européen de la protection des données concerne son champ d'application. Désormais, le règlement s'applique « *au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union* », lorsque les activités sont liées : « *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* »[900]. Ces nouvelles dispositions du droit européen viennent en réalité pallier les difficultés préexistantes à soumettre certains géants du web, notamment les réseaux sociaux dominants comme le site Facebook, aux exigences européennes de protection des données du fait que leur établissement principal se situe en dehors du territoire de l'Union européenne, principalement aux États-Unis. Dorénavant, dès lors que des citoyens de l'Union européenne sont visés par un traitement de données organisant entre autres un suivi comportemental, le droit européen est applicable.

2) L'application aux opérateurs des réseaux sociaux des exigences européennes en matière de protection des données

344. Application du droit européen aux opérateurs des réseaux sociaux. La Cour de justice de l'Union européenne a développé une jurisprudence conséquente sur les notions de traitement de données et de responsable de traitement. Selon elle, l'opération consistant à faire référence, sur une page internet, à diverses personnes et à les identifier, même indirectement,

[898] RGPD, considérant n° 18.
[899] RGPD, art. 4, 8).
[900] RGPD, art. 3, b).

constitue un traitement de données personnelles[901]. Le juge européen a également reconnu que l'activité consistant à collecter dans les documents de l'administration fiscale des données relatives aux revenus du travail et du capital ainsi qu'au patrimoine de personnes physiques et à les traiter en vue de leur publication constituait un traitement automatisé de données[902]. Mais surtout, le juge de Luxembourg a reconnu le 13 mai 2014 dans l'affaire Google Spain que l'exploitant d'un moteur de recherche, en l'espèce la société Google Inc., réalisait un traitement automatisé de données et qu'elle en était le responsable[903]. La jurisprudence européenne s'est prononcée l'année suivante sur le statut de l'entreprise Facebook. La Cour de justice de l'Union européenne[904] a alors reconnu à Facebook la qualité de responsable de traitement de données en se basant sur son activité le transfert de ces dernières. Suivant cette constatation, la Cour a estimé que « *l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel* ».

345. Plus largement, une majorité de la doctrine reconnaît aux sites de réseaux sociaux la qualité de responsable d'un traitement de données. Par exemple, selon Madame Myriam Quéméner les réseaux sociaux forment « *des traitements de données comportant des informations personnelles (nom, adresse e-mail, etc.) et sont à ce titre soumis à la loi du 6 janvier 1978 dite "informatique et libertés"* »[905]. Dans le même ordre d'idée le Professeur Ludovic Pailler soutient que l'activité de ciblage publicitaire de Facebook suscite un traitement à finalité commerciale qui pourrait être soumis au droit européen sur la protection des données[906]. Le groupe de travail de « *l'article 29* » considère également que les sites de réseaux sociaux effectuent un traitement de données et qu'ils en sont responsables. Cette position a été justifiée du fait que ces sites fournissent les moyens permettant de traiter les données des utilisateurs ainsi que tous les services « *basiques* » liés à la gestion des utilisateurs, notamment l'enregistrement et la suppression des comptes. Par ailleurs, le groupe de travail de l'« *article 29* » souligne que les réseaux sociaux en ligne déterminent également la manière dont les données des utilisateurs peuvent être utilisées à des fins publicitaires ou

[901] CJCE, *Bodil Lindqvist*, 6 novembre 2003, C-101/01.
[902] CJCE, *Tietosuojavaltuutettu*, 16 décembre 2008, C-73/07.
[903] Selon la CJUE, « *il convient de constater que, en explorant de manière automatisée, constante et systématique Internet à la recherche des informations qui y sont publiées, l'exploitant d'un moteur de recherche "collecte" de telles données qu'il "extrait", "enregistre" et "organise" par la suite dans le cadre de ses programmes d'indexation, "conserve" sur ses serveurs et, le cas échéant, "communique à" et "met à disposition de" ses utilisateurs sous forme de listes des résultats de leurs recherches* ». CJUE, *Google Spain c/ Mario Costeja González*, 13 mai 2014, grde ch., aff C-131/12.
[904] CJUE, *Maximilian Schrems c/ Data Protection Commissioner*, 6 octobre 2015, aff. C-362/14.
[905] M. QUEMENER, *Le droit face à la disruption numérique*, Gualino, 2018, p. 57, n° 164
[906] L. PAILLER, *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, 2012, p. 161.

commerciales, y compris la publicité fournie par des tiers[907]. Enfin, Monsieur Jean-Philippe Moiny affirme que « *la société Facebook détermine les finalités et les moyens de nombreux traitements de données se produisant à l'occasion du fonctionnement du réseau social* »[908]. De manière générale un site organisant un réseau social revêt par principe la qualité de responsable d'un traitement de données. Selon l'article 3 b) du nouveau règlement européen sur la protection des données, cette qualité s'observe même lorsque le responsable du traitement est établi en dehors de l'Union européenne dès le moment où l'activité de ce dernier s'adresse au public européen. En définitive, les opérateurs des réseaux sociaux sont soumis en droit européen sur la protection des données pour l'ensemble de leurs activités visant le public européen.

346. La responsabilité conjointe des filiales européennes des sites de réseaux sociaux. En outre, aux termes de l'article 28 du RGPD, la qualité de responsable d'un traitement de donnée peut également s'appliquer aux sous-traitants du responsable principal. Or, les grandes plateformes en ligne disposent de filiales au sein de l'Union européenne qui peuvent à ce titre être qualifiées de responsable d'un traitement de données. Par exemple, le réseau social Facebook est une société américaine établie à Palo Alto en Californie. À l'instar d'autres sites de réseaux sociaux comme Twitter ou d'autres grandes plateformes de partage comme YouTube, Dailymotion, ou encore Myspace, le site Facebook possède plusieurs bureaux en Europe dont certains « *International offices* » à Dublin, Paris ou encore Londres. La présence de telles entités sur le territoire européen manifeste une stratégie commerciale du réseau social dirigée vers le territoire de l'Union européenne. En l'occurrence, les deux filiales de Paris et Londres ont davantage une fonction commerciale en particulier concernant l'activité de ciblage publicitaire. Les bureaux de Paris et Londres sont par exemple directement impliqués dans la vente de publicités ciblant des citoyens de l'Union européenne[909]. Le rôle de l'*office* de Dublin serait quant à lui plus important, il constituerait un « *siège social international* » de l'entreprise concernant ses activités visant l'Europe mais également du Moyen Orient et de l'Afrique[910]. Ainsi, toute personne résidant sur le territoire de l'Union et désirant utiliser Facebook est tenue de conclure, lors de son inscription, un contrat avec Facebook Ireland,

[907] Groupe de travail «article 29» sur la protection des données, 01189/09/FR WP 163, avis 5/2009 sur les réseaux sociaux en ligne, 12 juin 2009.
[908] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *REDC*, 2010, n° 2, p. 249.
[909] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 237.
[910] V. J. BARRIGAR, « La vie privée sur les sites de réseau social- Analyse comparative de six sites », Commission à la protection de la vie privée au Canada, février 2009.
<www.priv.gc.ca> (dernière consultation le 9 octobre 2019).

filiale de Facebook Inc.[911]. Dès lors, les bureaux européens de la société Facebook peuvent être considérés au regard du nouveau RGPD comme un sous-traitant de la société mère Facebook située en Californie. Ce dernier possède alors un même niveau de responsabilité que le siège principal.

347. Finalement, les obligations énoncées dans le règlement européen deviennent applicables tant à l'égard de la société mère du fait qu'elle vise des citoyens européens, qu'à l'égard de ses filiales du fait de leur établissement sur le territoire de l'Union européenne. La CNIL a ainsi reconnu le 27 avril 2017[912] l'applicabilité de la loi informatique et libertés et *a fortiori* des exigences européennes en matière de protection des données pour les traitements de données à caractère personnel effectués par le réseau social Facebook dans le cadre des activités de Facebook France. À la lumière de la jurisprudence de la CJUE, la CNIL rappelle que le responsable de traitement est considéré « *comme établi sur le territoire d'un État membre dès lors que le traitement de données est effectué dans le cadre des activités d'un établissement de ce responsable sur le territoire d'un État membre* »[913]. L'autorité administrative indépendante rappelle que la société Facebook France, constituée le 3 février 2011 sous la forme d'une société à responsabilité limitée à associé unique a notamment pour objet social « *de fournir au groupe Facebook des prestations de service en rapport avec la vente d'espaces publicitaires, le développement commercial, le marketing (…) et toutes autres prestations de service visant à développer les services et la marque Facebook en France* ». En conséquence, Facebook France « *constitue une installation stable qui exerce une réelle et effective activité grâce à des moyens humains et technique nécessaires* » et que dès lors elle doit être conjointement qualifiée de responsable des traitements.

§2. La difficile sanction des opérateurs des réseaux sociaux en tant que responsables du traitement

348. L'existence d'un arsenal répressif dissuasif. Les opérateurs des sites de réseaux sociaux, en tant que responsables d'un traitement automatisé de données, peuvent devenir

[911] CJUE, *Maximillian Schrems c/ Data Protection Commissioner*, 6 octobre 2015, aff. C-362/14, n° 27.
[912] CNIL, Délib. n° 2017-006, 27 avril 2017, prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland.
[913] Faisant référence à l'arrêt : CJUE, *Google Spain c/ Mario Costeja González*, 13 mai 2014, grde ch., aff C-131/12.

auteurs d'infractions aux termes des articles 226-16 et suivants du Code pénal[914]. De plus, en tant que personnes morales, ils encourent des peines d'amende accrues en application de l'article 226-24 du Code pénal. Cet article prévoit expressément que les personnes morales peuvent être déclarées responsables des infractions prévues aux articles 226-16 et suivants du Code pénal dès le moment où l'infraction a été commise pour leur compte, par leurs organes ou représentants[915]. En application des règles de l'article 131-38 du Code pénal elles encourent alors le quintuple de l'amende prévue pour les personnes physiques soit une amende de 1 500 000 euros. Outre l'amende, les personnes morales encourent également les peines prévues par les 2° à 5° et 7° à 9° de l'article 131-39 du Code pénal qui comprennent : l'interdiction, à titre définitif ou pour une durée de 5 ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales (2°)[916] ; le placement, pour une durée de cinq ans au plus, sous surveillance judiciaire (3°) ; la fermeture définitive ou pour une durée de cinq ans au plus des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés (4°) ; l'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus (5°) ; l'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement (7°) ; la peine de confiscation, dans les conditions et selon les modalités prévues à l'article 131-21 (8°) ; l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique (9°).

Toutefois, l'encadrement par la loi pénale de l'activité des responsables de traitement de données (A) s'accompagne d'une faible effectivité des sanctions pénales à l'encontre des opérateurs des sites de réseaux sociaux (B).

A. L'encadrement par la loi pénale de l'activité des responsables de traitement de données

349. De multiples interdictions posées par la loi pénale. Les infractions des articles 226-16 et suivants du Code pénal encadrent l'activité du responsable d'un traitement de données autour d'une série d'interdictions répondant à la loi informatique et libertés et aux

[914] Livre II, Titre II, Section 5 : Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.
[915] C. pén., art. 121-2.
[916] L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. A. MIHMAN, *J.-Cl.* Pénal Code, Art. 226-16 à 226-24, fasc. 20, Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, janvier 2018, n° 17.

exigences européennes en matière de protection des données. Selon ces articles, le responsable d'un traitement de données peut engager sa responsabilité pénale s'il se livre à une collecte frauduleuse déloyale ou illicite de données personnelles[917], à un traitement de données personnelles malgré l'opposition de la personne concernée[918], en cas de non-respect de l'interdiction de traiter les données sensibles[919], de non-respect de la limitation de durée de conservation des données[920], de détournement de finalité[921], de divulgation d'informations susceptibles de porter atteinte à la considération ou à la vie privée[922] ou encore de transfert non-autorisé de données hors de l'Union européenne[923].

Le Code pénal prévoit ainsi des infractions relatives à collecte ou au traitement des données à caractère personnel (1) et des infractions relatives à l'usage des données à caractère personnel (2).

1) Les infractions relatives à collecte ou au traitement des données à caractère personnel

350. La collecte illicite de données à caractère personnel. La collecte des données à caractère personnel par un responsable d'un traitement de données n'est pas illégale lorsqu'elle s'effectue dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978[924]. L'article 226-18 vient cependant réprimer « *le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite* ». Cette expression large recouvre diverses situations comme l'obtention de ces données par un vol de fichier ou par un accès frauduleux à un système de traitement automatisé de données. Plus généralement, la collecte est réputée frauduleuse dès lors qu'il est fait usage d'un procédé contraire aux droits conférés par la loi informatique et libertés, notamment le droit d'opposition des personnes[925]. L'objectif de ce texte est notamment de lutter contre le développement des pratiques de collecte à l'insu des personnes concernées, s'effectuant par la mise en place de moyens

[917] C. pén., art. 226-18.
[918] C. pén., art. 226-18-1.
[919] C. pén., art. 226-19.
[920] C. pén., art. 226-20.
[921] C. pén., art. 226-21.
[922] C. pén., art. 226-22.
[923] C. pén., art. 226-22-1.
[924] L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, 7 janvier 1978, p. 227.
[925] P. CONTE, *Droit pénal spécial*, LexisNexis, 4ème éd., 2013, p. 193, n° 310.

techniques apparents ou cachés mais également par des comportements trompeurs à l'égard de la personne de bonne foi[926].

351. Le traitement de données à caractère personnel de contenus illicites. L'article 226-19 du Code pénal punit le fait de mettre ou de conserver en mémoire informatisée sans le consentement exprès de la personne certaines données réputées sensibles. L'article vise spécifiquement les données faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle ou à l'identité de genre. En l'occurrence, le consentement exprès de la personne doit être recueilli sur la base d'une information spécifique aux données sensibles. Autrement dit, l'utilisateur doit être en mesure de marquer son assentiment en cochant une case dédiée à l'approbation de l'usage de ses données personnelles sensibles auquel il consent[927]. En conséquence, un site internet doit mettre à la disposition de la personne auprès de laquelle les données sensibles sont collectées et traitées un moyen technique à l'endroit où les informations sont collectées permettant de s'assurer qu'elle y a consenti de manière expresse sur la base d'une information spécifique[928].

2) Les infractions relatives à l'usage des données à caractère personnel

352. Le détournement de finalité. L'article 226-21 du Code pénal dispose : « *le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalté telle que définie* […] *par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* ». Selon le présent texte, les données collectées avec le consentement de la personne doivent être utilisées conformément à la finalité initiale du traitement qui faisait l'objet du consentement. En conséquence, l'utilisation de données dans un but différent que celui autorisé au moment de la création du traitement automatisé de données est constitutif du présent délit. C'est le cas notamment d'un candidat d'une élection qui avait utilisé pour sa campagne électorale les adresses des administrés de sa commune grâce à une collaboration commerciale avec le groupe EDF-GDF[929]. Cette exigence revêt aujourd'hui un enjeu considérable en raison de l'accroissement sans précédent des collectes et

[926] A. MIHMAN, « Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques », *J.-Cl.* Pénal Code, Art. 226-16 à 226-24, fasc. 20, janvier 2018, n° 44.
[927] CNIL, décision n° 2015-048 du 24 juin 2015 mettant en demeure la société SAMADHI SAS.
[928] CNIL, décision n° 2015-021 du 24 juin 2015 mettant en demeure la société TOODATE.COM SARL.
[929] Aix-en-Provence, ch. d'accusation, 27 mai 1999, n° 859/99.

des traitements de données personnelles pour des finalités qui n'étaient pas prévues à l'origine[930]. L'affaire *Cambridge Analytica* a ainsi révélé un détournement de données à grande échelle opéré par le réseau social Facebook[931].

353. Le transfert non-autorisé de données. Les exigences européennes sur la protection des données ont été renforcées notamment concernant le transfert de données à caractère personnel en dehors du territoire de l'Union européenne. Cependant, une interdiction générale de tout flux de données à caractère personnel à destination ou en provenance de pays en dehors de l'Union européenne serait contraire au développement du commerce international et de l'économie numérique. Il s'agit alors d'encadrer l'augmentation de ces flux qui sont devenus une source d'atteinte aux droits des personnes. À ce titre, le règlement impose notamment que le niveau de protection des citoyens européens ne doit pas être compromis par un transfert de leurs données personnelles hors du territoire de l'Union européenne. Pour ce faire, le transfert de ces données n'est permis qu'à la condition que le pays tiers propose un niveau de protection d'égale importance à celui en vigueur dans l'Union européenne. « *En tout état de cause, les transferts vers des pays tiers et à des organisations internationales ne peuvent avoir lieu que dans le plein respect du présent règlement* »[932]. Ces exigences européennes ont été directement transposées[933] dans la loi du 6 janvier 1978 dite « *Informatique et libertés* » et particulièrement à l'article 226-22-1 du Code pénal. Ce dernier dispose : « *Le fait de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à l'Union européenne ou à une organisation internationale en violation du chapitre V du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016* […] *est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* ». On déduit de la lettre du texte que l'infraction suppose en premier lieu un transfert de données hors de l'Union européenne. L'infraction est applicable à la personne qui procède mais également à

[930] F. MATTATIA, *RGPD et droit des données personnelles*, Eyrolles, 2018, p. 195.

[931] Ce scandale a permis de révéler la transmission par le réseau social Facebook des données personnelles de millions d'utilisateurs *via* un sous-traitant à la firme anglaise *Cambridge Analytica* dans le cadre de la campagne présidentielle américaine de 2016. En tout, 87 millions d'utilisateurs de Facebook auraient potentiellement été touchés. Parmi eux, les données personnelles d'environ 2,7 millions d'utilisateurs européens du réseau social auraient pu être transmises de manière inappropriée au service d'analyse. La firme britannique travaillant pour le compte du candidat Donald Trump a non seulement pu recueillir les données personnelles d'utilisateurs de Facebook à leur insu mais également celles des personnes avec qui ils étaient en contact, ce qui explique le nombre important de personnes concernées. V. sur la question : N. DEVILLIER, « Cambridge Analytica et Facebook : "Le respect de votre vie privée nous tient à cœur." #OuPas », *The conversation*, Chron. juri-geek, 21 mars 2018 ; « Facebook : l'affaire Cambridge Analytica pourrait concerner 2,7 millions d'utilisateurs européens », *Le Monde*, 06 avril 2018. V. *Supra* n° 23.

[932] RGPD, considérant n° 101.

[933] Par la L. n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

celle qui « *fait procéder* » au transfert de données. La notion de transfert des données soulève en l'occurrence des questions à propos des sites web. En effet, des données personnelles publiées sur internet au sein de l'Union européenne et donc consultables dans le monde entier peuvent-elles être considérées comme un transfert de données ? La réponse est négative. Selon Monsieur Fabrice Mattatia « *la publication de données personnelles sur un site web implanté dans l'Union européenne mais consultable dans le monde entier ne constitue pas un transfert de données hors de l'UE* »[934]. Le transfert doit donc être effectif et ne saurait être caractérisé du seul fait que l'information peut être consultée en tout point du globe. En outre, pour que l'infraction soit qualifiée, il est indispensable de démontrer que le pays tiers vers lequel les données sont transférées, ne dispose pas du même degré de protection que le droit européen sur la protection des données. Cette exigence s'avère difficile à remplir tant les systèmes juridiques non-européens ne disposent pas, pour la plupart, d'un système de protection similaire.

B. La faible effectivité de la loi pénale à l'encontre des opérateurs des réseaux sociaux

354. Un faible nombre de sanctions pénales. Selon le rapport Braibant remis au premier ministre le 3 mars 1998, « *le régime répressif français en matière de fichiers informatiques* […] *se caractérise par une grande sévérité, dont le contraste avec une jurisprudence pusillanime est frappant* »[935]. En effet, de 1991 à 1995, seules 35 poursuites ont abouti à des condamnations dont une seule fut accompagnée d'une peine d'emprisonnement sans sursis d'une durée de six mois[936]. Une plus récente condamnation sous ces fondements confirmée par la Cour de cassation en date du 14 mars 2006[937] atteste un peu plus du caractère exceptionnel de la mise en œuvre de telles poursuites sur le plan pénal[938]. Selon une vision optimiste, le faible nombre de condamnations pourrait être le signe d'un bon respect des règles en matière de protection des données. La doctrine y voit cependant plutôt le signe d'une méconnaissance ou d'un désintérêt pour « *ce droit technique, dont les incriminations*

[934] F. MATTATIA, *Traitement des données personnelles*, Eyrolles, 2013, p. 144.
[935] G. BRAIBANT, *Données personnelles et société de l'information, Rapport au Premier ministre*, La documentation Française, 1998, p. 79.
[936] *Ibid*.
[937] Crim., 14 mars 2006, n° 05-83.423 : *CCE* n° 9, septembre 2006, A. LEPAGE comm. 131.
[938] Le Professeur Agathe Lepage observe à ce titre que « *les décisions de condamnation pour infractions à la législation Informatique et libertés ne sont pas très fréquentes, ce qui donne déjà un intérêt certain à cet arrêt de la Chambre criminelle de la Cour de cassation* ». A. LEPAGE, « Collecte déloyale de données personnelles sur Internet », *CCE* n° 9, septembre 2006, comm. 131.

peuvent sembler quelque peu absconses pour des non-spécialistes »[939]. Ce désintérêt est renforcé par l'absence de politique pénale en la matière relevée dès le rapport Braibant de 1998[940].

Ce constat général d'une faible mise en œuvre des infractions relatives aux traitements de données, et plus particulièrement le faible usage de ces incriminations à l'égard des pratiques menées par les opérateurs de réseaux sociaux peut toutefois s'expliquer en raison du pouvoir d'action concurrent de la Commission Nationale de l'Informatique et des Libertés (CNIL) en la matière (1) et par la présence d'accords internationaux légitimant le transfert de données hors de l'Union européenne (2).

1) Le pouvoir d'action concurrent de la CNIL en la matière

355. Un pouvoir sanctionnateur concurrent à celui du juge pénal. L'implication de la CNIL permet d'expliquer la faible importance du contentieux en matière pénale[941]. Le Professeur Jean Pradel observait en effet dès 1990 que la CNIL « *exerce une sorte de "justice retenue" en ce qu'elle ôte à la justice pénale le monopole de l'intervention étatique* »[942]. Cette commission, instituée en 1978 par la loi « *Informatique et Liberté* »[943] est une autorité administrative indépendante[944] disposant d'un pouvoir de sanction concurrent à celui du juge pénal. Elle est l'autorité de contrôle national au sens et pour l'application du règlement général sur la protection des données du 27 avril 2016[945]. Ses missions s'étendent de la vérification *a priori*[946] à la sanction *a posteriori* du respect du droit à la protection des

[939] A. LEPAGE, « Collecte déloyale de données personnelles sur Internet », *CCE* n° 9, septembre 2006, comm. 131 ; v. également en ce sens : A. LEPAGE, « Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Dr. pén.* n° 3, mars 2005, étude 5 ; J.-J. de BRESSON, « Inflation des lois pénales et législatives ou réglementations « techniques », *RSC* 1985, p. 245.

[940] Selon ce rapport : « *Il n'existe (...) guère de politique pénale dans ce domaine où, au surplus, les moyens d'investigation humains et matériels de la police judiciaire sont insuffisants et sous-dimensionnés, eu égard à l'ampleur de l'activité économique liée à l'informatique* ». G. BRAIBANT, *Données personnelles et société de l'information, Rapport au Premier ministre, op. cit.*, p. 79.

[941] A. LEPAGE, « réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *op.cit* ; A. DEBET, J. MASSOT, N. METALLINOS, *Informatique et libertés*, LGDJ, vol. 10, 2015, p. 799 et suiv.

[942] J. PRADEL, « Les infractions relatives à l'informatique », *RIDC* 2-1990, p. 820, citant R. GASSIN, « Le droit pénal de l'informatique », *D.* 1986, chron. p. 35, p. 41. Cité *in* : A. LEPAGE, « réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *op. cit*.

[943] La « *Informatique et Libertés* » lui consacre exclusivement son Chapitre 2.

[944] Cette qualification résulte expressément de l'article 8 de la loi « *Informatique et Libertés* ».

[945] L. n° 78-17, 6 janvier 1978, Art. 8.

[946] Au titre de ses pouvoirs *a priori*, la CNIL poursuit une mission à la fois règlementaire et administrative. Ainsi elle émet des normes (règlement intérieur, recommandations, avis) qui peuvent recevoir dans certains cas un

données. Concernant ses pouvoirs de sanction, la CNIL peut en premier lieu, dans une démarche préventive, adresser un avertissement ou une mise en demeure invitant le responsable du traitement de données à se mettre en conformité avec le règlement européen[947]. Cependant, lorsque ces démarches restent sans effet, l'autorité indépendante peut entrer en voie de répression par le biais notamment de sanctions pécuniaires qu'elle prononce au terme d'une procédure contradictoire. Sur ce point, les pouvoirs de sanction de la CNIL ont été grandement renforcés comparé aux anciennes dispositions de la loi du 6 janvier 1978 qui lui conféraient des pouvoirs de sanction limités[948]. Ainsi, la loi n° 2004-801 du 6 août 2004[949], est venue transposer les directives des 25 octobre 1995[950] et du 8 juin 2000[951], permettant à la commission de prononcer des amendes proportionnées à la gravité des manquements, de 150 000 euros à 300 000 euros ou 5% du chiffre d'affaires en cas de manquement réitérés. Cependant, dans le but d'adapter le pouvoir de sanction de la CNIL aux grands acteurs d'internet, l'ordonnance n° 2018-1125 du 12 décembre 2018[952] est venue prévoir à l'article 20 de la loi « *informatique et libertés* » de nouveaux pouvoirs de sanctions « *surdimensionnés* »[953]. La commission peut désormais prononcer en formation restreinte une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Par ailleurs, en cas de non-respect des principes de base du traitement de

caractère impératif. Concernant ses pouvoirs administratifs, elle autorise les traitements et reçoit les déclarations. V. J.-C. SAINT PAU (dir.), *Droit de la personnalité*, LexisNexis, Traités, 2013, p. 666, n° 1070.

947 L'article 20 de la LIL vient préciser ces mesures préventives : *« I.- Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable de traitement ou son sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ; II.- Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, si le manquement constaté est susceptible de faire l'objet d'une mise en conformité, prononcer à son égard une mise en demeure, dans le délai qu'il fixe* ».

948 Cette dernière ne pouvait alors que délivrer des avertissements aux organismes déclarants ou les dénoncer au parquet. V. L. n° 78-17, 6 janvier 1978, art. 21, 4° ancien.

949 L. n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n° 182, 7 août 2004, p. 14063.

950 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

951 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).

952 Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *JORF* n° 0288, 13 décembre 2018.

953 K. FAVRO, « La CNIL, une autorité à « l'âge de la maturité », *Dalloz IP/IT* 2018 p. 464.

données[954] ou des droits dont bénéficient les personnes concernées[955], ces plafonds sont portés respectivement à 20 millions d'euros et 4 % dudit chiffre d'affaires. Enfin, dans le but de faire cesser un manquement à « *caractère continu* », la CNIL dispose de la possibilité de prononcer une injonction assortie d'une astreinte d'un montant maximum de 100 000 euros par jour[956]. En conséquence, en raison de son fort pouvoir de sanction en matière financière, les mesures prononcées par la CNIL sont susceptibles de relever de la « *matière pénale* »[957]. Ainsi, selon le Conseil d'État, la CNIL, « *eu égard à sa nature, à sa composition et à ses attributions, peut être qualifiée de tribunal au sens de l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* ». Elle est alors tenue, « *lorsqu'elle se prononce sur des agissements pouvant donner lieu aux sanctions prévues par les dispositions des articles 45 et suivants de la loi du 6 janvier 1978* », de statuer « *dans des conditions respectant le principe d'impartialité* »[958].

356. La mise en œuvre de ce pouvoir sanctionnateur à l'égard des grandes plateformes numériques. Au regard de son fort pouvoir sanctionnateur, la CNIL a alors entrepris de durcir sa politique de sanction, particulièrement à l'égard des grandes plateformes numériques opérant un traitement de données à caractère personnel. La commission est venue sanctionner à trois reprises la société Google Inc : une première sanction pécuniaire de 100 000 €[959] puis une deuxième de 150 000 €[960] et plus récemment une sanction de 100 000 €[961]. Mais surtout, la CNIL est également venue prononcer à l'égard du réseau social Facebook une amende de 150 000 euros le 27 avril 2017[962]. Cette sanction s'est notamment justifiée en raison de la

[954] De manière générale le règlement général sur la protection des données rappelle que ces dernières doivent être « *traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)* ». RGPD, art 5, §1, a).

[955] Il s'agit d'une part d'un droit à la transparence des informations concernant le traitement de données réalisé à son encontre, et d'autre part, de la communication des modalités d'exercice de leurs droits en ce qui concerne ce traitement. V. RGPD, art. 12 à 22.

[956] L. n° 78-17, 6 janvier 1978, art. 20, III, 2°.

[957] CEDH, *Engel et autres c. Pays-Bas*, 8 juin 1976, n° 5100/71 – CEDH, *Öztünk c/ Allemagne*, 21 février 1984, n° 8544/79 : R. PERRAY, « Commission nationale de l'informatique et des libertés », *J.-Cl* Adm., fasc. 274-50, 24 Mai 2017, n° 101.

[958] CE, ord. réf., 19 février 2008, Sté Profil France, préc. n° 69 : R. PERRAY, « Commission nationale de l'informatique et des libertés », *J.-Cl* Adm., Fasc. 274-50, 24 Mai 2017, n° 101.

[959] CNIL, délib. n° 2011-035, 17 mars 2011 : *CCE* 2012, étude 1, note A. DEBET.

[960] CNIL, délib. n° 2013-420, 3 janvier 2014 : CNIL, « La formation restreinte de la CNIL prononce une sanction pécuniaire de 150 000 € à l'encontre de la société GOOGLE Inc. », 8 janvier 2014, www.cnil.fr ; *JCP* G 2014 n° 7, 211, obs. E. DERIEUX. *Adde* : R. PERRAY, « Commission nationale de l'informatique et des libertés », *J.-Cl* Adm., Fasc. 274-50, 24 Mai 2017, n° 118.

[961] CNIL, délib. n° 2016-054, 10 mars 2016 : *CCE* 2016, comm. 65, note A. DEBET. Google n'ayant pas modifié ses pratiques en vue de permettre l'exercice du droit au déréférencement que l'extension de la page Internet concernée soit en. fr ou en. com.

[962] CNIL, Délib. n° 2017-006, 27 avril 2017, prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland. Cette sanction prononcée par la CNIL s'est justifiée par le non-respect d'une série d'obligations relatives à la protection des données par le réseau social Facebook à savoir : l'absence de base

collecte des données de navigation des internautes inscrits ou non sur le réseau social *via* l'utilisation du cookie « *datr* ». Cela permettait au réseau social de suivre, sans les en informer, la navigation de tout internaute ayant visité une page Facebook publique ou un site tiers contenant un module social Facebook[963]. La sanction s'est également justifiée par la combinaison massive par le réseau social des données de ses utilisateurs sans en obtenir un consentement au moment de la création de leur compte ou lors de l'utilisation de la plateforme. Cette activité est d'autant plus critiquable que les utilisateurs sont dépourvus de tout contrôle sur cette combinaison et ne peuvent s'y opposer. La CNIL en a alors déduit le non-respect de l'obligation pour le responsable du traitement de collecter et traiter les données de manière licite et loyale[964]. Outre cette obligation, l'autorité administrative indépendante a également relevé un manquement du réseau social à l'obligation d'informer les personnes[965]. En l'occurrence, la délibération relève que Facebook ne fournit aucune des informations requises sur le formulaire d'inscription ou sur les pages permettant aux personnes inscrites de modifier leur profil. Les supports d'information par « *strate* » fournis par le réseau social ne permettent pas aux internautes d'avoir une information claire et précise des traitements mis en œuvre, particulièrement concernant les informations relatives aux transferts de données à l'étranger[966]. Enfin, la CNIL est venue souligner l'absence de base légale du traitement effectué par le réseau social[967]. Selon la commission, Facebook ne peut évoquer aucun fondement pour les traitements des données personnelles auxquels il procède en vue de faire de la publicité ciblée. Selon le Professeur Anne Debet, cette décision « *remet profondément*

---

légale pour les traitements combinant les données relatives aux utilisateurs du réseau social pour afficher de la publicité ciblée, le traitement de données sensibles sans recueil du consentement exprès, la collecte déloyale de données relatives aux internautes non-utilisateurs du réseau, l'insuffisante information des personnes notamment sur les transferts de données hors Union européenne, la fixation de durées de conservation disproportionnées par rapport aux finalités du traitement et le non-respect du cadre législatif relatif aux cookies. V. : A. DEBET, « Facebook condamné à une sanction pécuniaire de 150 000 euros par la CNIL », *CCE* n° 7-8, Juillet 2017, comm. 67 ; F.-P. LANI et E. BACQ, « Facebook sanctionné par la CNIL pour de nombreux manquements à la loi informatique et libertés », *Légipresse* n° 352, septembre 2017, p. 444.

963 Il s'agit par exemple des fonctionnalités « *j'aime* » ou « *like* » permettant de relier un site internet au réseau social Facebook.

964 L. n° 78-17, 6 janvier 1978, art. 6 1° ancien (art. 4 nouveau).

965 Le responsable du traitement a l'obligation d'informer la personne concernée par le traitement notamment sur : l'identité du responsable ; la finalité du traitement ; les destinataires ou catégories de destinataires des données ; leurs droits ; le transfert éventuel des données hors de l'Union européenne ; la durée de conservation des données. L. n° 78-17, 6 janvier 1978, art. 32 I ancien (art. 104 nouveau).

966 L. n° 78-17, 6 janvier 1978, art. 32 I, 7° ancien (RGPD, art 13, 1, f et 14, 1, f).

967 À défaut de consentement de la personne concernée, le responsable d'un traitement de données satisfaire l'une des conditions énoncées : Le respect d'une obligation légale incombant au responsable du traitement ; la sauvegarde de la vie de la personne concernée ; l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ; l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ; la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire. L. n° 78-17, 6 janvier 1978, art. 7 ancien (art. 5 nouveau).

en cause le modèle économique de Facebook, dont la publicité ciblée est la ressource financière principale »[968]. La CNIL semble ainsi s'ériger en acteur essentiel du contrôle et de la sanction des grandes plateformes numériques opérant un traitement de données. La mise en demeure de la société WatsApp Inc. réalisée par l'autorité administrative indépendante[969] confirme un peu plus ce constat.

357. La question du cumul des répressions entre l'autorité administrative et le juge pénal. Les sanctions prononcées par la CNIL démontrent que les mêmes faits peuvent parfaitement être attaqués soit devant les juridictions pénales en tant que violation d'une infraction mentionnée aux articles 226-16 et suivants du Code pénal, soit devant l'autorité administrative indépendante au titre d'une violation de la loi informatique et libertés et indirectement du règlement (UE) 2016/679 du 27 avril 2016. Les victimes disposent donc de deux juridictions qui ne sont pas exclusives l'une de l'autre et dont leur saisine simultanée est envisageable[970]. Bien que le nombre de condamnations par l'autorité judiciaire sous les fondements des articles 226-16 et suivants du Code pénal soit de faible importance, se pose quand bien même la question du cumul des répressions administratives et pénales. Le principe *ne bis in idem* impose en effet qu'une personne ne peut être poursuivie ou punie pénalement deux fois pour un même fait[971]. Sur ce point, la Cour de justice de l'Union européenne est venue récemment dans une série de trois arrêts[972] admettre un infléchissement de ce principe. La Cour reconnaît qu'un cumul entre des poursuites ou sanctions pénales et des poursuites ou sanctions administratives de nature pénale était, sous certaines conditions, possible à l'encontre d'une même personne poursuivie pour des mêmes faits. Selon le juge européen, un tel cumul doit alors : viser un objectif d'intérêt général, ces poursuites et sanctions devant

---

968 A. DEBET, « Facebook condamné à une sanction pécuniaire de 150 000 euros par la CNIL », *CCE* n° 7-8, Juillet 2017, comm. 67.

969 CNIL, décembre n° MED-2017-075, 27 novembre 2017 mettant en demeure la société WHATSAPPCNIL ; délib. du bureau, n° 2017-300, 12 décembre 2017 décidant de rendre publique la mise en demeure n° 2017-075, 27 novembre 2017 prise à l'encontre de la société WHATSAPP INC. En l'espèce, la CNIL remet en cause le fondement de la transmission de données opéré de WhatsApp à Facebook. La commission relève que les utilisateurs ont été informés de cette transmission par l'intermédiaire d'une modification des règles d'utilisation et de confidentialité. Or, selon la CNIL dans ces conditions, la transmission des données ne peut être fondée sur un consentement libre et informé des utilisateurs. Par ailleurs, cette transmission ne peut être justifiée par un intérêt légitime du responsable du traitement en raison de l'atteinte disproportionnée aux droits des utilisateurs qui ne peuvent s'opposer à une telle transmission. A. DEBET, « Dans la famille Facebook, la CNIL s'intéresse désormais à WhatsApp », *CCE* n° 5, Mai 2018, comm. 38.

970 F. MATTATIA, « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés ? », *RSC* 2009, p. 317.

971 Ce principe est consacré en droit interne par l'article 368 du C. proc. pén. et en droit européen par l'article 50 de la Charte des droits fondamentaux de l'Union européenne.

972 CJUE, *Menci*, 20 mars 2018, aff. C-524/15 – CJUE, *Garlsson Real Estate*, 20 mars 2018, aff. C-537/16 – CJUE, *Di Puma*, 20 mars 2018, aff. C-596/16 : *D. actu.*, 22 mars 2018, obs. E. MAUPIN ; *RTDE* n° 2 p. 419 ; *AJDA*, 2018, 602 ; *ibid*. 1026, chron. P. BONNEVILLE, E. BROUSSY, H. CASSAGNABERE et C. GÄNSER ; *D.* 2018 p. 616 ; *Rev. sociétés* 2018 p. 731, note H. MATSOPOULOU ; *RSC* 2018 p. 524, obs. F. STASIAK.

avoir des buts complémentaires ; établir des règles claires et précises permettant de limiter au strict nécessaire la charge supplémentaire résultant du cumul ; enfin assurer que la sévérité de l'ensemble des sanctions imposées soit limitée à ce qui est strictement nécessaire par rapport à la gravité de l'infraction concernée[973].

358. En droit internet un infléchissement du principe *ne bis in idem* s'est également observé par un arrêt de la Cour de cassation[974] reconnaissant que l'ancien Conseil des marchés financiers (aujourd'hui l'AMF) n'est pas une juridiction pénale et que partant, la double poursuite engagée devant l'autorité administrative et la juridiction pénale ne méconnait pas le principe *ne bis in idem*. Le Conseil constitutionnel a également admis au regard du principe de nécessité des délits et des peines qu'il n'était pas interdit « *à ce que les mêmes faits commis par une même personne puissent faire l'objet de poursuites différentes aux fins de sanctions de nature administrative ou pénale en application de corps de règles distincts devant leur propre ordre de juridiction* »[975]. Le Conseil a par la suite affiné sa position en précisant une série de conditions cumulatives justifiant l'interdiction d'un tel cumul, en l'occurrence lorsque les poursuites pénale et administrative portent sur des faits identiques, mettent en œuvre des répressions ayant les mêmes finalités, visent des sanctions de nature identique et enfin relèvent du même ordre juridictionnel[976]. Par ailleurs, lorsque le cumul des poursuites est admis, les sanctions s'additionnent sous réserve que le montant global ne dépasse pas le montant le plus élevé de l'une des sanctions encourues[977]. Cette hypothèse est directement prévue par la loi « *informatique et libertés* » selon laquelle : « *lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce* »[978].

359. Au final, au vu de la jurisprudence actuelle, il apparaît aux niveaux européen et national que l'autorité judiciaire et l'autorité administrative doivent dans leur rôle

---

[973] CJUE, communiqué de presse n° 34/18, 20 mars 2018.
[974] Crim., 13 septembre 2017, n° 15-84.823 : *D. actu.*, 28 septembre 2017, obs. W. Azoulay.
[975] Cons. const. 28 juillet 1989, n° 89-260 DC, *JO* 1er août 1989, p. 9676 ; *RFDA* 1989 p. 671, obs. B. GENEVOIS ; *Pouvoirs* 1990, n° 52, p. 189, obs. P. AVRIL et J. GICQUEL.
[976] Cons. const. 18 mars 2015, nos 2014-453/454 et 2015-462 QPC, *JO* 20 mars 2015, p. 5183 ; *D.* 2015 p. 874, obs. O. DECIMA ; *JCP* 2015, n° 13, p. 369, obs. J.-H. ROBERT ; *RSC* 2015. 705, obs. B. de LAMY – Cons. const. 14 janv. 2016, n° 2015-513/514/526 QPC, *JO* 16 janvier 2016, n° 54 ; *D.* 2016. 931, obs. O. DECIMA ; *Dr. pén.* 2016, n° 46, obs. E. BONIS-GARÇON et V. PELTIER ; *Banque et Droit* 2016, n° 165, p. 55, obs. J. CHACORNAC. *Adde* : A. CAPPELLO, Rép. pén. Dalloz, octobre 2016, *V°* Autorités administratives indépendantes, nos 107 et suiv.
[977] Cons. const., 28 juillet 1989, *JO* 1er août 1989, p. 9676 ; *RFDA* 1989 p. 671, obs. B. GENEVOIS ; *Pouvoirs* 1990, n° 52, p. 189, obs. P. AVRIL et J. GICQUEL.
[978] L. n° 78-17, 6 janvier 1978, art. 22, al. 4.

sanctionnateur poursuivre des buts complémentaires afin de justifier la dualité de leur compétence et plus encore la dualité de leur saisine[979]. La Cour européenne des droits de l'homme a par un nouvel arrêt du 27 juin 2019[980] synthétisé un peu plus la jurisprudence existante en la matière. Selon la juridiction strabourgeoise, les États peuvent cumuler les poursuites et les sanctions dès lors que « *les systèmes juridiques* […] *traitent de manière "intégrée" le méfait néfaste pour la société en question, notamment en réprimant celui-ci dans le cadre de phases parallèles, menées par des autorités différentes et à des fins différentes* ». Il ressort alors de cette jurisprudence que des procédures intégrées dans un tout cohérent peuvent parfaitement se cumuler[981].

360. La collaboration entre la CNIL et l'autorité judiciaire. Eu égard à la coloration pénale des sanctions prononcées par la CNIL il est nécessaire que cette dernière ainsi que l'autorité judiciaire fonctionnent en étroite collaboration afin de satisfaire les critères jurisprudentiels déterminant l'application du principe *ne bis in idem*. Or, concernant la protection des données à caractère personnel, une telle collaboration peut être observée entre la CNIL et les juridictions pénales. L'autorité administrative indépendante est chargée d'informer sans délai le procureur de la République lorsqu'elle acquiert la connaissance d'un crime ou d'un délit[982]. De son côté, le procureur de la République doit aviser le président de l'autorité administrative indépendante de toutes les poursuites relatives aux infractions relatives aux traitements de données à caractère personnel prévues aux articles 226-16 et suivants du Code pénal[983]. Le président de la CNIL ou son représentant peut dans ce cadre être invité par la juridiction d'instruction ou de jugement à déposer ses observations ou à les développer oralement lors de l'audience[984]. La CNIL et les juridictions pénales sont donc davantage amenées à se renforcer mutuellement plutôt que d'agir de manière concurrente[985] conduisant alors à une interraction adéquate entre ces deux autorités.

[979] Sur la question v. notamment : F. STASIAK, « Sac de "nœuds" *bis in idem* : cumul de sanctions pénales et administratives en droit de l'Union européenne », *RSC* 2018, p. 524.
[980] CEDH, *Nodet c. France*, 6 juin 2019, n° 47342/14 : *D. actu.*, 27 juin 2019, obs. P. DUFOURQ ; *JCP G* n° 25, 24 Juin 2019, note L. MILANO.
[981] P. DUFOURQ, « Répression des abus de marché : non bis in idem et bis repetita », *D. actu.*, 27 juin 2019.
[982] L. n° 78-17, 6 janvier 1978, art. Art. 8, I, 2°, f).
[983] L. n° 78-17, 6 janvier 1978, art. 41 al. 1.
[984] L. n° 78-17, 6 janvier 1978, art. 41 al. 2.
[985] Conseil d'État, Rapport public 2001, Les autorités administratives indépendantes, p. 329.

2) Des accords internationaux légitimant le transfert de données hors de l'Union européenne

361. Le mécanisme de certification du *Safe Harbor*. Les exigences européennes en matière de protection des données ont imposé à la Commission européenne à conclure un accord avec les États-Unis de manière à assurer un niveau de protection adéquat aux données transférées de l'Union européenne vers ces derniers. Cet accord était en effet rendu nécessaire en raison de l'absence de loi fédérale générale de protection des données personnelles aux États-Unis. Ainsi, à l'issue de négociations entre l'Union européenne et le département du commerce aux États-Unis[986] l'accord du *Safe harbor* (sphère de sécurité) a été adopté dans la décision de la Commission européenne du 26 juillet 2000[987]. Cet accord autorisait les flux transfrontaliers de données depuis l'Europe vers les entreprises établies aux États-Unis s'étant engagées à respecter les principes posés par l'accord, en l'occurrence : le droit de s'opposer à la divulgation de ses données personnelles ainsi que le droit à la sécurité et à l'intégrité des données émanant des citoyens de l'Union européenne. Le mécanisme était en l'occurrence basé sur un système d'autocertification amenant les entreprises à se déclarer auprès du ministère du commerce américain comme respectant les principes du *Safe Harbor*. De plus, l'accord reconnaissait aux autorités américaines leur compétence pour vérifier le bon respect de ces principes sur la base de plaintes déposées auprès de la *Federal Trade Commission* (FTC)[988]. Cet accord a alors permis de légitimer le transfert de données de l'Union européenne vers un espace juridique ne garantissant pas un même niveau de protection des données à caractère personnel.

362. L'invalidation du *Safe harbor*. Le niveau de protection offert par l'accord a toutefois été remis en cause suite à la publication en juin 2013 des révélations d'Edward Snowden à propos des programmes de surveillance à grande échelle mis en place par la *National Security Agency* (NSA) permettant l'accès à des données stockées par certaines entreprises américaines, notamment la société Facebook. Le *Safe Harbor* a alors été invalidé par la Cour de justice de l'Union européenne dans son arrêt du 6 octobre 2015[989] sanctionnant le transfert de données réalisé par la société Facebook *Ireland* vers sa société mère basée aux États-Unis. Cet arrêt reconnaît que les données d'un citoyen autrichien, Maximilian Schrems, fournies à

[986] *United States Department of Commerce* (DoC).
[987] Commission européenne, décision n°2000/250/CE, 26 juillet 2000.
[988] F. DONNAT, *Droit européen de l'internet. Réseaux, données et services*, Systèmes, LGDJ, 2018, pp. 111-112.
[989] CJUE, *Maximillian Schrems c/ Data Protection Commissioner*, 6 octobre 2015, aff. C-362/14.

Facebook ont été transférées, en tout ou partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis, où elles ont fait l'objet d'un traitement. Monsieur Maximilian Schrems s'est plaint de ce transfert auprès de l'autorité de contrôle irlandaise en argumentant que le droit et les pratiques des États-Unis n'offrent pas de protection suffisante concernant la protection des données. Ainsi, les révélations de l'affaire *PRISM* permettent de contester la réelle mise en œuvre du régime de la « *sphère de sécurité* » et donc la légalité du transfert de ces données. Le juge européen a mis en avant les failles du dispositif du *Safe Harbor* validé par la Commission. La Cour relève notamment que l'accord issu de la décision du 26 juillet 2000 ne définissait pas de critères objectifs permettant de délimiter l'accès des autorités publiques américaines aux données et leur utilisation à des fins précises, mais également qu'une telle ingérence n'était pas justifiée et qu'il n'était prévu aucune voie de recours permettant d'avoir accès aux données ou d'en obtenir la rectification ou la suppression. La Cour de justice de l'Union européenne a alors retenu que le régime de la « *sphère de sécurité* » mis en œuvre aux États-Unis n'offrait pas « *un niveau de protection adéquat des données personnelles* » justifiant l'invalidation de l'accord passé avec la Commission[990]. Cet arrêt a eu pour effet de priver subitement de fondement légal l'ensemble des transferts transatlantiques de données réalisé depuis le 26 juillet 2000[991].

363. Le nouvel accord transatlantique : le *Privacy Shield* . Suite à l'invalidation du *Safe Harbor* un nouveau dispositif rebaptisé *Privacy Shield* ou *Bouclier de protection* négocié entre la Commission européenne et le gouvernement américain est entré en vigueur le 1er août 2016[992]. De manière générale, ce nouvel accord reprend les éléments du *Safe Harbor* tout en les renforçant sur les failles relevées par la CJUE. Le mécanisme du *Privacy Shield* demeure en conséquence basé sur le principe d'autocertification des entreprises américaines. L'inscription se réalise auprès du ministère américain du commerce et est désormais renouvelable tous les ans. L'inscription engage l'entreprise à informer l'utilisateur sur les types de données qu'elle traite et sur la finalité du traitement. Ces données ne peuvent être utilisées pour une finalité incompatible avec celles précisées initialement dans le traitement et doivent être de surplus traitées de manière fiable et sécurisée. Le nouvel accord oblige également les entreprises inscrites sur la liste à donner un droit d'accès et de rectification aux données traitées. Le *Privacy Shield* opère par ailleurs un renforcement au regard du *Safe*

[990] CJUE, *Maximillian Schrems c/ Data Protection Commissioner*, communiqué de presse n° 117/15, Luxembourg, 6 octobre 2015, arrêt dans l'affaire C-362/14.
[991] F. DONNAT, *Droit européen de l'internet. Réseaux, données et services*, Systèmes, LGDJ, 2018, p. 114.
[992] <www.privacyshield.gov> (dernière consultation le 9 octobre 2019).

Harbor en précisant que si les entreprises conservent le droit de transférer leurs données à une autre société, un tel transfert n'est cependant possible que dans la mesure où la société qui recevrait ces données garantit un même niveau de protection des données. Toutefois, le principal apport du *Privacy Shield* réside dans la consécration d'un droit pour la personne dont les données ont fait l'objet d'un traitement d'introduire une réclamation et d'en obtenir réparation en saisissant directement la Commission fédérale du commerce des États-Unis, qu'elle soit citoyen américain ou non. Les utilisateurs peuvent également porter réclamation directement auprès de l'entreprise qui peut saisir l'autorité chargée de la protection des données d'un État membre de l'Union européenne. En cas d'épuisement de ces voies de recours, la personne peut saisir le comité d'arbitrage du bouclier de protection des données. Enfin, le *Privacy Shield* a introduit un nouvel acteur à savoir, un médiateur entre l'Europe et les États-Unis appelé *Ombudsman* chargé de s'assurer que toutes les réclamations relatives aux données à caractère personnel sont correctement examinées[993].

364. Si le *Privacy Shield* opère des améliorations significatives au regard du *Safe Harbor* il n'est toutefois pas exempt de critiques. Le G29 constate dans son avis du 13 avril 2016 que « *d'importantes préoccupations* » demeurent concernant le volet commercial du *Privacy Shield*[994]. Au-delà du « *manque général de clarté* » de cet accord, le G29 relève en premier lieu l'incertitude qui demeure concernant les pouvoirs des agences de renseignements américaines. Le G29 déplore ainsi que les autorités américaines n'aient pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens. En second lieu, le G29 salue la mise en place du médiateur offrant un nouveau mécanisme de recours qui devrait améliorer considérablement les droits des citoyens européens vis-à-vis des activités des services de renseignement américains. Toutefois, le G29 questionne son indépendance et l'étendue réelle de ses pouvoirs pour exercer son rôle efficacement. Le Contrôleur européen de la protection des données (CEPD) souligne quant à lui dans un avis concernant le *Privacy Shield*[995] les efforts accomplis par les parties pour proposer des solutions aux problèmes relatifs aux transferts de données à caractère personnel à des fins commerciales de l'UE vers les

[993] F. DONNAT, *Droit européen de l'internet. Réseaux, données et services*, Systèmes, LGDJ, 2018, pp. 115-116 ; M.-A. WEISS, « De la sphère au bouclier : qu'est-ce que le Privacy Shield ? », *I2D – Information, données & documents*, vol. 53, nº 3, 2016, pp. 20-22.
[994] Communiqué du G29, Publication de l'avis du G29 sur l'accord Privacy Shield, 13 avril 2016. <https://www.cnil.fr/fr/communique-g29-publication-de-lavis-du-g29-sur-laccord-privacy-shield> (dernière consultation le 9 octobre 2019).
[995] Avis 2016/C 257/05 du Contrôleur européen de la protection des données concernant le « Bouclier vie privée UE États-Unis » (*Privacy Shield*).

États-Unis. Cependant, des améliorations importantes doivent encore être réalisées pour parvenir à un cadre solide et fiable sur le long terme. Selon ce dernier, « *le projet de Bouclier vie privée peut constituer un pas dans la bonne direction, mais, tel qu'il est actuellement formulé, il ne comprend pas, à notre avis, l'ensemble des garanties nécessaires à la sauvegarde des droits de la personne au respect de la vie privée et à la protection des données de l'UE, ni en ce qui concerne les recours judiciaires* ». Le contrôleur préconise comme solution de long terme qu'une plus grande valeur juridique soit apportée aux garanties sur la protection des données et notamment de transposer et d'identifier précisément dans la loi fédérale les grands principes en la matière.

365. Conclusion de la Section 1. Les infractions des articles 226-16 et suivants du Code pénal ne sont qu'à de très rares occasions mise en œuvre alors même qu'elles prévoient un arsenal répressif complet et dissuasif concernant la protection des traitements de données à caractère personnel. Les opérateurs des sites de réseaux sociaux sont pourtant parfaitement assimilables à des responsables de traitement de données et les dispositions du Code pénal et *a fortiori*, de la loi informatique et liberté leur sont en tous points applicables. Partant, la faible mise en œuvre de ce dispositif répressif pourrait se justifier par le traitement diligent des données personnelles opéré par les opérateurs des sites de réseaux sociaux. Or, il a parfaitement été démontré que ces derniers se sont très largement affranchis des obligations européennes en matière de protection des données ce qui justifierait pleinement l'engagement de leur responsabilité pénale. Toutefois, malgré le manque évident de sanction en matière pénale, il ne peut être conclu à une impunité des opérateurs des sites de réseaux sociaux agissant en leur qualité de responsable d'un traitement de données à caractère personnel. En effet, avec l'accroissement considérable de ses pouvoirs de sanction administrative, la CNIL est devenue, devant le juge pénal, la principale autorité de contrôle et de sanction des obligations applicables aux responsables de traitement de données. Cette dernière n'a alors pas hésité à sanctionner le réseau social Facebook pour le non-respect de nombreuses dispositions de la loi informatique et libertés. Ce rôle accru de la CNIL en la matière ne signifie toutefois pas pour autant un effacement du rôle du juge pénal qui dispose en réalité d'un pouvoir d'action complémentaire avec celui de l'autorité administrative indépendante. En réalité, la problématique du respect effectif des règles nationales et européennes en matière de protection des données est davantage liée à la présence d'accords internationaux entre l'Union européenne et l'administration américaine. Ces accords permettent de légitimer le transfert de données hors de l'Union européenne vers un système juridique n'offrant pas le

même niveau de protection en la matière et permettant ainsi de contourner l'interdiction posée à l'article 226-22-1 du Code pénal. En l'occurrence, si le nouvel accord du *Privacy Shield* offre davantage de garanties que l'ancien accord *Safe Harbor*, il est encore permis de douter que les données des citoyens européens bénéficient dans le cadre de cet accord d'une protection équivalente sur le sol américain.

Section 2 : La responsabilité pénale des opérateurs selon la LCEN, un régime juridique favorable

366. Le statut juridique des sites de réseaux sociaux selon la LCEN. La qualification juridique des sites de réseaux sociaux revêt un enjeu majeur dans la mesure où elle détermine le régime de responsabilité applicable aux acteurs d'internet. En l'occurrence, la LCEN distingue d'un côté les éditeurs de contenus, à savoir l'intervenant à l'origine du contenu, et de l'autre, les prestataires techniques, à savoir les intervenants ne possédant qu'une fonction technique dans la mise en ligne du contenu. Les prestataires techniques, à savoir les fournisseurs d'hébergement et les fournisseurs d'accès à internet, jouissent en la matière d'un statut privilégié en raison de leur rôle subsidiaire dans la publication du contenu : ils n'en sont pas à l'origine mais fournissent les moyens techniques de sa publication. Cette distinction était à l'origine, dans les années 2000, claire et facilement identifiable. Les premiers prestataires techniques, particulièrement les hébergeurs, ne fournissaient qu'une prestation technique basique, ces derniers se contentaient d'accueillir les sites de leurs clients en mettant un espace de stockage à leur disposition sur un serveur central[996]. Ce que l'on pouvait appeler le web 1.0 a toutefois laissé rapidement place au web 2.0, ce qui a engendré une grande diversification du champ d'action des intermédiaires techniques. Ces derniers ne se réduisant plus à une simple fonction de stockage. Les hébergeurs rencontrés à l'origine et n'assurant qu'un stockage physique d'informations existent toujours mais d'autres prestataires techniques utilisent une technologie plus avancée contribuant à une complexification de la fonction de stockage au point de parler aujourd'hui d'un web 3.0. Les principaux réseaux sociaux sont aujourd'hui emblématiques de cette évolution technique d'internet, leur rôle dépassant de loin la simple intervention purement technique. La jurisprudence a cependant

[996] À l'origine, en France, le fournisseur d'hébergement le plus connu était OVH. L. MARINO, « Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl.* Comm., Fasc. 670, 30 août 2015 (dernière mis à jour 1er décembre 2017), n° 19.

choisi de leur attribuer le statut d'hébergeur (**§1**) leur assurant en conséquence l'application d'un régime de responsabilité favorable (**§2**).

§1. Le statut d'hébergeur octroyé aux opérateurs

367. Les sites de réseaux sociaux bénéficient actuellement du statut d'hébergeur tel qu'envisagé par l'article 6, I, 2 de la LCEN. Ce texte, plutôt que de faire référence aux fournisseurs d'hébergement eux-mêmes, base en réalité sa définition sur l'activité de stockage du founisseur d'hébergemen (A). Le travail d'interprétation jurisprudentiel a toutefois recentré la définition sur le rôle actif de l'hébergeur en y incluant notamment des opérateurs des réseaux sociaux (B).

A. Une définition légale basée sur l'activité de stockage du fournisseur d'hébergement

368. Un critère *ratione materiae*. L'article 14-1 de la directive du 8 juin 2000[997] sur le commerce électronique est venu apporter une définition de l'activité des fournisseurs d'hébergement. Cette dernière consisterait en la fourniture d'un service de la société de l'information qui équivaudrait à stocker des informations, fournies par un destinataire du service. Cette disposition a été reprise, peu ou prou, à l'article 6, I, 2 de la LCEN qui définit à son tour les fournisseurs d'hébergement comme : « *Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ». Le dénominateur commun de ces définitions réside dans le fait que la qualité de fournisseur d'hébergement est fonction de son activité de stockage[998]. Les textes ne font donc pas référence à la qualité d'hébergeur mais davantage à l'activité de ce dernier qui est perçue comme une activité purement technique. La définition légale s'articule donc sur la base d'un critère *ratione materiae* et non pas sur celle d'un critère *ratione personae*[999].

---

[997] Directive Européenne 2000/31/CE du Parlement européen et du conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur dite « *directive sur le commerce électronique* ».

[998] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 1137, n° 1935.

[999] P. STOFFEL-MUNCK, « Avis de tempête sur le Web 2.0 : la Cour de cassation juge que Tiscali n'est pas un hébergeur », *CCE*, mars 2010, n° 3, comm. 25.

B. Une définition jurisprudentielle recentrée sur le rôle actif de l'hébergeur

369. L'évolution des critères de définition. Sur la base de ces éléments venant décrire l'activité de fournisseur d'hébergement, la jurisprudence est venue étoffer la définition au point de l'élargir. La définition originelle de l'activité d'hébergement provient d'une époque où le législateur visait les fournisseurs d'hébergement au sens strict du terme, autrement dit, ceux assurant le stockage physique des données. Cependant, le développement constant d'internet a fait émerger de nouveaux acteurs que la jurisprudence devait faire correspondre aux catégories préexistantes. Cette interprétation dynamique des textes a contribué à maintenir les définitions initiales au contact de l'évolution technologique. Concrètement, l'activité d'hébergement ne consiste plus exclusivement à stocker physiquement une information, cette dernière pouvant également se matérialiser dans le stockage virtuel d'informations destinées à être mises à la disposition du public. Pour ainsi dire, « *tout intermédiaire assurant un stockage physique ou virtuel d'un contenu informationnel – quel qu'en soit le format – dans le but de le rendre consultable de tous doit être considéré comme étant un fournisseur d'hébergement* »[1000].

370. Le rôle actif de l'hébergeur, nouvelle clé d'interprétation. Allant à contre-courant de cette dynamique visant à intégrer davantage d'intervenants au régime des prestataires techniques, la Cour de cassation a opté dans un arrêt du 14 janvier 2010[1001] pour une approche restrictive de la notion de fournisseur d'hébergement. La présente jurisprudence consacrait une vision exclusive du rôle du prestataire de services : soit il se cantonne exclusivement à la fonction purement technique d'hébergeur, soit il ne peut bénéficier du régime de responsabilité aménagée[1002]. Cet arrêt fit l'objet de nombreuses critiques doctrinales[1003], certains l'assimilant même à une décision « *hébergicide* »[1004]. Face à ces incertitudes entourant la notion d'hébergeur, la Cour de justice de l'Union européenne donna la clé

[1000] F. DELIEGE, *La responsabilité des acteurs de l'internet en matière de délits de presse*, Thèse Université Nancy 2, 12 juin 2006, p. 147, n° 253.
[1001] Civ 1ère, 14 janvier 2010 : *CCE* 2010, nº 3, comm. 25 ; *RLDI*, 2010, n° 59, nº 1951 ; *RLDI*, 2010, n° 58, nº 1934 ; *RLDI*, 2010, n° 58.
[1002] La Cour de cassation a considéré à propos de le société Tiscali que, en offrant « *à l'internaute de créer ses pages personnelles à partir de son site et* [en proposant] *aux annonceurs de mettre en place, directement sur ces pages, des espaces publicitaires payants, dont elle assurait la gestion* », la société « *excédait les simples fonctions techniques de stockage* » et qu'ainsi *« elle ne pouvait pas invoquer le bénéfice* [de l'article 43-8 de la loi du 1er aout 2000] ».
[1003] V. notamment : P. STOFFEL-MUNCK, « Avis de tempête sur le Web 2.0 : la Cour de cassation juge que Tiscali n'est pas un hébergeur », *CCE*, n° 3, mars 2010, comm. 25 ; C. MANARA, « hébergement de contenus : une décision critiquable ! », *D.* 2010, p. 260 ; L. THOUMYRE, « Les notions d'éditeurs et d'hébergeurs dans l'économie numérique », *D.* 2010, p. 837.
[1004] L. THOUMYRE, « Les notions d'éditeurs et d'hébergeurs dans l'économie numérique », *op. cit.*

d'interprétation de l'activité d'hébergeur aux juridictions nationales dans son arrêt Google Adwords[1005]. Selon le juge de Luxembourg, l'hébergeur ne doit pas avoir joué « *un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées* ». Cette nouvelle position jurisprudentielle est désormais reprise par les juridictions nationales, notamment par la première chambre civile de la Cour de cassation qui dans une série de trois arrêts rappelle que le régime de responsabilité aménagée « *s'applique au prestataire d'un service de référencement sur internent lorsque ce prestataire n'a pas joué un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées* »[1006]. En définitive, il est désormais admis que le pouvoir d'action sur les contenus soit le critère principal de définition du fournisseur d'hébergement contribuant à élargir son champ d'application qui n'est plus restreint aux seuls intervenants purement techniques. Le rôle du juge dans la qualification de l'activité de prestataire revenant à établir si ce dernier a eu un rôle actif dans l'établissement du contenu en cause[1007].

371. Assimilation des réseaux sociaux à des fournisseurs d'hébergement. À l'aune de ce nouveau critère, la qualification de fournisseur d'hébergement a pu être appliquée à une grande variété de prestataires de services internet notamment à ceux appartenant au web 2.0. Certaines plateformes de partage de vidéos se sont ainsi vues attribuer la qualité d'hébergeur, l'exemple le plus marquant étant celui du site de streaming Dailymotion. En l'espèce, la Cour de cassation[1008] a considéré que le ré-encodage et le formatage sont « *des opérations techniques qui participent de l'essence du prestataire d'hébergement* ». Ils « *n'induisent en rien une sélection par ce dernier des contenus mis en ligne* ». Par ailleurs, la mise en place de cadres de présentation et la mise à disposition d'outils de classification permettent de rationaliser l'organisation, ce qui est « *encore en cohérence avec la fonction de prestataire*

[1005] CJUE, *Sté Google c/ Sté Louis Vuitton Malletier*, 23 mars 2010, aff. C-236/08 à C-238/08 : *JCP* G 2010, note 642, L. MARINO ; *JCP* G 2011, 1175, doctr. F. TERRÉ ; *CCE* 2010, comm. 88, note P. STOFFEL-MUNCK ; *CCE* 2010, comm. 70, note C. CARON ; *CCE* 2010, étude 12, G. BONET ; *D.* 2010, p. 885, obs. C. MANARA ; *RTDE* 2010, p. 939, obs. E. TREPPOZ ; *CCC* 2010, comm. 132, note M. MALAURIE-VIGNAL ; *RLDI*, 2010, n° 60, note L. GRYNBAUM ; *RLDI*, 2010, n° 61, note C. CASTETS-RENARD ; *Légipresse* 2010, n° 274, p. 158, note C. MARECHAL ; *Propr. industr.* 2010, comm. 31, note P. TREFIGNY-GOY.

[1006] Com., 13 juillet 2010, n° 06-15.136 – Com., 13 juillet 2010, n° 06-20.230 : *Bull. civ.* IV n° 124 ; *CCE* 2010, comm. 93, obs. C. CARON ; *CCC* 2010, comm. 229, obs. M. MALAURIE-VIGNAL ; *D.* 2010, p. 1966, obs. P. TRÉFIGNY-GOY ; RLDI, 2010, n° 63, n° 2063, note C. CASTETS-RENARD ; *Légipresse* 2010, p. 367, note P. ALLAEYS – Civ. 1ère, 17 février 2011, n° 09-13.202 : *CCE* 2011, comm. 32, C. CARON.

[1007] A. SAINT MARTIN, « Clarification de la qualification de service d'hébergement », *RLDI*, 2011, n° 70.

[1008] Civ. 1ère, 17 février 2011, n° 09-67.896 : *Bull. civ.* I n° 30 ; *CCE* 2011, comm. 32, note C. CARON ; *JCP* G 2011, 520, note A. DEBET ; Gaz. Pal 23 juin. 2011, p. 20, note L. MARINO ; Resp. civ. et assur. 2011, étude 8, L. MARINO ; *Propr. intell.* 2011, n° 39, p. 197, note A. LUCAS ; *D.* 2011, p. 1113, note L. GRYNBAUM ; *RLDI*, 2011, n° 69, n° 2258, note C. CASTETS-RENARD ; *Légipresse* 2011, n° 283, p. 297, note V. VARET.

technique ». L'ensemble de ces constatations a permis de conclure que Dailymotion n'intervient donc pas dans le choix des contenus. Mais surtout, l'exploitation du site par la commercialisation d'espaces publicitaires n'induit pas davantage « *une capacité d'action du service sur les contenus mis en ligne* ». Le caractère onéreux d'un site ne présume donc en rien de sa non appartenance à la catégorie des hébergeurs. Cette dernière observation s'inscrit dans la lignée de l'arrêt Google Adwords[1009] dans lequel la Cour de justice de l'Union européenne a affirmé que la détermination du rôle actif est déconnectée de la réalisation d'un profit[1010].

372. L'ensemble de ces constatations a permis de reconnaître le statut d'hébergeur à des blogs[1011], des forums de discussion[1012], des sites de partage de vidéos[1013] ou même des sites d'enchères en ligne[1014]. Mais surtout, les sites de réseaux sociaux ont également bénéficié de cette vision large de l'activité d'hébergement. En effet, partant de ce mouvement jurisprudentiel, les juges du fond ont considéré que le site Facebook était un prestataire technique de services de communication au public en ligne assimilable à un hébergeur de sites[1015]. L'appartenance de Facebook et plus largement de l'ensemble des sites de réseaux sociaux à cette catégorie semble donc acquise[1016]. Cette qualification revêt un enjeu considérable tant le fournisseur d'hébergement détient des obligations particulières ainsi qu'un statut privilégié.

§2. Un régime juridique favorable applicable aux opérateurs

373. Les opérateurs des réseaux sociaux bénéficient actuellement d'un régime juridique favorable en raison d'une part de l'application souple des obligations imposées aux hébergeurs (A) et d'autre part, en raison de l'irresponsabilité de principe octroyée à ces derniers (B).

[1009] CJUE, *Sté Google c/ Sté Louis Vuitton Malletier*, 23 mars 2010, aff. C-236/08 à C-238/08, précit.
[1010] L. MARINO, « Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl.* Comm., Fasc. 670, 30 août 2015 (dernière mis à jour 1er décembre 2017), n° 23.
[1011] Par exemple : le site < www.over-blog.com>, V. TGI Paris, 22 juillet 2010, www.legalis.net.
[1012] Par exemple : le site <www.foruminternet.org>, V. Versailles, 12 décembre 2007 : *RLDI*, 2008, n° 34, n° 1148, obs. A. SAINT MARTIN.
[1013] Par exemple le site <www.dailymotion.com>, Civ. 1ère, 17 février 2011, n° 09-67.896, précit.
[1014] Par exemple le site <www.ebay.com>, TGI Paris, 26 octobre 2004, Poiray France c/ SARL CJSF, Ophélie, Ibazar et SA eBay France.
[1015] TGI Paris, 20 avril 2010, *RLDI*, 2010, n° 61, n° 2019.
[1016] A. SAINT MARTIN, « Clarification de la qualification de service d'hébergement », *RLDI*, 2011, n° 70.

A. Une application souple des obligations des réseaux sociaux en tant qu'hébergeurs

374. La coopération des réseaux sociaux avec l'institution judiciaire. La pratique du pseudonyme est courante sur les réseaux sociaux en ligne, cette dernière permettant à leurs utilisateurs de rester anonymes et de protéger ainsi leur identité. Les réseaux sociaux détiennent alors un monopole concernant les informations d'identification de leurs utilisateurs, notamment lorsque ces dernies deviennent auteurs d'infractions. La LCEN a cependant prévu une obligation de conservation et de transmission de données d'identification à la charge des hébergeurs et donc des opérateurs des réseaux sociaux (1). Toutefois, si la coopération entre les opérateurs des réseaux sociaux et l'institution judicaire sur le fondement de cette obligation est existante, elle demeure toutefois délicate à mettre en œuvre (2).

1) L'obligation de conservation et de transmission de données d'identification

375. L'obligation de conservation des données. La LCEN a instauré une obligation de conservation des données d'identification à la charge des fournisseurs d'accès internet et des hébergeurs. L'article 6, II de cette loi dispose que les fournisseurs d'accès internet et les hébergeurs « *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires* ». La finalité de cette conservation est essentiellement de permettre de retrouver les internautes qui se livrent anonymement ou sous pseudonyme à la diffusion de contenus illicites. L'objectif de cette obligation de conservation est donc avant tout de tenter de lutter efficacement contre l'anonymat dont peuvent bénéficier les individus sur internet[1017]. Le décret du 25 février 2011[1018] précise à cette fin les types de données faisant l'objet de cette obligation de conservation permettant de déterminer l'étendue de l'obligation de conservation des opérateurs. L'article premier du décret dresse une liste limitative des données devant être conservées. Selon cet article, les hébergeurs, pour chaque opération de création, doivent conserver les données suivantes : « *l'identifiant de la connexion à l'origine de la communication ; l'identifiant attribué par le système d'information au contenu objet de l'opération ; les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ; la nature de l'opération ; les date et heure de l'opération ; l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni* ». Par ailleurs, les fournisseurs d'accès

[1017] F. CHAFIOL-CHAUMONT, « Retour sur l'obligation de conservation des données d'identification après la parution du décret du 25 février 2011 », *RLDI*, 2011, n° 71.
[1018] Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

internet et les hébergeurs, lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, devront fournir les informations suivantes : « *au moment de la création du compte, l'identifiant de cette connexion ; les nom et prénom ou la raison sociale ; les adresses postales associées ; les pseudonymes utilisés ; les adresses de courrier électronique ou de compte associées ; les numéros de téléphone ; le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour* ». L'article 3 de ce décret précise enfin que « *la durée de conservation des données est d'un an à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu* ». Le non-respect de cette obligation de conservation est sanctionné pénalement d'un an d'emprisonnement et de 75 000 € d'amende[1019].

376. Les outils juridiques permettant la transmission des données à l'autorité judiciaire. Si la conservation des données d'identification est indispensable pour lever l'anonymat de certains utilisateurs, en pratique seule la transmission de ces données aux autorités est de nature à permettre la poursuite de l'auteur d'une infraction agissant sous un pseudonyme ou sous une fausse identité sur un site de réseau social. À ce titre, l'autorité judiciaire dispose de certains outils juridiques lui permettant de requérir aux opérateurs des réseaux sociaux la transmission des données d'identification mentionnées par le décret du 25 février 2011. Cette demande peut être faite dans un premier temps en application de l'article 145 du Code de procédure civile selon lequel : « *s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé* ». Plus spécifiquement encore, l'article 6, I, 8 de la LCEN prévoit la possibilité pour l'autorité judiciaire de prescrire en référé ou sur requête « *toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ». Toutefois, lorsque la demande vise des données d'identification hébergées par un site de réseau social établi en dehors de l'Union européenne, ce qui est majoritairement le cas, il doit être fait application des traités d'assistance mutuelle en matière judiciaire conclu entre la France et les États-Unis le 10 décembre 1998[1020] et également entre l'Union européenne et les États-Unis le

[1019] LCEN, art. 6, VI.-1.

[1020] Traité d'entraide judiciaire en matière pénale entre la France et les États-Unis d'Amérique, signé à Paris le 10 décembre 1998 et entré en vigueur le 1er décembre 2001. Décret n° 2001-1122 du le 28 novembre 2001, *JORF* n° 277 du 29 novembre 2001, p. 18964.

25 juin 2003[1021]. Ces traités prévoient alors que l'autorité nationale, saisie par l'autorité étrangère, doit faire suite à la demande dès lors que l'infraction à laquelle se rapporte la demande n'est pas une infraction politique ou une infraction connexe à une infraction politique, ou que l'exécution de la demande risque de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels[1022].

377. Les outils juridiques permettant la transmission des données à l'autorité administrative. Par ailleurs, la loi n° 2013-1168 de programmation militaire du 18 décembre 2013[1023] et la loi n° 2015-912 sur le renseignement du 24 juillet 2015[1024] sont venues respectivement créer et préciser un cadre juridique d'accès administratif aux données de connexion. La loi de programmation militaire du 18 décembre 2013, est venue réformer le cadre juridique de l'accès aux données de connexion notamment par son article de 20 ajoutant un chapitre dans le Code de la sécurité intérieure intitulé « *accès administratif aux données de connexion* »[1025]. L'article L 851-1 du Code de la sécurité intérieure dispose que le recueil des données de connexion sera autorisé auprès « *des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* […] ». L'ensemble des prestataires techniques semble donc visé par ces dispositions, autant les fournisseurs d'accès à internet que les hébergeurs de sites internet et *a fortiori* les opérateurs des réseaux sociaux. En outre, ce même article précise que l'accès administratif concerne les informations ou documents traités ou conservés par les prestaitaires techniques, y compris « *les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ». À l'origine cantonné à la criminalité terroriste, le champ de compétence de l'accès administratif aux

[1021] Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, *JOCE* n° L181, 19 juillet 2003, p. 34.
[1022] Traité d'entraide judiciaire en matière pénale entre la France et les États-Unis d'Amérique, signé à Paris le 10 décembre 1998 et entré en vigueur le 1er décembre 2001. Décret n° 2001-1122 du le 28 novembre 2001, *JORF* n° 277 du 29 novembre 2001, p. 18964, art. 6.
[1023] L. n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, *JORF* n° 0294, 19 décembre 2013, p. 20570.
[1024] L. n° 2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n° 0171, 26 juillet 2015, p. 12735.
[1025] À l'origine : CSI, Livre II, Titre IV, Chapitre VI créant les articles L 246-1 et suiv. ; désormais : CSI, Livre VIII, Titre V, Chapitre 1er créant les articles L 851-1 et suiv.

données de connexion s'est considérablement étendu notamment avec la loi sur le renseignement du 24 juillet 2015. L'article L 811-3 du CSI établit en la matière les finalités justifiant une telle demande de la part de l'autorité administrative, l'article mentionnant outre la prévention du terrorisme d'autres notions plus diffuses telles que : « *l'indépendance nationale* », « *les intérêts majeurs de la politique étrangère* », « *les intérêts économiques, industriels et scientifiques majeurs de la France* » ; « *la prévention du terrorisme* », « *la prévention de la criminalité et de la délinquance organisées* ». Enfin, lorsque la demande de l'autorité administrative porte sur des données hébergées en dehors de l'Union européenne, l'article 8 de l'accord en matière d'entraide judiciaire entre l'Union européenne et les États-Unis[1026] précise alors que l'entraide judiciaire peut être également accordée à l'autorité administrative nationale lorsque la demande porte sur des faits en vue d'être poursuivi pénalement.

2) La coopération délicate des réseaux sociaux dans l'identification du responsable

378. La difficile soumission des sites de réseaux sociaux à l'obligation de conservation et de transmission des données. L'application de l'obligation de conservation et de transmission des données à l'égard des sites de réseaux sociaux ayant leur siège en dehors de l'Union européenne s'est toutefois révélée compliquée. La société Twitter s'est vue sollicitée par les juridictions françaises pour identifier certains de ses utilisateurs qui étaient à l'origine de tweet racistes et antisémites. Pour ce faire, le tribunal de grande instance de Paris[1027] a ordonné à Twitter de communiquer aux associations qui le réclamaient les données d'identification des auteurs de messages. La société Twitter a cependant contesté sa soumission à cette obligation issue de la LCEN et plus largement au droit français. Selon le raisonnement de la société Twitter, validé par le juge des référés, l'article 4 du décret du 25 février 2011 prévoit que « *la conservation des données mentionnées à l'article 1er est soumise aux prescriptions de la loi du 6 janvier 1978 susvisée, notamment les prescriptions prévues à l'article 34, relatives à la sécurité des informations* ». L'article 2 de la loi n° 78-12 du 6 janvier 1978 précise à ce titre que sont soumis à cette loi les traitements « *dont le responsable est établi sur le territoire français* » ou « *recourt à des moyens de traitement situés sur le territoire français* ». La société Twitter en a déduit que les données qu'elle recueille et conserve, le sont en vertu du droit californien et qu'elle ne peut en conséquence

[1026] Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, *JOCE* n° L181, 19 juillet 2003, p. 34, art 8.
[1027] TGI Paris, référé, 24 janvier 2013, n^{os} 13/50262 et 13/50276.

garantir avoir conservé l'ensemble des données exigées par le décret du 25 février 2011[1028]. Le juge des référés s'est alors fondé sur l'article 145 du Code de procédure civil pour justifier la communication des données. Selon ce dernier, l'identification des auteurs des infractions ne pouvait en l'espèce être possible sans le concours de l'exploitant du service. Le juge en a déduit un motif légitime d'enjoindre à Twitter de communiquer « *les données en sa possession de nature à permettre l'identification de quiconque a contribué à la création des tweets manifestement illicites* »[1029]. Cette difficulté d'application de la LCEN à l'égard des opérateurs des réseaux sociaux n'est cendant pas systématique. Dans d'autres hytpothèses les sites de réseaux sociaux se sont pliés à la réquisition judiciaire sans contester leurs soumissions aux règles prescrites par la LCEN. C'est le cas notamment du réseau social Facebook qui a également fait l'objet de telles réclamations par les autorités françaises. Ainsi, par une ordonnance de référé du tribunal de grande instance de Paris du 13 avril 2010[1030], il a été ordonné à Facebook au visa notamment de l'article 6, II de la LCEN, « *la communication des données de nature à permettre l'identification des auteurs* » des contenus litigieux. Le réseau social s'est astreint à cette injonction en communicant les adresses IP des auteurs des contenus illicites. Plus récemment encore, dans deux ordonnances des 6 et 30 juin 2014[1031], le tribunal de grande instance de Paris ordonnait à la société Facebook de lui transmettre des données d'identification d'un de ses utilisateurs sur le fondement de l'article 6, II de la LCEN et de l'article 145 du Code de procédure civile.

379. Le manque d'automaticité de la coopération des sites de réseaux sociaux avec les autorités françaises. Ces quelques exemples jurisprudentiels mettent en exergue les difficultés tenant à la bonne coopération des opérateurs des réseaux sociaux en la matière. Si les opérateurs des réseaux sociaux se montrent dans certains cas coopératifs, ces derniers ne satisfont cependant pas automatiquement les réquisitions judiciaires visant à dévoiler des éléments d'identification de leurs utilisateurs. Plus encore, le faible nombre d'ordonnances sur référé ou sur requête demandant aux opérateurs des réseaux sociaux de communiquer des données d'identification de leurs utilisateurs amène à remettre en cause l'efficacité des

[1028] V. sur le sujet : A. LEPAGE, « Même sur Internet, c'est dans les vieux pots qu'on fait les meilleures soupes », *CCE* n° 5, Mai 2013, comm. 58 ; A. COUSIN, « Twitter peut-il échapper à la loi française ? », *D.* 2013, p. 696.
[1029] C. MANARA, « Twitter : communication de données d'identification », *D.* 2013, p. 300.
[1030] TGI Paris, réf., 13 avril 2010, n° 10/53340.
[1031] TGI Paris, réf., 6 juin 2014 et 30 juin 2014 : ordonnances citées *in* : J. CATTAN, « *L'obtention des données d'utilisation des réseaux sociaux* », *in* V. NDIOR (dir.), *Droit et réseaux sociaux*, éd. Lextenso, coll. LEJEP, octobre 2015, p. 138.

procédures existantes[1032]. Le Conseil d'État a d'ailleurs observé que « *les grandes sociétés américaines ayant la qualité d'hébergeur, telles que Facebook, Twitter ou Youtube, ne s'estiment pas tenues par ces dispositions et répondent à leur guise aux demandes formulées par les autorités, selon des critères qui leur sont propres* »[1033]. Par exemple, le réseau social Facebook précise pour sa part qu'il répond « *aux demandes valables concernant des affaires criminelles* » et que « *la légitimité de chacune des demandes que nous recevons est vérifiée, et nous rejetons les demandes trop vagues ou imprécises, ou nous demandons davantage de précisions sur celles-ci* »[1034]. Le risque est de voir s'instaurer un traitement différencié en fonction de la gravité des infractions. Certains propos peuvent en effet être constitutifs selon le droit français d'une infraction, alors que selon l'approche américaine, plus libérale en la matière, ces mêmes propos ne revêtent aucune qualification pénale[1035]. La coopération des opérateurs des réseaux sociaux peut en conséquence varier selon le type d'infractions et selon la précision de la demande envoyée. Selon le ministère de l'intérieur, en 2015, le taux de réponse aux requêtes des services de police français était ainsi très aléatoire : 13 %, pour Twitter, 33 % pour Facebook et 50 % en moyenne pour Google[1036].

B. L'organisation d'un système d'irresponsabilité des opérateurs des réseaux sociaux

380. Genèse du régime de responsabilité de l'hébergeur. Chronologiquement, le premier texte relatif à la responsabilité du fournisseur d'hébergement est la directive du 8 juin 2000[1037], dite directive sur le commerce électronique. La section 4 du chapitre II de ce texte s'intitule: « *Responsabilité des prestataires intermédiaires* ». Elle a pour objet de définir les responsabilités des prestataires techniques que sont les fournisseurs d'accès et les fournisseurs d'hébergements. Ainsi, son article 14 précise que « *les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service* ». Cela signifie que lorsqu'un prestataire technique d'hébergement se contente de stocker un contenu sur son

[1032] J. CATTAN, « *L'obtention des données d'utilisation des réseaux sociaux* », *op. cit.*, p. 144.
[1033] Rapport Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 245.
[1034] Facebook, *Government Requests Report*, cité *in* : Rapport Conseil d'État, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 245.
[1035] V. *Infra.*
[1036] E. VINCENT, « Bernard Cazeneuve accuse les géants du Web d'entraver les enquêtes judiciaires », *Le Monde*, 21 février 2015.
<https://www.lemonde.fr/ameriques/article/2015/02/21/bernard-cazeneuve-a-tenu-un-dialogue-respectueux-avec-les-geants-du-web-en-californie_4581122_3222.html> (dernière consultation le 9 octobre 2019).
[1037] *JOCE*, 17 juillet 2000, L.178, p. 15.

serveur à la demande de l'un de ses usagers, il ne doit pas en être responsable. Cet article marque donc « *l'acte de naissance* »[1038] du régime d'irresponsabilité dont bénéficie le fournisseur d'hébergement.

381. Ce principe d'irresponsabilité est repris aux articles 6, I, 2 et 3 alinéa 1er de la LCEN selon lesquels les fournisseurs d'hébergement « *ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicite ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible* ». En outre, l'article 6, I, 6 de la LCEN précise que le fournisseur d'accès et l'hébergeur ne sont pas des producteurs. En conséquence, les hébergeurs ne peuvent voir leur responsabilité engagée sur le fondement de l'article 93-3 de la loi du 29 juillet 1982. Cette disposition ferme la dernière porte qui permettait de poursuivre le fournisseur d'hébergement devant les juridictions pénales, leur responsabilité ne pouvant pas non plus être engagée au titre du système de responsabilité en « *cascade* ».

Les sites de réseaux sociaux en leur qualité de fournisseurs d'hébergement bénéficient donc d'« *un extraordinaire régime de faveur* »[1039] excluant leur responsabilité dans deux hypothèses : en cas d'absence de connaissance de l'illicéité des contenus stockés (1), soit en cas de connaissance de l'illicéité des contenus stockés suivie d'un prompt retrait (2).

1) L'irresponsabilité issue de l'absence de connaissance de l'illicéité des contenus stockés

382. Absence d'obligation générale de surveillance. Afin d'affirmer le principe d'irresponsabilité des hébergeurs, la dircetive du 8 juin 2000 est venu rappeler que les hébergeurs ne sont pas investis d'une obligation générale de surveillance. Une telle obligation peut en effet s'avérer particulièrement sévère et dangereuse pour le prestataire technique qui prend le risque de voir sa responsabilité engagée pour chaque information hébergée. L'article 15 de la directive du 8 juin 2000 vient justement démentir une telle obligation en précisant que : « *les États membres ne doivent pas imposer aux prestataires, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation de rechercher activement des faits ou des circonstances révélant des activités illicites* ». Cette disposition

[1038] F. DELIEGE, *La responsabilité des acteurs de l'internet en matière de délits de presse*, thèse Université Nancy 2, 2006, p. 135, n° 232.
[1039] L. MARINO, « Responsabilité civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl. comm.*, Fasc. 670, 30 août 2015 (mis à jour décembre 2017), n° 43.

répond à l'irresponsabilité posée à l'article 14 de cette directive. Ainsi, si l'hébergeur n'est pas responsable des contenus illicites qu'il héberge, il ne l'est pas davantage s'il a omis de surveiller ces mêmes contenus. La loi du 21 juin 2004 réaffirme ce principe à son article 6, I, 7 qui dispose: « *les personnes mentionnées aux 1 et 2 (c'est à dire les fournisseurs d'accès et les fournisseurs d'hébergement) ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent* ». Selon le Professeur Laure Marino, cette absence de connaissance de l'illicéité des contenus stockés a deux importantes répercussions : « *les hébergeurs ne sont pas censés avoir connaissance par eux-mêmes des contenus hébergés. En conséquence, les hébergeurs ne sont pas censés,* a fortiori, *avoir connaissance de leur illicéité* »[1040].

383. Refus du système de *notice and stay down*. Le système de responsabilité mis au point par la LCEN est l'équivalent de la procédure américaine de *notice and take down*[1041] dans laquelle le retrait du contenu (appelé le *take down*) doit intervenir dans un prompt délai suite à sa prise de connaissance par l'hébergeur. Cette obligation de retrait du contenu qui forme la base du système de responsabilité des intermédiaires techniques n'implique cependant pas de veiller à ce que le contenu concerné ne réapparaisse pas. Cette obligation anti-réapparition appelée *notice and stay down* a été condamnée par la Cour de cassation[1042] considérant que cette dernière aboutirait à soumettre les hébergeurs « *à une obligation générale de surveillance (...) et de recherche des reproductions illicites et à leur prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps* ». En somme, la procédure de *notice and stay down* aboutit à imposer à l'hébergeur une obligation générale de surveillance qui contrevient directement aux principes posés par la LCEN. Cette observation vaut également pour toute obligation de filtrage[1043] généralisé des contenus imposée aux hébergeurs. Ceci a notamment été rappelé par la Cour de justice de l'Union européenne ayant jugé que l'exploitant d'un réseau social en ligne, en l'espèce Netlog, ne peut être contraint de mettre en place un système de filtrage général visant tous ces utilisateurs pour prévenir l'usage illicite d'œuvres musicales ou

[1040] L. MARINO, « Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl.* Comm., Fasc. 670, 30 août 2015 (dernière mis à jour 1er décembre 2017), n° 45.
[1041] Procédure introduite aux États-Unis par le *Digital Millennium Copyright Act* (DMCA) en 1998.
[1042] Civ. 1ère, 12 juillet 2012, n° 11-15.165 et 11-15.188 : *Gaz. Pal.* 18 octobre 2012, n° 292, p. 19, note L. MARINO ; *JCP* E 2012, 1627, note J.-M. BRUGUIERE ; *CCE* 2012, comm. 91, note C. CARON ; *D.* 2012, p. 2075, note C. CASTETS-RENARD ; *D.* 2012, p. 2071, concl. C. PETIT ; *Légipresse* 2012, n° 298, p. 566, note P. ALLAEYS ; *Propr. intell.* 2012, n° 45, p. 416, note A. LUCAS ; *RTD Com.* 2012, p. 771, note F. POLLAUD-DULIAN.
[1043] Le filtrage se définit comme « *une limitation sélective d'accès au Réseau* » : *Livre vert sur les techniques de filtrage*, Labs Hadopi, 14 décembre 2011, p. 5.

audiovisuelles. Selon la Cour, « *une telle obligation ne respecterait pas l'interdiction d'imposer à un tel prestataire une obligation générale de surveillance ni l'exigence d'assurer le juste équilibre entre, d'une part, la protection du droit d'auteur et, d'autre part, la liberté d'entreprise, le droit à la protection des données à caractère personnel et la liberté de recevoir ou de communiquer des informations* »[1044].

384. Présence d'une obligation particulière de surveillance. Le principe de l'absence d'obligation générale de surveillance permet toutefois de recourir à une surveillance limitée de certains contenus informationnels véhiculés par internet et les réseaux sociaux en particulier. À ce titre, le principe de l'absence d'obligation générale de surveillance comporte une exception. En effet, l'usage du terme « *général* » n'interdit pas de recourir à « *toute activité de surveillance ciblée et temporaire* »[1045] dans la mesure où cette surveillance est ordonnée par l'autorité judiciaire. En l'occurrence, l'article 6, I, 8° de la loi du 21 juin 2004 créée un référé spécial en matière d'internet. Cet article prévoit que « *l'autorité judiciaire peut prescrire en référé ou sur requête, à* [l'hébergeur] *ou, à défaut,* [au fournisseur d'accès], *toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ». Pour ne pas contrevenir au principe d'absence d'obligation générale de surveillance, cette procédure est soumise à un encadrement strict : elle doit être nécessairement assortie d'un délai d'exécution. Ainsi, le juge des référés[1046] a prescrit le 10 février 2012 une mesure de blocage du site *Copwatch* limitée à six mois afin de ne pas méconnaître les principes rappelés par la Cour de cassation et la Cour de justice de l'Union européenne. De plus, dans le cadre de la procédure de référé internet, le prestataire technique est saisi *in rem* c'est à dire qu'à l'égard du contenu ou de l'activité faisant l'objet de poursuites[1047] assurant pour ce dernier une surveillance ciblée en plus d'une surveillance temporaire.

2) L'irresponsabilité de l'hébergeur en cas de connaissance de l'illicéité des contenus suivie d'un prompt retrait

385. La responsabilité du fait de l'inaction de l'opérateur du réseau social. Le fournisseur d'hébergement est irresponsable du seul fait des contenus qu'il stocke. Cependant,

[1044] CJUE, *Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) c/ Netlog NV*, 16 février 2012, aff. C-360/10.
[1045] LCEN, art. 6, I, 7, al. 2.
[1046] TGI Paris, ord. réf., 10 février 2012, n° 12/51224, Claude Guéant c/ Free et a. ; www.legalis.net.
[1047] F. DELIEGE, *La responsabilité des acteurs de l'internet en matière de délits de presse*, thèse Université Nancy 2, 2006, p. 139, n° 239.

la loi du 21 juin 2004 prévoit une atténuation à ce principe. Aux termes de l'article 6, I, 2 et 3, ce dernier devient responsable lorsqu'une faute d'abstention peut lui être imputée. En effet, ce texte impose au fournisseur d'hébergement d'agir dès lors qu'à la suite d'une notification de contenu il a eu effectivement connaissance de l'illicéité de ce contenu. Ce n'est donc pas l'activité d'hébergement mais l'inaction de l'hébergeur suite à une notification de contenu qui est source d'engagement de responsabilité. Le comportement fautif provient alors nécessairement d'une omission. Autrement dit, ce que l'on reproche à l'hébergeur, c'est de ne pas avoir mis un terme à la consultation de l'information manifestement illicite une fois que ce contenu lui a été notifié dans le respect rigoureux des prescriptions de l'article 6, I, 5[1048].

386. La responsabilité dépendante du prompt retrait. Pour ce faire, l'article 6 de la LCEN impose à l'hébergeur d'agir « *promptement* » pour retirer les données sans toutefois fixer de délai. L'appréciation du temps de réaction de l'hébergeur suite à la notification relève dans ce cas de l'appréciation du juge qui apparaît plutôt rigoureuse[1049]. La société Dailymotion a été reconnue responsable du fait de son inaction pour ne pas avoir supprimé des vidéos qui lui avaient été notifiées 5 à 7 jours auparavant[1050]. Dans une autre espèce, un délai de réaction de deux semaines a également été jugé excessif[1051]. Enfin, en première instance, les juges du fond ont considéré que YouTube n'avais pas satisfait son obligation en supprimant le contenu dans un délai de 5 jours[1052]. Au vu de ces jurisprudences, pour que le fournisseur d'hébergement agisse promptement, autrement dit, dans un temps proche de la connaissance effective du contenu, le temps de réaction doit se mesurer davantage en heures qu'en jours. Sur ce point, le potentiel de diffusion à grande échelle de l'information permis par les réseaux sociaux en ligne rend nécessaire une action rapide de leur part. Par conséquent, dès lors que l'illicéité manifeste d'une information est portée à leur connaissance, ou dès que la décision judiciaire leur est notifiée, ces derniers doivent faire le nécessaire pour empêcher toute consultation ultérieure de l'information. Partant, la faute d'absention de l'hébergeur est à la fois le fait générateur de la responsabilité civile et l'acte matériel

[1048] V. *infra* n° 457.
[1049] L. MARINO, *Responsabilités civile et pénal des fournisseurs d'accès et d'hébergement, op. cit.*, n° 53.
[1050] Paris, pôle 5, 1ère ch., 2 décembre 2014, n° 13/08052, TF1 et a. c/ Dailymotion et a. : *Gaz. Pal.* 5 mars 2015, n° 64, p. 20, note L. MARINO ; *JCP* E 2015, 1165, note J.-B. BELIN et L. CONTASSOT-VIVIER.
[1051] Paris, pôle 5, ch. 2, 4 février 2011, n° 09/21941, Google et a. c/ Aufeminin.com et a. : *Légipresse* 2011, p. 209, n° 282-16 ; L. MARINO, « Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », J.-Cl. Comm., Fasc. 670, 30 août 2015 (dernière mis à jour 1er décembre 2017), n° 53.
[1052] TGI Paris, 3ème ch., 1ère sect., 29 mai 2012, TF1 et a. c/ YouTube : L. MARINO, « Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl.* Comm., Fasc. 670, 30 août 2015 (dernière mis à jour 1er décembre 2017), n° 53.

engageant sa responsabilité pénale. Il s'agit, en quelque sorte, d'une commission par omission[1053].

387. Les incertitudes du régime de responsabilité pénale de l'hébergeur. Selon l'article 6, I, 3 de la LCEN, la responsabilité pénale du fournisseur d'hébergement ne peut être engagée que s'il n'avait « *pas effectivement connaissance de l'activité ou de l'information illicites* » ou si, dès le moment où il en a eu connaissance, il n'a pas « *agi promptement pour retirer ces informations ou en rendre l'accès impossible* ». Cependant, aucune sanction n'est spécifiquement prévue pour ce comportement poussant alors à s'interroger sur le type de responsabilité pénale applicable au fournisseur d'hébergement. À cet égard, il apparaît difficile de reconnaître une responsabilité pénale de l'hébergeur soit en tant qu'auteur soit en tant que complice du contenu stocké sur ses serveurs.

388. Il est dans un premier temps difficile de concilier le régime de repsonsabilié pénale de l'hébergeur avec les règles en matière de complicité, cette dernière exigeant la réunion simultanée de deux éléments incompatibles avec le comportement répréhensible. L'élément matériel, en premier lieu, implique notamment que l'acte complice ait été accompli antérieurement ou concomitamment à la réalisation de l'acte délictueux principal. L'article 121-7 du Code pénal exige effectivement que le complice ait « *facilité la préparation ou la consommation* » de l'infraction. En l'espèce, l'acte complice qui consiste en une abstention volontaire, intervient après l'acte délictueux. L'impossible complicité *a posteriori* interdit de considérer ce comportement comme pouvant relever d'un acte de complicité. En second lieu, l'élément moral, concerne la participation au projet délictuel « *en connaissance de cause* ». Or, dans l'hypothèse visée à l'article 6, I, 3, l'hébergeur n'acquiert la connaissance de l'activité ou de l'information illicite qu'après avoir fourni les moyens nécessaires à la réalisation de l'infraction constituée par celle-ci. L'élément moral n'est donc pas concomitant à l'élément matériel. Il ne serait donc pas possible, au regard du droit commun, de considérer que l'hébergeur ait pu faciliter la préparation ou la consommation du délit « *en connaissance de cause* », à moins, peut-être, que l'infraction ne soit répétée après que l'hébergeur ait acquis la connaissance de celle-ci, ou qu'elle soit continue. La Cour de cassation considère cependant que les délits de presse commis sur internet consistent en des infractions instantanées[1054] retirant toute possibilité de mise en œuvre de la responsabilité de l'hébergeur sur les critères définis par le droit commun. La LCEN n'instaurerait-elle pas en son article

[1053] F. DELIEGE, *La responsabilité des acteurs de l'internet en matière de délits de presse*, thèse Université Nancy 2, 2006, p. 159, n° 271.
[1054] Crim., 30 janvier 2001 : *Bull. crim.* n° 28 ; *JCP* éd. G 2001, II, n° 10515, note A. LEPAGE.

6, I, 3 un régime de complicité partiellement dérogatoire à celui visé à l'article 121-7 du Code pénal ? L'article 6, I, 3 permettrait ainsi de considérer l'hébergeur complice d'une infraction, quelle qu'en soit la nature, instantanée, répétée ou continue, dès lors qu'il se soustrait aux obligations posées par la loi du 21 juin 2004[1055]. Dès lors, deux solutions s'offrent au législateur, soit créer un régime de complicité spécifique aux hébergeurs, soit prévoir une sanction à leur éventuelle abstention fautive.

389. Si l'hébergeur ne peut être considéré selon les cas de complicité classique comme complice, sa responsabilité pénale doit s'envisager comme celle de l'auteur de l'infraction. Cependant, ce n'est pas l'hébergeur qui est à l'origine du contenu publié sur ses services, il ne peut donc être considéré comme l'auteur des délits qu'il héberge. L'hébergeur ne serait-il alors pas coupable d'un délit distinct à savoir celui de s'être abstenu de retirer le contenu illicite ? Ce comportement s'apprente en l'espèce au délit de recel tel que prévu par l'article 321-1 du Code pénal : l'hébergeur stocke un contenu tout en sachant que celui-ci est constitutif d'une infraction, il peut en être ainsi déduit qu'il détient le produit d'un crime ou d'un délit. Par ailleurs, le fait que l'opérateur du réseau social ne fasse pas suite à la notification du contenu peut également s'analyser comme le fait que ce dernier retire un avantage de laisser le contenu en ligne et donc qu'il bénéficie en quelque sorte du produit de l'infraction[1056]. Cette analyse permettrait d'assimiler dans cette hypothèse l'hébergeur à un receleur d'autant plus que l'article 321-12 du Code pénal précise que les personnes morales peuvent être déclarées responsables du délit de recel. L'hébergeur encourerait en tant que personne morale une amende de 1 875 000 € correspondant, en application de l'article 131-38 du Code pénal, au quintuple de l'amende encourue par les personnes physiques.

390. Conclusion de la Section 2. L'assimilation des opérateurs des réseaux sociaux à des fournisseurs d'hébergement a pour conséquence d'engager à leur égard l'application du système de responsabilité avantageux des intermédiaires techniques. Ce régime juridique favorable s'observe dans un premier temps à l'égard des obligations applicables aux opérateurs des réseaux sociaux en leur qualité d'hébergeurs. Ainsi, le respect de l'obligation de conservation et de transmission des données posée par la LCEN dans le but d'assurer la poursuite effective d'auteurs d'infractions agissant de manière anonyme est rendue difficile en raison du manque d'automaticité de la coopération des grands acteurs d'internet en la matière.

[1055] L. THOUMYRE, « les hébergeurs en ombres chinoises. Une tentative d'éclaircissement sur les incertitudes de la LCEN », *RLDI*, 2005, p. 58.
[1056] Le recel est en l'occurrence une infraction de conséquence qui suppose l'existence d'une infraction préalable et la réunion d'éléments constitutifs qui lui sont propres. V. C. pén. art. 321-1.

Mais plus encore, les opérateurs des réseaux sociaux bénéficient d'un système de responsabilité modéré voire, d'un quasi régime d'irresponsabilité. En effet, la LCEN leur reconnaît dans un premier temps une absence d'obligation générale de surveillance qui se justifie en raison de la quantité de données considérable que ces acteurs sont amenés à héberger. Leur responsabilité pénale ne peut alors être engagée que dans l'hypothèse où suite à une notification de contenu illicite les opérateurs des réseaux sociaux n'auraient pas retiré promptement un contenu apparaissant comme manifestement illicite. Ce système de responsabilité avantageux se fonde en l'occurrence sur le rôle purement technique assigné aux hébergeurs et donc sur leur neutralité dans la diffusion des contenus. Or, cette vision classique du réseau social bénéficiant d'une responsabilité modérée en raison de sa qualité d'hébergeur n'est cependant plus en phase avec la réalité technique qu'offrent ces sites. L'apparition de tels acteurs est en réalité de nature à justifier la refonte du système de responsabilité applicable aux acteurs d'internet[1057].

[1057] V. *infra*. Partie 2, Titre 2, Chapitre 2, Section 1.

Conclusion du Chapitre 1

391. Les opérateurs des sites de réseaux sociaux peuvent engager leur responsabilité pénale sur deux fondements. Ces derniers sont en premier lieu des responsables de traitement de données à caractère personnel. Sous couvert de cette qualité ils peuvent engager leur responsabilité pénale sous le fondement du droit commun et plus particulièrement des infractions prévues aux articles 226-16 et suivants du Code pénal. Ces infractions renvoient en réalité aux obligations issues de la loi informatique et libertés et à l'échelle européenne, au règlement général sur la protection des données. La présence d'un dispositif pénal dissuasif en la matière n'est toutefois pas garant du bon respect par les opérateurs des sites de réseaux sociaux des obligations relatives à la protection des données et d'une mise en œuvre concrète de ces textes à leur égard. Ce constat est d'autant plus renforcé par la présence d'accords internationaux venant légitimer le transfert de données à caractère personnel hors de l'Union européenne. En réalité, la mise en jeu de la responsabilité des opérateurs des sites de réseaux sociaux se situe davantage sur le plan administratif par le biais de l'action sanctionnatrice de la CNIL en la matière. L'enjeu consiste alors pour cette dernière à mobiliser ses pouvoirs de sanction de manière à dissuader les grands responsables de traitement de continuer leurs mauvaises pratiques.

392. Les opérateurs des réseaux sociaux peuvent également engager leur responsabilité pénale sous le fondement de la loi pour la confiance en l'économie numérique en leur qualité d'hébergeur. Ce régime particulier permet de sanctionner un hébergeur pour un contenu diffusé sur sa plateforme par un internaute. Il s'agit toutefois d'un régime de responsabilité favorable conditionné à la prise de connaissance effective du contenu illicite par l'hébergeur auquel il est par ailleurs reconnu une absence d'obligation générale de surveillance. L'organisation d'un régime de responsabilité favorable était justifiée à l'origine par le rôle purement technique auquel étaient assignés les hébergeurs. Or, l'émergence des grandes plateformes numériques et particulièrement des réseaux sociaux en ligne est toutefois aujourd'hui de nature à remettre en cause l'application à leur égard d'un tel régime de responsabilité[1058].

[1058] V. *Infra.* Partie 2, Titre 2, Chapitre 2, Section 1.

Chapitre 2 – La sévérité de la responsabilité pénale des utilisateurs des réseaux sociaux

393. Une responsabilité pénale sous deux fondements. L'utilisateur d'un réseau social peut engager sa responsabilité pénale consécutivement à un comportement délictueux qu'il aurait commis au moyen de ce dernier. Dans le cas présent, sa responsabilité pénale revêt un caractère plus sévère que celle des opérateurs des réseaux sociaux du fait que les utilisateurs sont considérés, sur le fondement du droit pénal commun et du droit de la presse, comme auteur principal du fait délictueux. De surcroît, les deux régimes de responsabilité pénale applicables à l'égard des utilisateurs des réseaux sociaux démontrent chacun d'eux une particulière sévérité à leur égard. Le droit pénal commun marque en effet une intention répressive particulière et une politique pénale affirmée à l'égard des différentes formes de cybercriminalité y compris celles rencontrées sur les sites de réseaux sociaux. Par ailleurs, les propos tenus sur les sites de réseaux sociaux possèdent dans leur majorité un caractère public et constituent à ce titre une publication soumise au droit de la presse[1059]. En conséquence, les utilisateurs des réseaux sociaux engagent également leur responsabilité sur le fondement de la loi sur la liberté de la presse. Ce texte met en œuvre un régime particulier de responsabilité dite « *en cascade* » qui était destiné à l'origine aux professionnels des métiers de la communication et qui est désormais applicable à tout utilisateur d'un réseau social aussi amateur qu'il soit en la matière. Toutefois, la sévérité qui caractérise les régimes de responsabilité applicables aux utilisateurs des réseaux sociaux n'est pas gage pour autant d'une mise en jeu effective de cette dernière, particulièrement concernant les nombreux abus de la liberté d'expression rencontrés sur les sites de réseaux sociaux.

La sévérité des règles de responsabilité pénale applicables aux utilisateurs des sites de réseaux sociaux se retrouve à travers la mise en œuvre de leur responsabilité sur le fondement du droit pénal commun (**Section 1)** ainsi que dans l'inadaptation du système de responsabilité du droit de la presse applicable à leur égard (**Section 2**).

[1059] V. *supra* Partie 1, Titre 1, Chapitre 1, Section 1.

Section 1 : Une responsabilité pénale de droit commun empreinte de sévérité

394. De nombreuses infractions du droit pénal commun peuvent être commises au moyen des sites de réseaux sociaux, voire, à l'encontre de ces derniers[1060]. Dans ces hypothèses, l'utilisateur d'un réseau social en ligne peut engager sa responsabilité pénale selon les règles du droit pénal commun. Cependant, les règles applicables ou l'interprétation qui leur en ait donné met en évidence une certaine sévérité répressive à l'égard des utilisateurs des réseaux sociaux. Celle-ci se manifeste en raison du caractère extensif des personnes concernées par l'engagement de leur responsabilité pénale mais également en raison du régime d'aggravation applicable aux utilisateurs des réseaux de communication en ligne. Il sera ainsi distingué une sévérité quant aux personnes concernées (**§1**) et quant à la peine encourue (**§2**).

§1. Une sévérité quant aux personnes concernées

395. Le régime de responsabilité pénale prévu par le droit pénal commun est empreint de sévérité à l'égard des utilisateurs des réseaux sociaux en raison de l'étendue des personnes concernées. Ceci s'observe d'une part par l'interprétation extensive donnée à la notion de responsable d'un traitement permettant d'engager la responsabilité pénale des utilisateurs sous le fondement des articles 226-16 et suivants du Code pénal concurremment avec celle des opérateurs des réseaux sociaux (A). Cette sévérité s'observe d'autre part par l'adoption d'un cas de complicité visant une nouvelle forme de délinquance rencontrée sur les sites de réseaux sociaux (B).

A. Une interprétation extensive de la notion de responsable d'un traitement

396. La responsabilité pénale de l'utilisateur pour son activité de traitement de données. Lorsque l'activité d'un utilisateur d'un réseau social entre sous la qualification d'une infraction de droit pénal commun, ce sont les règles classiques de responsabilité qui s'appliquent. L'utilisateur d'un réseau social peut alors dans certains cas être assimilé au même titre que l'opérateur à un responsable d'un traitement de données (1) et donc engager sa responsabilité pénale sur ce fondement (2).

[1060] V. s*upra* Partie 1, Titre 1, Chapitre 2.

1) L'utilisateur d'un réseau social, un responsable d'un traitement de données

397. Le *webtracking*, un traitement de données. Si les entreprises mettant en œuvre un site de réseau social peuvent être assurément considérées comme un responsable d'un traitement de données[1061], la question se pose également à propos de l'utilisateur d'un réseau social lui-même. La Cour de justice de l'Union européenne[1062] a apporté des éléments de réponses en considérant que l'administrateur d'une page fan sur Facebook est conjointement responsable avec le réseau social du traitement des données des visiteurs de sa page au vu de la pratique du *webtracking*. L'assimilation de l'administrateur de la page fan, en l'espèce celle de l'entreprise de formation allemande *Wirtschaftsakademie* (nommée ci-après l'académie), à un responsable d'un traitement de données s'est déduite d'une analyse *in concreto* de la pratique du *webtracking* mise en œuvre sur le réseau social Facebook. Cette pratique, consiste à observer et analyser les comportements des utilisateurs d'internet à des fins commerciales et de marketing, permettant notamment d'identifier leurs centres d'intérêt à partir de l'observation de leurs comportements de navigation et grâce à l'utilisation de leurs *cookies*.

398. La Cour de justice rappelle que les pages fan sont des comptes d'utilisateurs qui peuvent être configurés sur Facebook par des particuliers ou des entreprises. À ce titre, l'auteur de la page fan peut utiliser la plateforme aménagée par le réseau social pour promouvoir son activité aux utilisateurs et particulièrement aux personnes visitant la page fan. Afin de mieux cibler leur public, les administrateurs de pages fan peuvent obtenir des données statistiques anonymes concernant les visiteurs de ces pages à l'aide d'une fonction intitulée *Facebook Insight*, mise gratuitement à leur disposition par le réseau social. Ce *webtracking* a été utilisé dans le but d'optimiser et de configurer de manière plus effective un site web, en l'occurrence celui de l'Académie. Le traçage des comportements de navigation a permis de fournir aux exploitants du site des statistiques d'audience relatives aux personnes qui le consultaient. La Cour en a ainsi déduit que la page fan de l'académie opérait un traitement de données personnelles au regard du droit européen[1063].

399. La capacité de l'administrateur à influer sur les finalités et les moyens du traitement. La Cour a en outre reconnu un pouvoir d'influence de l'administrateur sur les finalités et les moyens du traitement. Pour ce faire, elle relève que toute personne souhaitant créer une page fan sur Facebook conclut avec le réseau social un contrat spécifique relatif à

[1061] V. *supra* n° 124.
[1062] CJUE, *Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 juin 2018, aff. C-210/16 : *JCP* G, n° 28, 9 juillet 2018, note D. BERLIN ; *RLDI*, 2018, n° 149, L. COSTES.
[1063] CJUE, *Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 juin 2018, aff. C-210/16, n° 15, précit.

l'ouverture d'une telle page et souscrit, à cette occasion, aux conditions d'utilisation de cette page notamment celle concernant la politique d'utilisation des cookies. Ce traitement de données à caractère personnel permet, d'une part, à Facebook d'améliorer son système de publicité qu'il diffuse à travers son réseau et d'autre part, à l'administrateur de la page fan d'obtenir des statistiques établies par le réseau social à partir des visites de cette page. Les juges en concluent alors que « *si le simple fait d'utiliser un réseau social tel que Facebook ne rend pas un utilisateur de Facebook coresponsable d'un traitement de données à caractère personnel effectué par ce réseau, il convient, en revanche, de relever que l'administrateur d'une page fan hébergée sur Facebook, par la création d'une telle page, offre à Facebook la possibilité de placer des cookies sur l'ordinateur ou sur tout autre appareil de la personne ayant visité sa page fan, que cette personne dispose ou non d'un compte Facebook* »[1064]. Partant, la création d'une page fan sur Facebook induit de la part de son administrateur une action de paramétrage en fonction de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, ce qui est de nature à influer sur le traitement de données à caractère personnel[1065]. Par conséquent il est logique de considérer l'administrateur d'une page fan hébergée sur Facebook comme étant coresponsable avec le réseau social du traitement des données à caractère personnel des visiteurs de sa page.

2) La responsabilité pénale de l'administrateur d'une page fan sur Facebook

400. Une responsabilité conjointe avec le réseau social. La Cour de justice de l'Union européenne a retenu que l'administrateur d'une page fan hébergée sur un réseau social pouvait engager sa responsabilité en cas d'atteinte aux règles relatives à la protection des données à caractère personnel. La Cour rappelle que la directive 95/CE, en vigueur au moment des faits, définit de manière large la notion de responsable d'un traitement comme visant : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* »[1066]. Il ressort de cette définition que la notion de responsable

[1064] CJUE, 5 juin 2018, aff. C-210/16, n° 35, précit.
[1065] Par exemple : « *l'administrateur de la page fan peut demander à obtenir –et donc que soient traitées – des données démographiques concernant son audience cible, notamment des tendances en matière d'âge, de sexe, de situation amoureuse et de profession, des informations sur le style de vie et les centres d'intérêt de son audience cible ainsi que des informations concernant les achats et le comportement d'achat en ligne des visiteurs de sa page, les catégories de produits ou de services qui l'intéressent le plus, de même que des données géographiques qui permettent à l'administrateur de la page fan de savoir où effectuer des promotions spéciales ou organiser des événements et, de manière plus générale, de cibler au mieux son offre d'informations* », CJUE, 5 juin 2018, aff. C-210/16, n° 37, précit.
[1066] CJUE, *Google Spain c/ Mario Costeja González*, 13 mai 2014, grde ch., aff C-131/12, n° 34.

d'un traitement de données ne renvoie pas nécessairement à un organisme unique et peut concerner plusieurs acteurs participant à ce traitement, chacun d'eux étant soumis aux obligations de la directive. La Cour précise alors que la société Facebook Inc. et plus précisément Facebook Ireland concernant le droit de l'Union européenne, doivent être assimilées au responsable du traitement à titre principal du fait qu'elles déterminent les finalités et les moyens du traitement des données à caractère personnel de leurs utilisateurs mais également des personnes ayant simplement visité les pages fan hébergées sur leur site sans en être pour autant membres[1067]. Cependant, les juges ne s'arrêtent pas là et affirment que l'administrateur de la page fan a également contribué à déterminer, conjointement avec le réseau social, les finalités et les moyens du traitement. Dès lors, l'administrateur de la page peut engager sa responsabilité pénale au titre des articles 226-16 et suivants du Code pénal conjointement avec l'opérateur du réseau social en sa qualité de responsable d'un traitement automatisé de données.

401. Une Responsabilité justifiée par la qualité de professionnel de l'administrateur. Cette décision doit s'analyser en outre au regard du statut que possédait l'entreprise allemande. Cette dernière agissait sur le réseau social dans le cadre de son activité et donc à titre professionnel. La qualité de professionnel est sur ce point essentielle au regard du nouveau règlement européen sur la protection des données pour être reconnu comme responsable d'un traitement de données. Selon le droit européen, les obligations pesant sur un responsable d'un traitement de données ne s'appliquent pas aux traitements effectués par une personne physique n'agissant pas en qualité de professionnel, c'est-à-dire, au cours d'une activité strictement domestique ou personnelle[1068]. En définitive, l'usage d'un réseau social à titre professionnel ou non professionnel est ici de nature à influer sur la responsabilité pénale de l'utilisateur. Cette distinction semble de ce fait introduire une notion objective justifiant l'engagement ou non de la responsabilité du simple utilisateur.

[1067] CJUE, 5 juin 2018, aff. C-210/16, n° 30, précit.

[1068] « *Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques* ». RGPD, considérant n° 18.

B. L’émergence d’un cas de complicité en ligne

402. Un cas de complicité *sui generis*. Avec l’émergence de la pratique du *happy slapping* consistant à filmer la commission de violences sur autrui en vue de diffuser les images, le législateur est intervenu par la loi n° 2007-293 du 5 mars 2007[1069] venant créer le nouvel article 222-33-3 du Code pénal. Ce dernier prévoit non seulement une infraction autonome de diffusion d’images de violences[1070] mais également une présomption légale de complicité pour le preneur d’images. Aussi, le premier alinéa de l’article 222-33-3 dispose : « *Est constitutif d’un acte de complicité des atteintes volontaires à l’intégrité de la personne prévues par les articles 222-1 à 222-14-1 et 222-23 à 222-31 et 222-33 et est puni des peines prévues par ces articles le fait d’enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission de ces infractions* ». Cette technique d’assimilation légale n’est toutefois pas nouvelle et se retrouve dans d’autres textes sous diverses formules[1071]. Le législateur a en l’espèce estimé opportun de punir spécifiquement l’acte initial d’enregistrement en l’assimilant par une présomption légale à un cas de complicité de l’infraction principale dont est objet l’enregistrement. En conséquence, l’utilisateur d’un réseau social se livrant à la pratique du *happy slapping* peut engager sa responsabilité pénale, d’une part, en tant qu’auteur principal de l’infraction de diffusion d’images de violences prévue au deuxième alinéa de l’article 222-33-3 du Code pénal et d’autre part, en tant que complice de l’infraction faisant l’objet de l’enregistrement au titre du premier alinéa du même texte. Au-delà de permettre à l’utilisateur d’un réseau social d’être poursuivi sous deux fondements, ce cas de complicité *sui generis* est d’une sévérité particulière du fait qu’il déroge à l’ensemble des règles applicables en matière de complicité[1072]. En effet, sous l’égide de ce régime, la complicité peut être qualifiée sans qu’il y ait eu concertation entre les agents et indépendamment du fait que le complice ait favorisé la commission de l’infraction principale[1073]. La spécificité et la sévérité de ce régime de

[1069] L. n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance, *JORF* n° 55, 6 mars 2007, p. 4215.
[1070] V. *supra* n° 145.
[1071] Monsieur Stéphane Detraze relève ainsi que des cas de « *présomption de complicité* » existent déjà en législation et se retrouvent par diverses formules : « *est considéré comme complice* » (C. com., art. L. 322-5, al. 2), « *est tenu comme complice* » (C. env., art. L. 218-34, III), « *peut être retenu comme complice* » (C. env., art. L. 218-50, al. 2), « *sont considérés comme complices* » (C. just. mil., art. L. 122-4). S. DÉTRAZ, « L'enregistrement d'images de violence : un cas de présomption légale de complicité », *Dr. pén.* 2007, n° 11, étude 23.
[1072] V. S. FOURNIER, Rép. pén. Dalloz, janvier 2013, *V°* Complicité, n° 72.
[1073] M.-H. GALMARD, « L'incrimination de la pratique du "vidéolynchage" ou la rupture du lien de causalité entre l'acte de complicité et l'infraction principale », *RPDP* 2007, n° 3, p. 583.

« *complicité en ligne* »[1074] seront ainsi décrites à travers ses éléments constitutifs (1) et ses règles applicables en matière de répression (2).

1) Les éléments constitutifs de l'acte de complicité

403. Un cas de complicité sur le modèle d'une infraction. Le premier alinéa de l'article 222-33-3 du Code pénal met en œuvre une présomption de complicité concernant un acte d'enregistrement relativement éloigné du concept habituel de complicité. La qualification de cette hypothèse particulière de complicité peut donc être retenue alors même que les conditions d'ordre matériel et moral posées par l'article 121-7 du Code pénal ne sont pas entièrement remplies. Selon Monsieur Stéphane Detraze, « *l'acte de complicité institué à l'article 222-33-2 du Code pénal est textuellement construit comme une infraction à part entière* »[1075]. Il peut alors être distingué un élément matériel (a) et un élément moral (b).

a- L'élément matériel

404. Les infractions visées par le texte. L'hypothèse de complicité prévue à l'article 222-33-3 du Code pénal renvoie à des infractions spécifiques, plus précisément aux actes de torture et de barbarie prévus aux articles 222-1 à 222-6-2, les violences incriminées par les articles 222-7 à 222-14-1 ainsi que les agressions sexuelles, notamment le viol, prévues aux articles 222-23 à 222-31 et le harcèlement sexuel prévu à l'article 222-33. En dehors de ces qualifications spécifiques, ce cas de complicité ne peut être observé. Ceci étant, l'article 222-33-3 du Code pénal reste applicable lorsque l'hypothèse d'atteinte volontaire à l'intégrité physique auquel renvoie ce texte ne constitue pas l'infraction principale mais la circonstance aggravante de l'acte délictueux[1076].

405. Des images relatives à la commission de ces infractions. L'acte de complicité consiste à enregistrer « *des images relatives à la commission de ces infractions* ». Le terme « *images* » renvoie ici à la représentation visuelle et parfaite d'une chose par un procédé technique le permettant. Sont ainsi exclues la représentation graphique de la personne ou la fixation sonore de la scène de violence. Le terme « *images* » est par ailleurs rédigé au pluriel ce qui induit que l'enregistrement d'une seule image, une photographie par exemple, n'entre

[1074] V. CANTAT-LAMPIN, « Les atteintes à la personne par le biais des communication électroniques. Une réponse imparfaite du droit pénal. », *in* Mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, p. 352.
[1075] S. DÉTRAZ, « L'enregistrement d'images de violence : un cas de présomption légale de complicité », *Dr. pén.* 2007, n° 11, étude 23.
[1076] *Ibid.*, n° 19.

pas dans les prévisions de ce cas particulier de complicité. Les images doivent être par ailleurs « *relatives à la commission* » des atteintes à l'intégrité d'autrui. L'enregistrement doit intervenir au moment où l'infraction est en cours d'exécution comprenant l'étape d'exécution mais également celle de la tentative. À l'inverse, l'enregistrement des actes préparatoires ou de la période postérieure à la consommation de l'infraction ne peuvent constituer l'acte de complicité prévu à l'article 222-33-2 du Code pénal. En définitive, les images doivent permettre « *de visualiser l'infraction en train ou sur le point de se commettre* »[1077].

406. L'acte d'enregistrement. L'acte d'enregistrement évoque le fait de « *transcrire et fixer sur un support matériel (disque, bande magnétique, papier, film, etc.) une information (son, image, phénomène)* »[1078]. La lecture du texte renvoie en l'occurrence à l'enregistrement d'une suite d'images constitutives d'un film mais n'exclut pas pour autant l'enregistrement de plusieurs images isolées. En revanche l'action de l'enregistrement doit être effectuée au moment où les actes de violences sont commis, autrement dit, la reproduction postérieure d'images sur un autre support, par exemple d'un disque dur vers un ordinateur, n'entre pas dans les circonstances de l'acte de complicité. Ce dernier vise à punir « *l'enregistrement visuel des violences, par élaboration d'images* » ce qui diffère du fait de procéder à « *la reproduction des images préalablement créées au moment des faits* »[1079].

b- L'élément moral

407. Le dol général. L'acte de complicité prévu à l'article 222-33-3 alinéa 1er du Code pénal est intentionnel, l'enregistrement doit être en conséquence réalisé sciemment. Ceci implique d'une part que l'agent ait accompli volontairement l'acte d'enregistrement des images de violences. Cependant, l'élément intentionnel nécessite également que l'auteur de l'enregistrement ait eu conscience que les images sont relatives à l'une des infractions énoncées par le texte. Il peut arriver dans ce cas que l'auteur de la vidéo s'associe consciemment à une atteinte illicite sans pour autant en connaître la qualification exacte. Dans cette hypothèse, les règles générales en matière de complicité sont applicables. Le complice sera réputé avoir accepté de se soumettre à la qualification correspondant aux faits accomplis par l'auteur principal. Toutefois, si l'individu pensait filmer une atteinte d'une plus grave importance il n'encourra pour autant que la qualification applicable à l'infraction réellement

[1077] *Ibid.*, n° 24.
[1078] Dictionnaire Larousse en ligne, *V°* Enregistrer.
<https://www.larousse.fr/dictionnaires/francais/enregistrer> (dernière consultation le 9 octobre 2019).
[1079] S. DÉTRAZ, « L'enregistrement d'images de violence : un cas de présomption légale de complicité », *op. cit.*, n° 27.

exécutée. À l'inverse, si le complice pensait enregistrer une atteinte d'une moindre gravité à celle réellement exécutée, la complicité sera caractérisée si le degré de gravité supérieur résulte de l'existence d'une circonstance aggravante propre au fait principal. La complicité est cependant exclue lorsque la personne réalisant l'enregistrement a cru à une atteinte moins grave sujette à une autre qualification que celle s'appliquant aux faits accomplis[1080].

408. Des faits justificatifs spéciaux. Le législateur a retenu au troisième alinéa de l'article 222-33-3 du Code pénal deux hypothèses particulières venant attester de la bonne foi de l'auteur de l'enregistrement et justifiant la non application de ce régime de complicité. Le premier fait justificatif spécial est déduit lorsque l'enregistrement ou la diffusion « *résulte de l'exercice normal d'une profession ayant pour objet d'informer le public* ». Cette première hypothèse ne peut alors bénéficier qu'aux seuls journalistes professionnels excluant tout journaliste amateur ou simple citoyen. De plus, l'acte d'enregistrement doit intervenir dans le cadre de « *l'exercice normal* » de sa profession. La seconde hypothèse permettant d'exclure la responsabilité pénale du preneur d'image est lorsqu'il est démontré que l'enregistrement a été réalisé « *afin de servir de preuve en justice* ». Cet élément exonératoire est ainsi purement psychologique[1081] et nécessite d'établir qu'au moment des faits l'auteur de l'enregistrement était effectivement animé par une telle intention. En outre, les faits justificatifs généraux tels que le commandement de l'autorité légitime, l'ordre ou la permission de la loi, l'état de nécessité, demeurent applicables à cette hypothèse particulière de complicité.

2) Les règles applicables en matière de répression

409. L'emprunt de pénalité. La qualification de l'acte de complicité soumet l'individu qui a réalisé l'enregistrement des images de violences aux mêmes peines que celles encourues par l'auteur de l'infraction principale. Le législateur a ainsi mis en œuvre un système répressif « *particulièrement rigoureux* »[1082] en la matière. Il convient alors de préciser dans quelle mesure les circonstances aggravantes sont communicables de l'auteur de l'infraction principale au complice qui filme cette dernière. En l'espèce, les circonstances aggravantes réelles, c'est-à-dire tenant aux circonstances de l'action ou à la personne de la victime, sont parfaitement applicables au complice. En revanche, les circonstances aggravantes personnelles relevant de la personnalité de l'agent ne seront applicables au complice que lorsqu'elles sont de nature à s'appliquer également à ce dernier.

[1080] *Ibid.*, n° 35.
[1081] *Ibid.*, n° 38.
[1082] *Ibid.*, n° 53.

410. Concours de l'acte de complicité avec d'autres infractions. Enfin, ce cas de complicité *sui generis* peut entrer en concours avec d'autres qualifications pénales, en particulier celles de non-assistance à personne en danger ou de non-obstacle à la commission d'un crime ou d'un délit contre les personnes[1083] mais également l'infraction de l'enregistrement de l'image ou de la représentation d'un mineur présentant un caractère pornographique[1084]. Il conviendrait dans cette hypothèse d'appliquer la règle « *speciala generalibus derogant* » et de privilégier ainsi l'hypothèse nouvelle de complicité. Or, cette solution aboutirait dans certains cas, particulièrement en cas de violences légères n'ayant entrainé aucune ITT, à faire encourir au complice une sanction moindre que celle prévue notamment pour l'infraction de non-assistance à personne en danger. Dans cette hypothèse particulière, la mise en œuvre de ce cas spécial de complicité manquerait alors à l'objectif répressif qui avait animé le législateur[1085].

§2. Une sévérité quant à la peine encourue

411. Une aggravation justifiée. La sévérité de la responsabilité pénale sous le fondement du droit commun s'observe également quant aux peines encoures suite à l'utilisation d'un réseau social dans un but criminel ou délinquant. L'utilisation d'un réseau social dans un tel but constitue en effet une source justifiée d'aggravation de la répression. Les réseaux sociaux en ligne sont un outil de communication qui facilite le passage à l'acte dès l'instant où ils permettent que les échanges soient réalisés de façon anonyme, à distance et nécessairement de manière indirecte du fait que l'auteur ne soit pas confronté avec sa victime. L'augmentation significative de la délinquance liée à l'usage sous toutes leurs formes des moyens de communication en ligne justifie en conséquence une réponse ferme et systématique à toute forme d'atteinte qu'elle soit le principal ou l'accessoire d'une action délictueuse[1086]. L'utilisation d'un moyen de communication en ligne devient alors une source d'aggravation pénale dans nombre d'infractions existantes. Ainsi, l'usage d'un site de réseau social dans un dessein infractionnel peut constituer à plus d'un titre une circonstance aggravante. L'aggravation peut résulter soit de la mise en contact de l'auteur des faits et de la victime sur

[1083] C. pén., art. 223-6.
[1084] C. pén., art. 227-23.
[1085] En ce sens : S. DÉTRAZ, « L'enregistrement d'images de violence : un cas de présomption légale de complicité », *op. cit.*, n[os] 51 et 52.
[1086] T. CASSUTO, « Usurpation d'identité numérique », *AJ Pénal* 2010, p. 220.

un réseau social (A), soit de l'utilisation d'un réseau social comme moyen de commettre l'élément incriminé (B).

A. L'aggravation résultant de la mise en contact de l'auteur des faits et de la victime sur un réseau social

412. La présence d'une telle aggravation. L'utilisation d'un réseau social et plus généralement d'un réseau de communication électronique est retenue comme circonstance aggravante lorsque ces derniers ont servi à mettre en contact la victime d'une infraction avec l'auteur des faits. La loi n° 98-468 du 17 juin 1998, relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs[1087], a pour la première fois intégrer la notion de réseau de communication comme mode opératoire de certaines infractions sexuelles classiques[1088]. Son article 13 aggrave un certain nombre de comportements lorsque « *la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique* ». Cette circonstance aggravante se retrouve pour diverses infractions de nature sexuelle et est particulièrement appliquée lorsque la victime de l'infraction est mineure. Elle porte par exemple les peines à vingt ans de réclusion criminelle en cas de viol[1089], à sept ans d'emprisonnement et 100 000 euros d'amende pour les agressions sexuelles[1090], à cinq ans d'emprisonnement et 75 000 euros d'amende dans l'hypothèse d'un recours à la prostitution[1091], à sept ans d'emprisonnement et 100 000 euros d'amende en cas de corruption de mineurs[1092], ou encore à dix ans d'emprisonnement et 150 000 euros d'amende pour les atteintes sexuelles sur mineur[1093].

413. La justification d'une telle aggravation. Cela s'explique par l'utilisation de plus en plus fréquente d'internet et en particulier des sites de réseaux sociaux par les mineurs dans un but de communiquer. En l'occurrence, les réseaux de rencontre en ligne accessibles aux plus jeunes se sont considérablement développés et ont permis aux cyberdélinquants d'atteindre

[1087] L. n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, *JORF* n° 0139, 18 juin 1998, p. 9255.
[1088] A.-S. CHAVENT-LECLERE, « Le renouveau des infractions sexuelles à l'ère d'internet », *in* Mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, p. 341.
[1089] C. pén., art. 222-24 8°.
[1090] C. pén., art. 222-28 6 °.
[1091] C. pén., art. 225-12-2 2°.
[1092] C. pén., art. 227-22.
[1093] C. pén., art. 227-26 4°.

avec une plus grande facilité leur victime[1094]. Cette circonstance aggravante se retrouve également dans d'autres types d'infractions comme celle de la traite des êtres humains dont les pénalités sont portées en pareille hypothèse à dix ans d'emprisonnement et de 1 500 000 euros d'amende[1095]. Au final, cette circonstance aggravante sanctionne l'entrée en contact avec la victime facilitée par le réseau internet. En conséquence, le législateur prend en considération une action se réalisant en amont dans *l'iter criminis* et relevant normalement des actes préparatoires à la commission d'une infraction qui se réalise pour sa part à travers d'autres comportements matériels distincts[1096].

B. L'aggravation résultant de l'utilisation d'un réseau social comme moyen de commettre l'élément incriminé

414. La prise en compte d'une telle aggravation pour les atteintes aux personnes. Le système d'aggravation pénale prévoit par ailleurs une sanction accrue lorsque l'infraction aurait été commise en lien ou au moyen d'un réseau social. La loi fait dans ces hypothèses référence à diverses formulations sans qu'il soit possible d'expliquer réellement ces disparités[1097]. Le législateur mentionne comme circonstance aggravante : l'utilisation d'un « *réseau de communication* »[1098], d'un « *réseau de communications électroniques* »[1099], d'un « *moyen de communication électronique* »[1100] ou encore d'un « *service de communication au public en ligne* »[1101]. Il en est ainsi notamment pour la traite des êtres humains[1102], pour le harcèlement[1103], pour le viol[1104], les autres agressions sexuelles[1105], le proxénétisme[1106] et le recours à la prostitution[1107], pour des délits mettant en péril ou portant atteinte à des mineurs[1108]. En revanche certaines incriminations ne bénéficient pas de ce régime

[1094] V. CANTAT-LAMPIN, « Les atteintes à la personne par le biais des communication électroniques. Une réponse imparfaite du droit pénal. », *in* Mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, p. 341.
[1095] C. pén., art. 225-4-2 5°.
[1096] A.-S. CHAVENT-LECLERE, « Le renouveau des infractions sexuelles à l'ère d'internet », *op. cit.*, p. 343.
[1097] M. DALLOZ, Rép. pén. Dalloz, juin 2017 (mis à jour août 2018), *V°* Circonstances aggravantes, n° 25.
[1098] Pour le recours à la prostitution : C. pén. art. 225-12-2 2º.
[1099] Pour la corruption de mineur : C. pén. art. 227-22.
[1100] Pour la transmission de l'image pornographique d'un mineur : C. pén. art. 227-23.
[1101] C. pén. art. 222-33-2-2 4° (pour le harcèlement moral) ; C. pén. art. 421-2-5 al. 2 (pour l'apologie de terrorisme).
[1102] C. pén., art. 225-4-2, 3°
[1103] C. pén., art. 222-33-2-2, al. 2, 4°
[1104] C. pén., art. 222-24, 8°
[1105] C. pén., art. 222-28, 6°
[1106] C. pén., art. 225-7, 10°
[1107] C. pén., art. 225-12-2, 2°.
[1108] C. pén., art. 227-22 : corruption de mineurs ; C. pén., 227-23, al. 3 : fixation, enregistrement ou transmission d'images de mineurs à caractère pornographique en vue de leur diffusion ; C. pén., 227-26.4° : atteinte sexuelle

d'aggravation alors même que l'utilisation d'un réseau de communication constitue pour ces dernières un moyen d'atteinte privilégié, c'est le cas notamment du délit de provocation au suicide prévu aux articles 223-13 et suivants.

415. L'absence d'une telle aggravation pour les atteintes aux biens. L'absence injustifiée d'un tel régime d'aggravation se retrouve également de manière générale dans les délits d'atteinte aux biens alors même que leurs éléments constitutifs sont parfaitement transposables dans l'environnement numérique[1109]. Ainsi, il n'est pas prévu une circonstance aggravante résultant de l'utilisation d'un moyen de communication électronique pour le délit d'escroquerie bien que cette forme de délinquance constitue le principal « *contentieux de masse* » de la cybercriminalité[1110]. Le même constat peut également être porté sur le délit de chantage dont les formes de réalisation se sont parfaitement transposées à l'utilisation d'internet[1111]. Ce constat a amené un auteur à regretter « *un tel manque de réflexion d'ensemble de la part du législateur sur cette circonstance aggravante* »[1112].

416. Conclusion de la Section 1. Loin de paraître inadapté, le régime de responsabilité pénale de droit commun applicable à l'utilisateur d'un réseau social est empreint de sévérité en raison des personnes concernées mais également des peines encourues. Cette affirmation se vérifie dans un premier temps par l'interprétation jurisprudentielle extensive de la notion de responsable d'un traitement de donnée. Ainsi, il a été reconnu que l'administrateur d'une page sur le réseau social Facebook peut engager sa responsabilité pénale au titre des articles 226-16 et suivants du Code pénal conjointement avec l'opérateur du réseau social en sa qualité de responsable d'un traitement automatisé de données. Cette conception large de la notion de responsable d'un traitement de données se justifie toutefois par la qualité de professionnel de l'utilisateur du réseau social en cause[1113] et par la pratique de *webtracking* à laquelle il se livrait. Dans un second temps, au-delà de l'interprétation jurisprudentielle excessive de certaines notions, le législateur a également créé de nouvelles dispositions permettant de

---

sur mineur de quinze ans) ainsi que pour la diffusion d'informations relatives à la fabrication d'explosif (C. pén., art. 322-6-1, al. 2) et pour la provocation directe ou l'apologie du terrorisme (C. pén., art. 421-2-5, al. 2).

[1109] V. *supra* n^{os} 111 et suiv.

[1110] Le rapport sur la cybercriminalité a relevé qu'en 2012, 63% des faits relevant de la cybercriminalité concernaient des escroqueries et abus de confiance. Précisément, 21 077 soit 34% du total des escroqueries et abus de confiance constatés. M. ROBERT, *Protéger les internautes. Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, p. 21.

[1111] Selon le rapport sur la cybercriminalité, en 2012 4% des faits relevant de la cybercriminalité concernaient des menaces ou chantages, soit 1374 faits. La proportion est toutefois bien plus forte pour ceux de ces faits qui sont motivés par une volonté d'extorsion de fonds: 22%. M. ROBERT, *Protéger les internautes. Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, p. 21.

[1112] M. DALLOZ, Rép. pén. Dalloz, juin 2017 (mis à jour août 2018), *V°* Circonstances aggravantes, n° 25.

[1113] En l'espèce : l'entreprise de formation allemande *Wirtschaftsakademie*.

retenir de manière étendue la responsabilité pénale des utilisateurs des réseaux sociaux. C'est le cas des dispositions de la loi n° 2007-293 du 5 mars 2007[1114] apportant de nouvelles solutions répressives en réponse au développement de la pratique du *happy slapping* en lien avec l'utilisation de ces moyens de communication. Le législateur a ainsi créé un cas de complicité *sui generis* s'affranchissant des éléments traditionnels de la complicité et s'apparentant davantage à une incrimination. Ce système répressif particulièrement rigoureux soumet l'individu qui a réalisé l'enregistrement d'images de violences aux mêmes peines que celles encourues par l'auteur de l'infraction principale. La sévérité du régime de responsabilité de droit commun applicable aux utilisateurs des réseaux sociaux se caractérise en outre par le système d'aggravation pénal mis en œuvre dès lors qu'une infraction est commise en lien avec l'utilisation d'un moyen de communication électronique. L'aggravation peut alors résulter de la mise en contact de l'auteur des faits avec la victime par un réseau social ou de son utilisation dans le but de commettre l'élément incriminé. Cette circonstance aggravante n'est toutefois pas prévue de manière homogène à toutes les infractions pouvant être commises au moyen d'un service de communication en ligne, particulièrement concernant certaines atteintes aux biens pour lesquelles un tel système d'aggravation serait justifié.

[1114] L. n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance, *JORF* n° 55, 6 mars 2007, p. 4215.

Section 2 : L'inadaptation du système de responsabilité de la loi de presse

417. L'utilisateur d'un réseau social, un éditeur de services. La LCEN fait assumer la responsabilité principale des contenus mis en ligne aux éditeurs de services. Ces derniers sont décrits à l'article 6, III, 1 de ladite loi comme étant « *les personnes dont l'activité est d'éditer un service de communication au public en ligne* ». Les éditeurs de services également appelés les « *fournisseurs de contenus* »[1115] sont, à la différence des prestataires techniques, à l'origine des contenus publiés, ou du moins peuvent avoir le choix ou la maîtrise de leur diffusion. Il en est ainsi du titulaire d'un compte d'un réseau social que ce dernier le soit à titre professionnel ou simplement amateur, du moment qu'il diffuse lui-même des informations ou données personnelles ou s'il laisse d'autres personnes utiliser son compte aux mêmes fins[1116].

418. Le système de responsabilité en cascade. Les dispositions de la loi du 29 juillet 1881 qui déterminent les infractions et les règles de procédure spécifiques sont applicables aux services de communication au public en ligne et donc aux éditeurs de services[1117]. L'article 93-3 de la loi du 29 juillet 1982[1118] transpose le régime de la responsabilité dite « *en cascade* »[1119] à la communication au public par voie électronique. Ce régime de responsabilité distingue une cascade de trois auteurs principaux, dite « *petite cascade* », selon laquelle le directeur de publication ou le codirecteur de publication sera poursuivi comme auteur principal, à défaut, l'auteur et à défaut de l'auteur, le producteur. Ces règles de responsabilité spécifiques appliquées aux utilisateurs des réseaux sociaux (**§1**) permettent de mettre en évidence les limites de ce régime de responsabilité (**§2**).

[1115] « *Le fournisseur de contenus peut être défini comme la personne qui souhaite émettre une information sur un réseau. Il s'agit, selon les cas, d'un simple particulier ou d'un professionnel, lequel charge sur la plate-forme des données qu'il a créé ou collectées sur un sujet déterminé. Le fournisseur d'informations a donc une totale maîtrise des informations qu'il diffuse par l'intermédiaire du réseau. Il se distingue "naturellement" de l'hébergeur en ce sens qu'il intervient intellectuellement, et non pas techniquement* ». H. BITAN, *Droit et expertise du numérique*, Coll. Lamy Axe Droit, 2015, p. 447, n° 567.

[1116] E. DERIEUX, « Réseaux sociaux et responsabilité des atteintes aux droits de la personnalité », *RLDI*, 2014, n° 100.

[1117] LCEN, art. 6, V. : « *Les dispositions des chapitres IV et V de la loi du 29 juillet 1881 précitée sont applicables aux services de communication au public en ligne et la prescription acquise dans les conditions prévues par l'article 65 de ladite loi* ».

[1118] L. n° 82-652, 29 juil. 1982, sur la communication audiovisuelle, *JORF* 30 juillet 1982, p. 2431.

[1119] Régime de responsabilité prévu à l'article 42 de la loi du 29 juillet 1881.

§1. Les règles de responsabilité appliquées aux utilisateurs de réseaux sociaux

419. Une responsabilité à plusieurs niveaux. La catégorie des éditeurs de services à laquelle peuvent être rattachés les utilisateurs des réseaux sociaux comprend diverses sous-catégories impliquant une mise en jeu de la responsabilité à différents degrés. Il faut dès lors distinguer sur le réseau social la responsabilité principale du directeur de publication (A) de la responsabilité subsidiaire de l'auteur du contenu (B).

A. La responsabilité principale du directeur de publication

420. Notion et régime. Le régime de responsabilité propre au directeur de publication sur les sites de réseaux sociaux (2) nécessite au préalable de l'identifier (1).

1) L'identification du directeur de publication sur les sites de réseaux sociaux

421. La notion de directeur de publication. Le premier alinéa de l'article 93-2 alinéa 1er de la loi du 29 juillet 1982 dispose : « *Tout service de communication au public par voie électronique est tenu d'avoir un directeur de la publication* ». Le directeur de publication est, traditionnellement, « *la personne chargée au sein de l'entreprise de rendre public le journal, l'ouvrage ainsi que tout écrit afin de le communiquer au public* ». Sur internet, il est la personne qui rend « *le message public, celui qui "dirige" le site Internet* »[1120]. Dans l'hypothèse où le fournisseur de contenu est une personne morale, le directeur de publication est « *le président du directoire ou du conseil d'administration, le gérant ou le représentant légal, suivant la forme de la personne morale* »[1121]. En revanche, si le fournisseur est une personne physique c'est à lui qu'est attribuée la qualité de directeur de publication[1122]. En matière de communication au public en ligne, l'identité du directeur de publication doit être mise à disposition du public[1123]. Cette exigence ne vaut toutefois pas pour les sites édités à titre non-professionnel dans le but de préserver l'anonymat du directeur de publication, ce dernier doit toutefois communiquer ses éléments d'identification personnelle à son hébergeur.

422. Identification du directeur de publication sur les sites de réseaux sociaux. Les sites de réseaux sociaux mettent en œuvre un service de communication au public en ligne et

[1120] A. CAPPELLO, « L'adaptation du régime de responsabilité pénale au support d'Internet », *in* N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, coll. Grands colloques, 2017, p. 198.
[1121] L. du 29 juillet 1982 sur la communication audiovisuelle, art. 93-2 al. 6.
[1122] L. du 29 juillet 1982 sur la communication audiovisuelle, art. 93-2 al. 7.
[1123] LCEN, art. 6, III, 1, c).

sont à ce titre soumis aux présentes dispositions. Il est en conséquence de rigueur d'identifier un directeur de publication assumant la responsabilité principale des contenus mis en ligne. Sur les réseaux sociaux ce sont les utilisateurs eux-mêmes qui revêtent la qualité d'éditeurs de services et c'est donc parmi eux qu'il revient d'identifier le directeur de publication. Cette qualité doit en ce cas être attribuée au titulaire du compte ou à l'administrateur de la page sur laquelle est publié le contenu. Ceci se justifie par sa capacité à agir sur les contenus publiés son espace, en les supprimant de lui-même ou en les notifiant au réseau social. Il est fréquent que le directeur de publication soit également l'auteur du message litigieux[1124]. Il se peut toutefois qu'il s'agisse de deux personnes distinctes. Ceci se vérifie dans l'hypothèse où un contenu constituant une infraction de presse est publié sur le compte d'un utilisateur par une personne autre que le titulaire de ce compte. Par exemple, un élu du Front National s'est vu condamner à 3000 euros d'amende en sa qualité de directeur de publication suite à la mise en ligne, par d'autres individus, de messages constitutifs d'une provocation à la haine raciale sur sa page Facebook[1125]. Enfin, dans l'hypothèse où le titulaire du compte est une personne morale, cette dernière ne peut être tenue responsable pénalement des propos publiés sur son compte[1126]. La qualité de directeur de publication est alors attribuée à son dirigeant qui n'est pas forcément la personne chargée de la gestion du compte ou de la page[1127].

2) Le régime de responsabilité du directeur de publication sur les réseaux sociaux

423. La responsabilité conditionnée du directeur de publication. En principe, la responsabilité pénale du directeur de publication est une responsabilité de plein droit, cependant, la loi organise un système de responsabilité atténuée. L'article 93-3 de la loi du 29 juillet 1982 propose de limiter la responsabilité de plein droit du directeur de la publication aux cas où « *le message incriminé a fait l'objet d'une fixation préalable à sa communication au public* ». Sur les réseaux sociaux, la responsabilité du directeur de publication serait donc difficile à mettre en œuvre du seul fait que les propos envoyés ou postés sont directement accessibles au public. Il n'existe aucun système de différé permettant de retenir une éventuelle responsabilité du directeur de publication. Cependant, un cas supplémentaire de

[1124] P. AUVRET et C. AUVRET, « Délits de presse sur Twitter et responsabilité », *Légipresse* n° 353, 12 octobre 2017, p. 481.
[1125] Nîmes, 3ème ch., 18 octobre 2013, n° 13/00447, Leila T. c/ Stéphane B. et Julien S. : *CCE* n° 2, Février 2014, comm. 23, É. CAPRIOLI.
[1126] Les personnes morales ne sont pas responsables pénalement des infractions de presse prévues par la loi du 29 juillet 1881 lorsqu'elles sont commises sur Internet conformément aux dispositions de l'article 93-2 alinéa 6 de la loi du 29 juillet 1982. V. par exemple pour une application de ce principe : civ. 1ère, 14 janvier 2016, n° 14-28.327 : inédit.
[1127] L. du 29 juillet 1982 sur la communication audiovisuelle, art. 93-2 al. 6.

non-responsabilité du directeur de publication a été introduit par la loi Hadopi du 12 juin 2009[1128], au dernier alinéa de l'article 93-3 de la loi du 29 juillet 1982. Selon ce dernier : « *lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de la publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message* ». Dans cette dernière hypothèse le directeur de publication a un régime de responsabilité comparable à celui de l'hébergeur[1129] : l'engagement de poursuites pénales dépendra de sa connaissance effective d'un propos illicite et de son manque de promptitude dans la suppression du message.

424. Connaissance effective du contenu publié. Dans un premier temps, le directeur de publication peut être exonéré de sa responsabilité s'il est démontré qu'il n'a pas eu la connaissance effective du contenu litigieux. Le meilleur moyen d'établir cette connaissance effective consiste à notifier le contenu au directeur de publication, cette notification permettant également d'évaluer son temps de réaction. Cependant, à la différence du régime des hébergeurs, le législateur n'a pas pris soin de préciser quelle forme prenait celle-ci. La démonstration de la connaissance effective peut donc être rapportée par tout moyen. Par exemple, en constitue la preuve, la remise en ligne du message litigieux par le directeur de publication[1130] mais aussi la réponse par le directeur de publication sur le forum au message incriminé[1131] ou encore l'aveu du directeur de publication[1132]. Plus généralement, la connaissance effective du contenu litigieux résulte des faits propres à chaque cas d'espèce, qu'il appartient aux juridictions saisies d'apprécier. La preuve d'une telle connaissance peut en outre être déduite de la qualité du directeur de publication. C'est précisément la démarche suivie par le juge de la Cour d'appel de Nîmes à propos de la condamnation de l'élu du Front

[1128] L. n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, *JORF* n° 0135, 13 juin 2009, p. 9666, texte n° 2.
[1129] V. en ce sens : J. BOYER, « La responsabilité "allégée" des directeurs de publication de services de communication au public en ligne à raison des messages d'internautes sur les espaces de contributions personnelles », *Légicom* n° 45, 2010/2, p. 80 ; A. LEPAGE, « Droit pénal des médias », *RPDP*, n° 1, janvier-mars 2017, p. 176. *Adde* : J. BOSSAN, « Responsabilité pénale en cascade dans la communication audiovisuelle et l'internet », *J.-Cl.* Comm., fasc. 142, septembre 2015 (mise à jour décembre 2017), n° 31 et suiv.
[1130] TGI Paris, 17ème ch., 9 octobre 2009, n° 08-02.523039 : *CCE* 2010, comm. 6, obs. A. LEPAGE ; *Dr. pén.* 2010, n° 28, chron. 5, obs. O. MOUYSSET.
[1131] Montpellier, 14 novembre 2012 : *Légipresse* 2013, n° 301, p. 14.
[1132] Crim., 30 octobre 2012, n° 11-88.562 : inédit ; *D.* 2013, p. 463, obs. E. DREYER.

National en tant que directeur de publication de sa page Facebook[1133]. En l'occurrence, le juge a déduit la connaissance effective des contenus litigieux du prévenu en raison de sa qualité de personnage public qui l'obligeait à une vigilance particulière. Par ailleurs, le paramétrage de confidentialité de son compte Facebook a également permis de déduire la connaissance effective du contenu. Monsieur Éric Caprioli remarque à ce titre qu' : « *à partir du moment où il a volontairement rendu public son mur Facebook en autorisant ses amis à y publier des commentaires,* […] *"il est devenu responsable de la teneur des propos publiés"* »[1134]. Au final, un paramétrage de confidentialité ouvert couplé avec un devoir de vigilance particulier à raison de la fonction du prévenu permet de déduire sur un réseau social la connaissance effective d'un contenu. Le titulaire d'un compte de réseau social ou d'une page personnelle ouverts aux commentaires de ses contacts ou de tiers doit garder la maîtrise éditoriale des contenus qui y gravitent, d'autant plus lorsque la personne entretient le compte à titre professionnel. On peut en déduire l'existence pour le directeur de publication d'une obligation particulière de surveillance concernant les propos dont il a la maîtrise éditoriale. Dès lors, ce dernier doit être capable de réagir avec promptitude pour ne pas engager sa responsabilité pénale du fait d'un contenu publié sur son espace personnel.

425. Promptitude de la réaction. Dans un second temps, s'il est rapporté que le directeur de publication a eu la connaissance effective du contenu publié, ce dernier doit supprimer le contenu en cause dans un prompt délai pour ne pas engager sa responsabilité pénale. Ce délai de réaction n'étant pas précisé par le législateur il paraît judicieux de raisonner par analogie à la jurisprudence rendue en la matière pour les hébergeurs[1135]. En l'occurrence il est exigé un délai de réaction très rapide, un délai de 48 heures entre la réception de la demande et la suppression du contenu ayant été jugée excessif[1136]. Concernant les réseaux sociaux, après avoir déduit la connaissance effective du contenu publié sur le mur du représentant régional du front national, le juge du tribunal correctionnel de Nîmes a déduit l'absence de promptitude dans la réaction en observant que le contenu litigieux fut publié le 24 octobre et que les enquêteurs constatèrent encore sa présence le 6 décembre. L'appréciation des exigences relatives au délai de retrait varient ici également en fonction de chaque situation. Le

[1133] Nîmes, 3ème ch., 18 octobre 2013, n° 13/00447, Leila T. c/ Stéphane B. et Julien S. : *CCE* n° 2, Février 2014, comm. 23, É. CAPRIOLI.
[1134] É. CAPRIOLI, « Condamnation d'un député pour des propos racistes publiés sur son mur Facebook », *CCE* n° 2, Février 2014, comm. 23.
[1135] C. BIGOT, *Pratique du droit de la presse*, Éd. Victoire, 2013, p. 224 ; J. BOYER, « La responsabilité "allégée" ds directeurs de publication de services de communication au public en ligne à raison des messages d'internautes sur les espaces de contributions personnelles », *Légicom* n° 45, 2010/2, p. 81.
[1136] TGI Toulouse, ord. Réf., 13 mars 2008 : <www.legalis.net>

juge pouvant faire preuve d'une plus grande souplesse à l'égard d'un directeur de publication agissant à titre particulier et non professionnel.

B. La responsabilité subsidiaire de l'auteur du contenu et du producteur

426. Le système de la « *petite cascade* » mis en œuvre par l'article 93-3 de la loi n° 82-652 du 29 juillet 1982[1137] prévoit une responsabilité subsidiaire d'une part pour l'auteur du contenu (1) et d'autre part pour le producteur (2).

1) La responsabilité de l'auteur du contenu

427. Condamnation en tant qu'auteur du propos. En raison de l'importance centrale de l'acte de publication dans la réalisation des infractions de presse, l'auteur du contenu litigieux est responsable au deuxième rang, lorsque l'identité du directeur de publication fait défaut. Il est cependant fréquent que l'auteur du contenu soit également le directeur de publication du contenu pour peu que le message soit publié dans l'espace dont la personne a la maîtrise, autrement dit, l'espace dont il est administrateur. Les exemples de condamnation sur le fondement de la loi de 1881 sont nombreux en la matière. Ainsi, un individu fut reconnu coupable du délit d'injure publique pour la diffusion d'un message sur son compte Facebook[1138]. De même pour la diffusion d'images incitant à la provocation à la haine raciale[1139] ou encore pour la diffusion d'une vidéo comportant des propos injurieux envers l'Urssaf[1140] ou envers la police[1141].

428. Condamnation en tant que complice du directeur de publication. L'auteur du contenu délictueux peut en outre engager sa responsabilité en tant que complice du directeur de publication, lorsque ce dernier est identifié comme auteur principal de l'infraction[1142]. Il s'agit d'un cas de complicité automatique qui n'exige pas de démonstration particulière autre que la qualité d'auteur du contenu délictueux[1143].

[1137] L. n° 82-652, 29 juil. 1982, sur la communication audiovisuelle, *JORF* 30 juillet 1982, p. 2431.
[1138] Nancy, 1ère ch. civ., 3 juillet 2018, n° 17/011693.
[1139] Dijon, ch. corr., 7 février 2018, n° 18/00081.
[1140] TGI Paris, 17ème ch., 30 juin 2017, Urssaf Ile-de-France c/ José X : *Légipresse* n° 354, novembre 2017, p. 529.
[1141] TGI Paris, 17ème ch., 7 juin 2017, Ministère public c/ Mohamed B. et Jenna K : *Légipresse* n° 354, novembre 2017, p. 529.
[1142] L'article 93-3 al. 3 de la loi du 29 juillet 1982 précise cette règle de manière explicite : « *Lorsque le directeur ou le codirecteur de la publication sera mis en cause, l'auteur sera poursuivi comme complice* ».
[1143] E. DREYER, *Responsabilité civile et pénale des médias*, Litec, 2ème éd., 2008, p. 372, n° 805.

2) La responsabilité du producteur

429. Assimilation du directeur de publication et du producteur sur les réseaux sociaux. Dernier acteur de la responsabilité en cascade, le producteur ne peut voir sa responsabilité pénale engagée que lorsque celle du directeur de publication et de l'auteur du contenu font défaut. La notion de producteur connaît diverses définitions en fonction du support sur lequel apparaît la publication litigieuse. Par exemple, l'article L. 132-23 du Code de la propriété intellectuelle précise que « *le producteur de l'œuvre audiovisuelle est la personne physique ou morale qui prend l'initiative et la responsabilité de la réalisation de l'œuvre* ». L'article L. 215-1 du même Code dispose que « *le producteur de vidéogrammes est la personne, physique ou morale, qui a l'initiative et la responsabilité de la première fixation d'une séquence d'images sonorisée ou non* ». À l'origine, la notion de producteur provient du monde de l'audiovisuel et était justifiée du fait qu'un propos diffamatoire prononcé en direct lors d'une émission de télévision ne pouvait engager la responsabilité du directeur de publication. Le législateur a alors établi le régime du producteur permettant de rechercher sa responsabilité dans cette situation. Dans le secteur de l'audiovisuel le producteur a donc une fonction précise et identifiable : il choisit le thème d'émission, son format, ses invités, etc[1144]. Cette fonction est cependant difficilement transposable sur internet, la notion de producteur venant se confondre avec celle de directeur de publication[1145]. Selon la jurisprudence, le producteur est la personne qui a pris l'initiative de créer un service de communication par voie électronique en vue d'échanger des opinions sur des thèmes définis à l'avance[1146]. Typiquement sur les réseaux sociaux, le producteur peut être assimilé à l'administrateur d'une page Facebook portant sur une thématique particulière. Cependant, cette personne est également le directeur de publication de cette page et peut ainsi engager sa responsabilité à titre principal. La question est en revanche plus épineuse concernant la reconnaissance du

[1144] J. BOYER, « La responsabilité "allégée" des directeurs de publication de services de communication au public en ligne à raison des messages d'internautes sur les espaces de contributions personnelles », *Légicom* n° 45, 2010/2, p. 78.

[1145] V. en ce sens : J. BOSSAN, « Responsabilité pénale en cascade dans la communication audiovisuelle et l'internet », *J.-Cl.* comm., fasc. 142, 1er septembre 2015 (mise à jour 20 décembre 2017), n° 39 et suiv. ; E. DERIEUX, *Droit des médias, droit français, européen et international*, LGDJ, 7e éd., 2015, p. 407, n° 1492 ; du même auteur : « Réseaux sociaux et responsabilité des atteintes aux droits de la personnalité », *RLDI*, 2014, n° 100 ; J. BOYER, « La responsabilité "allégée" des directeurs de publication de services de communication au public en ligne à raison des messages d'internautes sur les espaces de contributions personnelles », *Légicom* 2010, n° 45, p. 78 ; E. DREYER, *Responsabilité civile et pénale des médias*, Litec, 2ème éd., 2008, p. 371.

[1146] Crim., 8 décembre 1998, n° 97-83.709 : *Bull. crim.* 1998, n° 335 ; *RSC* 1999, p. 607, obs. J. FRANCILLON ; *JCP* G 1999, II, 10135, note J.-Y. LASSALLE – TGI Paris, 2 décembre 2011 : *Légipresse* 2011, n° 279, p. 12 – Cons. Const., 16 septembre 2011, QPC n° 2011-164 : *JCP* G 2011, 1247, note E. DREYER ; *CCE* 2011, comm. 106, obs. A. LEPAGE ; *Gaz. Pal.* 12-13 octobre 2011, p. 11, obs. F. FOURMENT.

statut de producteur pour l'instigateur d'un hashtag sur Twitter. Certes, le hashtag en cause permet d'échanger des opinions sur un thème prédéfini, cependant, l'individu ne dispose pas de pouvoir de modération sur les contenus publiés *a posteriori* sous ce hashtag, il n'a donc pas la maîtrise éditoriale du service de communication même s'il en a impulsé la thématique. Il ne peut donc être déduit une responsabilité de ce dernier au titre de producteur ou de directeur de publication de l'ensemble des individus reprenant son hashtag.

430. Le statut de directeur de publication primant sur celui de producteur. De manière générale les qualités de directeur de publication et de producteur sont confondues sur les réseaux sociaux. Les juges du fond ont reconnu dans ce sens lors de la condamnation de l'élu du Front National à 3000 euros d'amende qu'à partir du moment où il a volontairement rendu public son mur Facebook en autorisant ses amis à y publier des commentaires, « *il est devenu responsable de la teneur des propos publiés en tant que producteur d'un site de communication au public en ligne et directeur de la publication* »[1147]. La Cour de cassation a cependant dans un premier temps utilisé cette identité de personne pour exploiter une « *faille* »[1148] du régime spécifique de responsabilité prévu à l'article 93-3. À l'origine, l'allégement de responsabilité dont bénéficiait le directeur de publication d'un espace de contribution personnelle n'était pas transposable au producteur. Cette maladresse législative servit à la Cour de cassation[1149] pour retenir la responsabilité du producteur lorsque celle du directeur de publication ne pouvait être engagée, alors même que très souvent une seule et même personne revêtait ces qualités. Il suffisait donc de requalifier le directeur de publication en producteur pour pouvoir engager sa responsabilité sans tenir compte du régime particulier institué par la loi Hadopi[1150]. Le Conseil constitutionnel[1151] condamna toutefois rapidement cette jurisprudence en ce qu'elle introduisait un régime de responsabilité automatique à l'égard du producteur et donc un risque pesant sur la liberté d'expression. En réaction à cette condamnation, la Cour de cassation[1152] assimila finalement le régime de responsabilité du

[1147] Nîmes, 3ème ch., 18 octobre 2013, n° 13/00447, Leila T. c/ Stéphane B. et Julien S. : *CCE* n° 2, Février 2014, É. CAPRIOLI, comm. 23.
[1148] G. TILLEMENT, « La loi de 1881 sur la liberté de la presse et le contrôle de constitutionnalité », *in Légalité, légitimité, licéité : regards contemporains*, Mélanges en l'honneur du Professeur Jean-François Seuvic, PUN, 2018, p. 266.
[1149] V. Crim. 16 février 2010, n° 09-81.064 et n° 08-86.301 : *Dr. pén.* 2010, n° 80, note M. VÉRON ; *D.* 2010, p. 2206, obs. E. DREYER.
[1150] G. TILLEMENT, « La loi de 1881 sur la liberté de la presse et le contrôle de constitutionnalité », *op. cit.*, p. 266.
[1151] Cons. Const., 16 septembre 2011, QPC n° 2011-164 : *D.* 2011. p. 2444, note L. CASTEX ; AJ Pén. 2011, n° 594, obs. S. LAVRIC ; *RSC* 2011, n° 647, obs. J. FRANCILLON, *Dr. pén.* 2012, chron. n° 5, obs. O. MOYSSET ; *Légipresse* 2011, p. 688, note A. FOURLON.
[1152] Crim. 31 janvier 2012, n° 11-80.010 : *Bull. crim.* n° 29 ; *CCE* 2012, comm. 43, obs. A. LEPAGE ; *D.* 2012, p. 1249, note C. RAVIGEAUX ; *D.* 2013, p. 457, obs. E. DREYER ; *Dr. pén.* 2012, n° 4, comm. 53, note

producteur sur celui du directeur de publication. Partant, le statut de directeur de publication, étant placé en amont dans la cascade de responsabilité, prime dorénavant en tout état de cause sur celui de producteur[1153].

431. Le régime de responsabilité propre à la loi sur la liberté de la presse est devenu très spécifique sur le support d'internet et particulièrement sur les réseaux sociaux en ligne. Les différentes qualités (Directeur de publication, auteur, producteur) qui, sur les médias traditionnels sont clairement segmentés, se confondent souvent sur ces espaces de discussion dématérialisés. Ceci s'explique par le caractère direct et sans fixation préalable des contenus publiés mais également par la capacité technique des utilisateurs à modérer eux-mêmes les contenus circulant sur leurs espaces personnels. Il arrive ainsi que des utilisateurs amateurs soient reconnus comme responsables de contenus dont ils ne sont pas à l'origine en raison du statut de directeur de publication qu'ils endossent. Ceci démontre les limites d'un tel régime de responsabilité appliqué aux sites de réseaux sociaux.

§2. Les limites du régime de responsabilité applicable aux utilisateurs de réseaux sociaux

432. Deux limites. Le régime de responsabilité prévu par la loi sur la liberté de la presse présente deux limites. Une première consiste en l'absence de distinction entre la qualité professionnelle et amateur des utilisateurs, il convient alors de proposer une telle distinction (A). Une seconde limite porte sur le manque d'effectivité dans la répression des comportements (B).

A. Une nécessaire distinction entre la qualité professionnelle et amateur des utilisateurs

433. Une nécessaire distinction entre l'activité professionnelle et amateure. La loi sur la liberté de la presse, malgré son intitulé, n'est pas uniquement un texte destiné aux professionnels de la communication. Cette loi s'adresse à tout individu, professionnel ou amateur, du moment que l'individu s'exprime par un mode d'expression publique. L'article 23 de la loi sur la liberté de la presse rappelle ce principe très clairement. La loi de

---

M. VERON ; *Gaz. Pal.* 13-14 juin 2012, p. 11, obs. F. FOURMENT ; Crim., 30 octobre 2012, n° 10-88.825, *D.* 2013, p. 160, note E. DREYER.

[1153] Selon Joël Boyer : « *dans la cascade, le "producteur" est souvent un directeur de publication de site qui ne peut voir sa responsabilité engagée es qualité. C'est l'autre nom du "coupable" que l'on recherche, et parfois l'ultime recours des victimes* ». J. BOYER, « La responsabilité "allégée" des directeurs de publication de services de communication au public en ligne à raison des messages d'internautes sur les espaces de contributions personnelles », *Légicom* n° 45, 2010/2, p. 81.

du 29 juillet 1881 n'est donc pas réservée aux journalistes professionnels, les amateurs ont toujours été présents dans l'histoire des médias, de la presse écrite à internet. Ces derniers sont même perçus par certains professionnels comme constituant une concurrence dangereuse, les amateurs étant susceptibles d'apporter diversité et complémentarité dans l'information[1154]. Cependant, en mettant à disposition un espace où la liberté et la facilité d'accès se conjuguent avec une diffusion publique à vocation universelle, internet renouvelle radicalement la problématique de l'amateur et de la liberté d'expression[1155]. Les profanes sont de plus en plus présents et de plus en plus nombreux et la question centrale revient à savoir « *si l'amateur doit recevoir le même régime juridique que le professionnel* »[1156].

434. Selon le Professeur Emmanuel Derieux : « *pour ce qui est de quelques aspects du droit des médias, la distinction doit être faite entre les amateurs et les professionnels. Pour le reste, ce droit s'applique de la même façon aux uns comme aux autres* »[1157]. Plus particulièrement, s'il a été démontré que les infractions du droit pénal de la presse sont largement et légitimement applicables aux usagers des réseaux sociaux[1158], professionnels comme amateurs, en revanche le système de responsabilité qui leur est actuellement applicable démontre une distanciation prise entre la réalité de la communication au public en ligne et la volonté initiale du législateur. Il est difficilement concevable que la qualité de directeur de publication ait été prévue à l'origine comme pouvant être attribuée à un très large public y compris d'amateurs. Le statut des éditeurs et des directeurs de publication provient en effet du statut spécifique des entreprises de presse et de la volonté d'assurer par leur fonction une transparence, une garantie de l'indépendance de la publication et le pluralisme de l'information[1159]. Le régime de la loi sur la liberté de la presse place le directeur de publication en tête du système de responsabilité en cascade en raison de son rôle central au sein de l'entreprise de presse. Il est dans ce cas nécessaire de redonner du sens à cette catégorie d'acteur emblématique de la loi du 29 juillet 1881 dont le champ d'application est

[1154] E. DERIEUX, « Amateurs et médias : nouveaux défis juridiques ? », *Légicom*, n° 41, 2008/1, p. 22-23.
[1155] N. BONNAL, « les responsabilités de l'amateur internaute au regard du droit de la presse », *Légicom*, n° 41, 2008/1, p. 15.
[1156] P.-Y. GAUTIER, « Le contenu généré par l'utilisateur », *Légicom*, n° 41, 2008/1, p. 8.
[1157] E. DERIEUX, « Amateurs et médias : nouveaux défis juridiques ? », *op. cit.*, p. 124.
[1158] V. *supra*, Partie 1, Titre 1, Chapitre 1.
[1159] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 403, n° 666.

devenu trop large. Pour ce faire, peuvent être distingués les usages professionnels des usages amateurs au sein du régime de responsabilité en cascade applicable aux réseaux sociaux[1160].

435. Qualification de l'utilisation professionnelle et amateure sur les réseaux sociaux. Il convient d'adopter une conception large de l'usage professionnel d'un réseau social. Il ne serait pas pertinent de restreindre cette qualification aux seuls métiers du journalisme ou des médias en général. L'usage d'un compte de réseau social à titre professionnel doit être reconnu si le compte est utilisé en lien avec une activité professionnelle ou lucrative, quelle qu'elle soit. En conséquence, l'utilisateur amateur peut être reconnu comme « *celui qui met en ligne des contenus à titre non professionnel, non lucratif, non économique* »[1161]. Autrement dit, cela invite à distinguer entre l'usage professionnel et privé d'un compte de réseau social. Par exemple, le dirigeant d'une entreprise de bâtiment peut avoir à la fois un compte Facebook personnel destiné à son usage privé, révélant un usage amateur et une page Facebook destinée à promouvoir son entreprise révélant un usage professionnel[1162]. De même, on peut également considérer que le représentant politique du Front National ayant été condamné à une peine d'amende en tant que directeur de publication de sa page Facebook agissait à titre professionnel car la page Facebook le représentait en tant que député effectuant une campagne dans le cadre d'élections cantonales[1163]. Cette distinction qui a le mérite d'être objective permet de justifier l'application d'une plus grande rigueur à l'usage professionnel qu'à l'usage amateur.

436. Une différence de régime entre l'activité professionnelle et amateure. Une distinction doit être proposée entre le régime de responsabilité applicable aux utilisateurs amateurs et aux utilisateurs professionnels des espaces de contributions personnelles. Ceci se justifie du fait que le régime actuellement applicable s'identifie fortement à celui des hébergeurs, voire serait plus strict en ce qu'il instaurerait une obligation de surveillance ou du moins de vigilance à l'égard du directeur de publication. Un tel régime de responsabilité semble alors empreint d'une trop grande rigueur si ce n'est sévérité pour un utilisateur non-professionnel. Nous suggérons en conséquence de distinguer au sein de l'article 93-3 le régime de responsabilité applicable aux utilisateurs professionnels et le régime applicable aux utilisateurs amateurs concernant les espaces de contributions personnelles. Il semble logique

[1160] Notons que le régime juridique applicable à la communication au public en ligne propose déjà des distinctions entre les utilisateurs professionnels et non professionnels notamment concernant les obligations de l'éditeur de service : LCEN, art. 6, III-1.
[1161] P.-Y. GAUTIER, « Le contenu généré par l'utilisateur », », *Légicom*, n° 41, 2008/1, p. 8
[1162] E. DREYER, « L'amateur sur Interne ou le blog rattrapé par le droit… », *Légicom*, n° 41, 2008/1, p. 22-23.
[1163] Nîmes, 3ème ch., 18 octobre 2013, n° 13/00447, Leila T. c/ Stéphane B. et Julien S. : *CCE* n° 2, Février 2014, comm. 23., É. CAPRIOLI.

de conserver le régime actuel pour les usages professionnels et à l'inverse de rebasculer vers le régime de droit commun concernant les usages amateurs. Ceci aurait pour conséquence, pour les amateurs, de faire peser le poids premier de la responsabilité pénale sur l'auteur du contenu délictueux. Par ailleurs, en s'appliquant uniquement aux usagers professionnels, le régime de responsabilité en cascade serait, en un sens, renforcé car il serait justifié par la qualité du responsable. Précisons en définitive que s'il s'agit de distinguer le régime de responsabilité applicable entre les utilisateurs amateurs et professionnels, les règles de procédure favorables propres au droit de la presse doivent demeurer applicables à l'égard de ces deux catégories d'acteurs.

437. Proposition de réécriture de l'article 93-3. Il s'agit de modifier la rédaction du 5ème alinéa et de proposer la rédaction d'un sixième alinéa de l'article 93-3 de la loi du 29 juillet 1982. La nouvelle rédaction pourrait se présenter comme suit :

« *Lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de publication* ***peut voir sa responsabilité pénale engagée comme auteur principal s'il agissait à titre professionnel et s'il est établi qu'il avait effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour le retirer.***

Lorsque la gestion de l'espace de contributions personnelles est faite à titre non-professionnel, les règles de responsabilité de droit commun s'appliquent ».

B. La difficile répression des infractions de presse rencontrées sur les réseaux sociaux

438. Un manque d'effectivité constaté. La répression des infractions relevant de la loi du 29 juillet 1881 sur les réseaux sociaux est devenue un enjeu particulièrement important tant le contentieux s'avère massif. Selon une étude, « *les pages associées à un contenu violent ont bondi de 125 % sur Internet entre 2006 et 2007, celles faisant l'apologie du racisme de 70 %, celles relatives aux drogues de 62 %. Les pages au contenu relatif à la pornographie infantile ont progressé de 18 %* »[1164]. De même, un rapport[1165] met également en évidence, particulièrement concernant le web 2.0, l'inefficacité de la répression des délits d'expression

[1164] Rapport au Premier ministre, *Lutter contre le racisme sur Internet*, I. FALQUE-PIERROTIN, 2010, p. 13.
[1165] M. ROBERT, *Protéger les internautes. Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014.

raciste et l'impunité des internautes qui en résulte. Au regard des données de la police et de la gendarmerie nationale, ce dernier relève une augmentation sensible des atteintes à la dignité et à la personnalité commises par le biais d'internet (injures, diffamations, discriminations). Précisément 1 235 en 2009, 1 528 en 2010, 1 691 en 2011 et 2 300 en 2012[1166]. Citant les statistiques judiciaires, le rapport fait également état de 800 condamnations pour l'année 2012 sur le fondement d'infractions à la loi de presse commises par voie de communication en ligne[1167]. On constate ainsi une augmentation particulièrement importante des contenus haineux au vu des autres catégories d'infractions, cette évolution étant favorisée par l'apparition et l'usage intensif des sites de réseaux sociaux[1168]. Or, le nombre de poursuites engagées en matière d'actes et de propos racistes commis sur internet est encore faible au regard du nombre des actes recensés de cette nature[1169].

439. Ce manque de cohérence entre les comportements observés et les sanctions pénales prononcées trouve des explications en plusieurs endroits. Les spécificités propres au droit de la presse couplées avec la technicité du droit applicable à internet ainsi que la complexité de l'analyse de certaines infractions à la liberté d'expression « *rendent le travail des magistrats particulièrement ardu* »[1170]. Les magistrats qualifiés pour statuer sur ce genre de contentieux est objectivement insuffisant pour permettre la poursuite effective de tous les comportements relevant d'une infraction à la loi de 1881. En conséquence, la politique pénale n'est pas la même envers certaines catégories d'infractions au sein de cette loi. Les provocations à la haine raciale ou l'apologie du terrorisme font l'objet d'une sévérité pénale particulière à l'inverse des diffamations ou injures classiques alors même que ces dernières constituent, en nombre, le contentieux pénal le plus important.

Le manque d'effectivité de la sanction pénale constaté concernant les infractions de presse commises sur internet est toutefois contrebalancé par le souci du législateur d'engager certaines réformes visant à adapter la réponse pénale aux évolutions constatées. Ce dernier est venu étendre une procédure de droit commun, l'ordonnance pénale, aux infractions de presse (1) et souhaite également adapter le régime répressif de la loi de 1881 (2).

[1166] *Ibid.*, p. 20.
[1167] *Ibid.*, p. 28.
[1168] V. sur la question l'étude du Centre Simon Wisenthal concernant les réseaux sociaux. <http://www.wiesenthal.com/atf/cf/%7B54d385e6-f1b9-4e9f-8e94-890c3e6dd277%7D/NY-RELEASE.PDF> (dernière consultation le 9 octobre 2019).
[1169] Rapport au Premier ministre, *Lutter contre le racisme sur Internet*, I. FALQUE-PIERROTIN, 2010, v. tableau p. 21.
[1170] M. QUÉMÉNER, Y. CHARPENEL, *Cybercriminalité, Droit pénal appliqué*, Économica, 2010, p. 215, n° 1047.

1) L’extension de la procédure de l’ordonnance pénale aux infractions de presse

440. La procédure de l’ordonnance pénale. La loi n° 2002-1138 du 9 septembre 2002[1171] a créé la procédure simplifiée de l’ordonnance pénale prévue aux articles 495 à 495-6 du Code de procédure pénale. Cette procédure consiste, pour le procureur de la République, à renvoyer directement le dossier de la procédure au président du tribunal avec ses réquisitions quant à la ou aux peines qui doivent être prononcées. Par la suite, le président statue sans débat préalable par une ordonnance portant relaxe ou condamnation à une amende ou à une ou plusieurs des peines complémentaires encourues. L’ordonnance est ensuite transmise au ministère public qui doit la faire notifier au prévenu et à la partie civile qui disposent d’un délai de quarante-cinq jours pour former opposition[1172]. Cette procédure a été validée au moment de sa création par la décision du 29 août 2002 du Conseil constitutionnel qui affirme que l’ordonnance pénale assure de façon suffisante l’existence d’un procès juste et équitable[1173].

441. Une procédure désormais applicable aux diffamations et injures. Depuis son adoption, la procédure d’ordonnance pénale a été progressivement étendue à d’autres types d’infractions. Ainsi, la loi n° 2009-1311 du 28 octobre 2009[1174] a prévu l’application de cette procédure aux délits de contrefaçon prévus aux articles L. 335-2, L. 335-3 et L. 335-4 du Code de la propriété intellectuelle, lorsqu’ils sont commis au moyen d’un service de communication au public en ligne[1175]. Plus récemment encore, la loi n° 2011-1862 du 13 décembre 2011[1176] est venue étendre encore le champ d’application de l’ordonnance pénale à de nombreuses autres infractions incriminées par le Code pénal[1177] ou d’autres codes[1178]. Enfin, dans le but de répondre au besoin d’efficacité et de célérité de la justice pénale en matière d’infractions de presse, la loi n° 2019-222 du 23 mars 2019 est venue étendre la

[1171] L. n° 2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice, *JORF*, 10 septembre 2002, p. 14934.
[1172] F. MOLLINS, Rép. pén. Dalloz, novembre 2017 (mis à jour mars 2018), *V°* Action publique, n° 147.
[1173] « *Considérant que, si le législateur peut prévoir des règles de procédure différentes selon les faits, les situations et les personnes auxquelles elles s'appliquent, c'est à la condition que ces différences ne procèdent pas de discriminations injustifiées et que soient assurées aux justiciables des garanties égales, notamment quant au respect du principe des droits de la défense, qui implique en particulier l'existence d'une procédure juste et équitable* » Cons. const. 29 août 2002, DC 2002-461.
[1174] L. n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, *JORF* n° 0251, 29 octobre 2009, p. 18290, art. 6.
[1175] C. proc. pén., art 495, II, 12°.
[1176] L. n° 2011-1862 du 13 décembre 2011 relative à la répartition des contentieux et à l'allègement de certaines procédures juridictionnelles, *JORF* n° 0289, 14 décembre 2011 p. 21105.
[1177] Plus précisément : le vol simple, recel, filouterie, destruction ou dégradation volontaire d'un bien privé ou public, délit de fuite commis à l'occasion de la conduite d'un véhicule etc.
[1178] En l’occurrence : les délits en matière de chèques des articles L. 163-2 et L. 2163-7 du Code monétaire et financier.

procédure de l'ordonnance pénale aux diffamations et injures prévues par la loi du 29 juillet 1881[1179].

442. L'opportunité mesurée de l'extension de l'ordonnance pénale aux délits de diffamation et d'injure. La procédure simplifiée de l'ordonnance pénale qui n'est pas soumise à l'exigence du contradictoire et donc d'une audience, permet un traitement plus rapide des affaires. Par ailleurs, cette procédure permettrait de prononcer des peines alternatives à l'emprisonnement notamment des peines de travaux d'intérêt général ou encore de jour-amende dont le prononcé permettrait de favoriser une diversification de la réponse pénale dans le contentieux des infractions de presse. Toutefois, la mise en œuvre d'une telle procédure peut également révéler certaines difficultés au regard des spécificités du droit de la presse. À ce titre, le premier alinéa de l'article 495 I précise que l'ordonnance pénale est applicable « *lorsqu'il résulte de l'enquête de police judiciaire que les faits reprochés au prévenu sont simples et établis* ». Autrement dit, la procédure d'ordonnance pénale est légitime à être mise en œuvre lorsque la qualification pénale des faits ne fait aucun doute. Cette exigence s'accommode mal de la spécificité des infractions de presse et notamment du délit de diffamation qui obéit « *à de subtiles conditions de qualification* »[1180]. En effet, « *les restrictions à la liberté d'expression sont d'interprétation étroite* »[1181] et relèvent en principe d'un juge spécialisé qui est le mieux à même de qualifier le caractère diffamatoire ou injurieux d'une allégation ainsi que l'éventuelle existence de faits justificatifs spéciaux tels que l'exception de vérité ou la bonne fois du diffamateur. La distinction entre les délits de diffamation et d'injure s'avère en outre parfois difficile à établir, cette affirmation s'illustre par la décision de la Cour de cassation du 18 octobre 2016[1182] invalidant la qualification d'injure retenue par les juges du fond au profit de la qualification de diffamation. Il n'est donc pas certain que la célérité et la simplicité de la procédure qui caractérisent l'ordonnance pénale soient une solution adéquate concernant le manque d'effectivité de la répression des infractions de presse.

[1179] L. n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *JORF* n° 0071, 24 mars 2019, art. 61, II.
[1180] B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 594 et 595, n^{os} 718 et suiv.
[1181] Crim., 14 février 2006 : *Bull. crim.* 2006, n° 42.
[1182] Crim, 18 octobre 2016, n^{o} 15-84.068 : *RLDI*, 2016, n^{o} 131, obs. L. COSTES.

2) Vers une adaptation du régime répressif de la loi de 1881

443. La diversification et l'adaptation des sanctions. Au-delà de la nécessaire célérité des procédures, le rapport visant à Renforcer la lutte contre le racisme et l'antisémitisme[1183] préconise également une diversification et une adaptation des sanctions à l'espace numérique, en particulier des sanctions prévues par la loi de presse. Il peut s'agir par exemple de la réalisation de travaux d'intérêt général auprès de la plateforme de signalement de contenus PHAROS[1184] ou encore l'obligation d'effectuer un stage de sensibilisation à la lutte contre les propos haineux sur internet. Concernant les peines complémentaires, le rapport propose d'accroître l'éventail des dispositions présentes dans la loi de 1881, en insérant notamment la possibilité d'une suspension de compte, d'une résiliation de compte, d'une suspension du fonctionnement d'un site ou d'une confiscation du matériel ayant servi à commettre l'infraction (serveur, poste de travail etc.). Le rapport propose d'étudier l'instauration d'une peine complémentaire qui consisterait à donner la possibilité au juge d'ordonner la suppression de contenus identiques ou analogues à ceux visés par sa décision, lorsqu'ils sont produits par un même auteur. Le rapport cite l'exemple suivant : « *ordonner la suppression du compte Twitter de la personne, lorsque la décision prévoit d'ores et déjà la suppression de sa page Facebook, au motif que les contenus haineux publiés sont de nature équivalente* ». En outre, il est proposé d'encourager les publication des décisions de justice et plus particulièrement, leur publication sur les espaces personnels de l'individu condamné comme sa page Facebook, son compte Twitter ou son blog personnel[1185]. Ce type de sanction devant toutefois être motivé aux strictes fins d'intérêt général sans porter une atteinte aux droits fondamentaux de la personne notamment le respect de sa vie privée et de ses chances de réinsertion.

444. La spécialisation des magistrats, des policiers et gendarmes. Enfin, compte tenu de la technicité du droit de la presse et aux caractéristiques mouvantes de l'espace numérique il est proposé de renforcer la formation initiale et continue des magistrats, autant du siège que du parquet mais également des policiers et gendarmes recevant les plaintes[1186]. Concernant les affaires dont les spécificités ne permettent pas de recourir à la procédure de l'ordonnance pénale, le rapport propose la création de chambres spécialisées au sein des tribunaux de

[1183] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018.
[1184] V. *infra* n° 455.
[1185] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, *op. cit.*, recommandation n° 15, p. 40.
[1186] *Ibid.*, recommandation n° 16, p. 41.

grande instance conformément à la proposition formulée à l'article 54 du projet de loi de programmation de la justice[1187].

445. Conclusion de la Section 2. Les utilisateurs des réseaux sociaux sont éditeurs de services soumis au système de responsabilité prévu par la loi sur la liberté de la presse. Ce régime de responsabilité n'entre cependant pas en adéquation avec le statut de l'utilisateur du réseau social. Effectivement, au titre du système de responsabilité en cascade l'utilisateur d'un réseau social peut voir sa responsabilité pénale engager à titre principal pour un contenu dont il n'est pas l'auteur lorsque ce dernier peut être reconnu comme directeur de publication de l'espace au sein duquel le contenu a été publié. Il convient alors de distinguer le système de responsabilité selon la qualité de l'utilisateur du réseau social. Il est ainsi proposé la distinction suivante : lorsque le réseau social est utilisé à titre professionnel, l'utilisateur sera soumis à ces règles de responsabilité contraignantes. À l'inverse, lorsque le réseau social n'est utilisé qu'à titre personnel ou domestique, la responsabilité pénale de droit commun doit être privilégiée. La sévérité du régime de responsabilité applicable aux utilisateurs des réseaux sociaux en ligne n'empêche toutefois pas de constater un manque d'effectivité de la sanction pénale concernant les infractions de presse commises sur ces sites. Les mesures proposées telles que l'extension de l'ordonnance pénale aux infractions de presse ne semblent pas en mesure de pallier les difficultés du juge pénal à connaître l'ensemble du contentieux de presse généré par les sites de réseaux sociaux.

[1187] *Ibid.*, recommandation n° 14, p. 39.

Conclusion du Chapitre 2

446. Les utilisateurs de réseaux sociaux sont soumis à des règles de responsabilité imprégnées d'une particulière sévérité. Cette observation se vérifie d'abord à l'égard de la responsabilité pénale de droit commun. Il est en effet reconnu que l'utilisateur d'un réseau social peut revêtir sous certaines conditions la qualité de responsable d'un traitement de données. Cette qualité a ainsi justifié l'engagement de la responsabilité pénale de l'administrateur d'une page fan du réseau social Facebook. De plus, les comportements déviants générés par les sites de réseaux sociaux tels que la pratique du *happy slappling* ont justifié l'apparition d'un cas de complicité en ligne *sui generis*. Au final, loin de se montrer dépassé par les nouveaux comportements permis par les réseaux sociaux, le droit pénal démontre une sévérité particulière à l'égard de ces derniers qui constituent dans nombre d'infractions un cas d'aggravation de la peine encourue. Cette sévérité se retrouve également dans le régime de responsabilité en cascade applicables aux utilisateurs des réseaux sociaux en leur qualité d'éditeurs de service. Cependant, elle se déduit en l'occurrence de l'inadaptation de ce régime de responsabilité visant à l'origine un nombre restreint d'individus qui plus est professionnels. Il apparaît alors justifié de faire sortir de ce système de responsabilité inadapté les internautes n'utilisant un service de réseau social qu'à titre personnel ou domestique. Dans cette hypothèse les règles de responsabilité pénale de droit commun doivent être privilégiées.

Conclusion du Titre 1

447. Les règles organisant la responsabilité pénale sont mises au défi des différents acteurs des sites de réseaux sociaux. Dans un premier temps les opérateurs des réseaux sociaux bénéficient en leur qualité d'hébergeur de l'application de régimes juridiques qui leur sont favorables et en conséquence d'un faible engagement de leur responsabilité. À l'inverse, leurs utilisateurs sont soumis à des règles de responsabilité qui ne distinguent pas suffisamment l'usage professionnel d'un réseau social d'un usage amateur. Ces régimes de responsabilité empreints d'une sévérité accrue à l'égard des utilisateurs et atténuée à l'égard des opérateurs laissent apercevoir au final l'incapacité du système répressif à poursuivre de manière effective l'ensemble des comportements délictueux générés par les sites de réseaux sociaux.

448. Cette « *conversation mondiale sans fin* »[1188] orchestrée par les réseaux sociaux en ligne entrainant l'incapacité du système judiciaire à connaître l'ensemble des infractions, particulièrement celles liées à l'expression illicite, force alors le constat de l'inadéquation des règles de responsabilité pénale appicables aux acteurs des réseaux sociaux. Une évolution du droit est alors souhaitable à travers la création d'une troisième catégorie d'acteurs au sein de l'internet, se situant entre les éditeurs de service et les hébergeurs. Accroître la responsabilité des opérateurs des réseaux sociaux permettrait de réguler à une échelle différente et par une voie complémentaire au chemin répressif classique les contenus illicites y circulant. Pour ce faire, il est nécessaire de prendre pleinement conscience de l'essor du web 3.0 et de redéfinir les postulats écrits pour l'internet originel. Il est dès lors indispensable de s'interroger sur les nouveaux moyens de réponse aux infractions commises sur les réseaux sociaux pouvant intervenir à la place ou en parallèle des voies répressives classiques.

[1188] E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, p. 146, n° 118.

Titre 2 – L'évolution de la réponse aux infractions commises sur les réseaux sociaux

449. Développement et encadrement du pouvoir régulateur des réseaux sociaux. L'importance des comportements délictueux générés par les sites de réseaux sociaux, particulièrement concernant les infractions à la loi sur la liberté de la presse, empêche les voies répressives traditionnelles d'assurer leur répression effective. La solution revient alors à passer d'une logique répressive basée sur la sanction d'un comportement constitutif d'une infraction, à une logique préventive consistant à faire cesser le trouble à l'ordre public causé par la diffusion de telles infractions sur les réseaux sociaux. Sur ces moyens de communication, le trouble à l'ordre public consécutif à la commission d'un comportement délictueux est exacerbé par l'accessibilité facile du contenu mis en ligne et surtout, par la largesse de son champ de diffusion. En conséquence, outre une répression effective de l'auteur de l'infraction, l'enjeu concerne également les moyens permettant de faire cesser la diffusion du contenu délictueux. Pour ce faire, les opérateurs des réseaux sociaux disposent de la faculté technique de modérer, à savoir de supprimer ou de rendre inaccessibles les contenus mis en ligne sur leurs plateformes. Cette action permet de faire cesser le trouble consécutif à la mise en ligne et à la disponibilité du contenu sur le réseau social. En outre, la pratique de la modération des contenus ne fait pas disparaître la voie pénale classique qui peut être sollicitée dès lors que le contenu était constitutif d'un comportement pénalement sanctionné. Autrement dit, le retrait du contenu par l'opérateur du réseau social n'efface pas la responsabilité pénale de son auteur. Cette modération effectuée en amont des voies répressives traditionnelles constitue une nouvelle voie de réponse aux infractions qui devient un complément nécessaire au schéma répressif classique. Le développement du pouvoir régulateur des opérateurs des réseaux sociaux se doit toutefois d'être encadré au risque de générer un système de régulation privé des contenus s'exerçant au détriment des droits de leurs utilisateurs. Cette adaptation du droit implique la définition d'un nouveau régime juridique applicable aux sites de réseaux sociaux ainsi que de nouveaux acteurs venant assurer leur encadrement. En l'occurrence, les limites du système actuel d'autorégulation des sites de réseaux sociaux (**Chapitre 1**) amène à mettre en avant les enjeux du nouvel encadrement de ces derniers (**Chapitre 2**).

Chapitre 1 – Les limites de l'autorégulation des réseaux sociaux

450. Une régulation privée des contenus insatisfaisante. Avec le système de modération en ligne des contenus, la réponse pénale ne relève plus exclusivement de la voie répressive traditionnelle, mais davantage en amont, si ce n'est en parallèle de celle-ci. Le risque est alors que les opérateurs des réseaux sociaux deviennent eux-mêmes juges de l'illicéité des contenus qui y sont diffusés. À ce titre, le développement d'une réponse préventive intervenant en amont de la mise en mouvement de l'action publique ne doit pas entraîner un risque concernant le respect des libertés fondamentales. Or, les opérateurs des réseaux sociaux, en leur qualité d'hébergeurs, ont l'obligation de retirer tous les contenus qui leur sont notifiés mais uniquement dans l'hypothèse où ces derniers présenteraient un caractère manifestement illicite. Cette obligation formulée par l'article 6 de la LCEN est censée garantir un exercice mesuré de la modération des contenus par l'hébergeur. Cependant, la faible mise en œuvre de ce régime de responsabilité à l'égard des opérateurs des sites de réseaux sociaux favorise l'émergence d'une autorégulation des contenus se rapprochant davantage de leurs propres règles de fonctionnement interne que des exigences posées par la loi. Cette privatisation de la régulation des contenus est problématique à deux égards. Elle entraîne d'une part une censure trop stricte de certains contenus portant ainsi atteinte à la liberté d'expression des utilisateurs des réseaux sociaux. D'autre part, elle se montre trop laxiste concernant la modération des propos constitutifs d'abus de la liberté d'expression alors que certains d'entre eux sont de nature à présenter un caractère manifestement illicite. Cette dernière hypothèse démontre les limites du présent système de régulation des contenus à préserver certains standards juridiques européens et en conséquence, l'ordre public à l'échelle numérique.

Ainsi, malgré l'encadrement actuel du pouvoir de régulation des sites de réseaux sociaux (**Section 1**), la pratique de leur pouvoir de régulation aboutit à un système de régulation privé qu'il convient de critiquer (**Section 2**).

Section 1 : l'encadrement actuel du pouvoir de régulation des opérateurs des réseaux sociaux

451. Un pouvoir de régulation de l'expression encadré. La LCEN du 21 juin 2004 prévoit à son article 6 un régime de responsabilité limitée des hébergeurs conditionné à leur connaissance ou non du contenu illicite[1189]. En contrepartie de ce régime de faveur, les intermédiaires techniques ont le devoir de collaborer techniquement à la lutte contre les contenus illicites. Cette collaboration passe notamment par le devoir pour ces derniers de faire le nécessaire pour rendre certains contenus inaccessibles dès lors qu'ils en ont eu connaissance. Cette responsabilisation des intermédiaires techniques mis en œuvre par la LCEN vient en réalité reconnaître et encadrer un pouvoir de régulation de l'expression pour ces derniers. La régulation s'entend comme toute forme d'intervention visant à assurer le fonctionnement correct d'un système économique ou social, en l'occurrence l'expression publique à l'échelle numérique. Il s'agit concrètement de la faculté pour les opérateurs des réseaux sociaux de juger par eux-mêmes de l'illicéité de certains contenus et le cas échéant, de les modérer afin de maintenir l'état souhaité du système dont ils assurent le fonctionnement. Pour ce faire, la LCEN prévoit une procédure d'avertissement des hébergeurs par un système de notification ou de signalement de contenus intervenant en amont de toutes poursuites pénales (**§1**). Les opérateurs des réseaux sociaux étant tenus de supprimer les contenus apparaissant comme « *manifestement illicite* » (**§2**).

§1. Une nécessaire connaissance par les opérateurs du contenu illicite

452. Signalement ou notification. En raison de son absence d'obligation générale de surveillance, l'opérateur d'un réseau social n'est pas censé connaître de lui-même les contenus illicites postés sur sa plateforme. La LCEN fait alors reposer la responsabilité des hébergeurs sur leur connaissance ou non du contenu illicite. Cette connaissance pouvant être apportée par de simples internautes. Il faut dès lors distinguer la procédure de signalement (A) et de notification (B) de contenus illicites.

[1189] V. *supra* n° 380 et suiv.

A. Le signalement de contenus illicites

453. Signalement sur le réseau social ou sur une plateforme publique. Les fournisseurs d'accès internet et les hébergeurs ont l'obligation de mettre en place un dispositif permettant à toute personne de porter à leur connaissance les contenus illicites transitant sur leurs plateformes. L'absence de respect de cette obligation est sanctionnée d'un an d'emprisonnement de et de 75 000 euros d'amende[1190]. En application des règles de l'article 131-38 du Code pénal les opérateurs des réseaux sociaux en tant que personnes morales encourent alors le quintuple de l'amende prévue pour les personnes physiques soit une amende de 375 000 euros. Les peines complémentaires prévues aux 2° et 9° de l'article 131-39 du Code pénal sont également applicables à ces derniers à savoir d'une part, l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales d'autre part, l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique. Ainsi, le signalement est une procédure répondant aux obligations posées par la LCEN proposée directement par le réseau social (1). Cependant, des dispositifs de signalement ont également été mis en place par l'autorité publique afin de porter à la connaissance de cette dernière certaines catégories d'infractions (2).

1) Le signalement du contenu directement sur le réseau social

454. Fonctionnalité présente sur chaque réseau social. Selon l'article 6, I, 7 alinéa 4 de la LCEN, les opérateurs des réseaux sociaux en leur qualité d'hébergeurs « *doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données* ». L'internaute doit pouvoir localiser sur le réseau social un lien hypertexte facilement identifiable et simple d'utilisation le renvoyant vers une page sur laquelle il peut notifier à l'hébergeur ce type particulier de comportement. Lorsqu'une notification lui est adressée, la responsabilité de l'hébergeur devient fonction de son inaction. Dès lors, l'ensemble des plateformes de réseaux sociaux proposent de signaler directement les contenus illicites *via* une fonctionnalité spécialement prévue à cet effet. La procédure de signalement dépend des règles propres à chaque plateforme. Par exemple, le réseau social Facebook prévoit pour chaque contenu la possibilité de le signaler au moyen d'un lien : « *le meilleur moyen de nous signaler un contenu abusif ou indésirable sur*

[1190] LCEN, art. 6, VI, 1.

Facebook est d'utiliser le lien Signaler qui s'affiche à côté du contenu en question. Pour signaler une entreprise auprès de laquelle vous avez acheté un produit sur Facebook, vous pouvez remplir ce formulaire ». Le réseau social Twitter prévoit également une procédure de signalement pour chaque tweet : « *vous pouvez effectuer un signalement directement depuis un Tweet ou un profil donné pour certaines infractions, notamment : spam, contenu inapproprié ou préjudiciable, publicités inappropriées, conduite autodestructrice et usurpation d'identité* ». Par ailleurs, les réseaux sociaux en ligne posent souvent des conditions pour la prise en compte du signalement, notamment que l'auteur du signalement soit directement concerné par la publication du contenu illicite[1191]. Enfin, sur les réseaux sociaux le signalement n'est pas anonyme car provenant directement d'un de ses utilisateurs.

2) Le signalement du contenu sur une plateforme publique

455. Le dispositif de signalement PHAROS. Le signalement de contenus illicites peut également se faire sur des plateformes publiques qui font preuve de souplesse dans leurs conditions d'utilisation de manière à favoriser cette pratique. Par exemple, lancée le 6 janvier 2009 par une circulaire[1192], la plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS)[1193] recueille, traite et redirige vers les services adéquats, en France ou à l'étranger, les signalements du grand public et des fournisseurs d'accès. Ces derniers portent sur des contenus ou comportements présumés illicites au regard du droit pénal[1194]. Ainsi, « *un signalement, ce n'est pas une plainte, ni une enquête, c'est comme un renseignement que vous portez à la connaissance d'un service de police* » explique le commissaire divisionnaire François-Xavier Masson[1195]. La plateforme PHAROS n'est donc pas un service de plainte en ligne, cela restant de la compétence des services d'enquête de la police et de la gendarmerie ainsi que des procureurs de la République. Par ailleurs, ce dispositif n'est pas destiné à recevoir le signalement de contenus ou comportements jugés simplement immoraux ou nuisibles. De même, les affaires privées, même si elles utilisent

1191 <https://eduscol.education.fr/internet-responsable/ressources/legamedia/faire-retirer-un-contenu-illicite.html> (dernière consultation le 9 octobre 2019).
1192 Circulaire interministérielle relative au dispositif national de signalement des contenus illicites d'internet du 19 juillet 2013, NOR INT/C/1318958 C.
1193 < https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action> (dernière consultation le 9 octobre 2019).
1194 M. QUEMENER, « Signalez un contenu illicite sur Internet », *D.* 2013, p. 2096.
1195 Commissaire divisionnaire responsable de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication de la direction centrale de la police judiciaire (OCLCTIC). V. X. BERNE, « Dans les coulisses de la plateforme de signalement Pharos », NextInpact, 21 juin 2016. <https://www.nextinpact.com/news/100300-dans-coulisses-plateforme-signalement-pharos.htm> (dernière consultation le 9 octobre 2019).

internet (insultes, propos diffamatoires, harcèlements) relèvent de la compétence du commissariat de police ou de la brigade de gendarmerie et non de PHAROS. Le dispositif concerne à l'inverse les catégories d'infractions suivantes : La pédophilie et pédopornographie ; l'expression du racisme, de l'antisémitisme et de la xénophobie ; l'incitation à la haine raciale, ethnique et religieuse ; le terrorisme et apologie du terrorisme[1196]. Ces infractions peuvent être signalées dès lors qu'elles sont commises sur le support internet y compris les blogs, les réseaux sociaux et les plateformes *peer to peer*.

456. Le dispositif de signalement Pointdecontact.net. En parallèle de PHAROS, l'Association Française des Prestataires de l'Internet (AFPI) a mis en place le 19 septembre 2011 la plateforme Point de contact[1197] poursuivant les mêmes finalités. Elle offre un service de signalement en ligne ouvert à tous permettant de signaler par le biais d'un formulaire tout contenu choquant rencontré sur internet. Les catégories d'infractions comprises dans ce dispositif sont similaires à celles prévues par PHAROS : la pornographie enfantine ; les incitations à la violence, à la discrimination ou à la haine ; les contenus pornographiques, violents ou contraires à la dignité humaine accessibles aux mineurs ; les provocations aux crimes et délits contre les personnes ; les provocations au suicide ; les provocations au terrorisme ou à la fabrication de bombes ; l'apologie de crimes contre l'humanité ; le proxénétisme ; le harcèlement sexuel. Les atteintes à la propriété intellectuelle ne sont donc pas comprises dans ces services de signalement. La plateforme Pointdecontact.net fonctionne en réalité en liens étroits avec PHAROS, ses agents effectuant une préqualification pénale des contenus signalés et faisant suivre, si nécessaire, le signalement auprès de PHAROS. Ces dispositifs de signalement sur plateforme publique présentent l'avantage de pouvoir signaler anonymement des contenus qui ne concernent pas directement la personne à l'origine du signalement. La procédure de notification de contenus illicites est quant à elle davantage encadrée.

B. La notification de contenus illicites

457. Le formalisme de la notification. La LCEN a également prévu une procédure de notification de contenus potentiellement illicites à l'hébergeur. Cette notification vaut présomption simple de connaissance du contenu pour l'hébergeur et produit en conséquence

[1196] <https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Signaler-un-contenu-suspect-ou-illicite-avec-PHAROS> (dernière consultation le 9 octobre 2019).
[1197] <www.pointdecontact.net> (dernière consultation le 9 octobre 2019).

un effet probatoire[1198]. Afin que la présomption de la notification fasse effet, cette dernière doit contenir un certain nombre d'éléments. À la différence des procédures de signalement il s'agit d'une procédure formaliste. L'article 6, I, 5° de la LCEN exige que la notification comporte : « *la date de la notification ; si le notifiant est une personne physique : ses noms, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ; les noms et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ; la description des faits litigieux et leur localisation précise ; les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits* ». En outre, à la différence du signalement de contenus qui s'effectue *via* des services en ligne, la notification peut être réalisée au moyen d'une lettre, d'un courriel ou d'un formulaire, à charge pour l'expédiant de respecter les formalités prescrites.

458. L'interprétation jurisprudentielle du formalisme de la notification. Les tribunaux opèrent un contrôle strict du respect des formalités. Selon la Cour de cassation[1199], la notification délivrée au visa de la loi du 21 juin 2004 doit comporter à peine de nullité l'ensemble des mentions prescrites par ce texte. Si une seule de ces mentions fait défaut, alors la notification ne sera pas opposable à l'hébergeur. Ce principe de nullité en cas de notification incomplète a été réaffirmé par les juges du fond[1200], notamment concernant le cas d'une diffamation sur un blog[1201]. Le tribunal de grande instance de Paris a en l'espèce jugé que la société 20 minutes France, hébergeur du blog, ne pouvait voir sa responsabilité engagée « *dès lors que ni la mise en demeure […], ni la sommation […] ne satisfaisaient aux conditions légales, les formalités prévues par l'article 6 I, 5 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique n'ayant pas été respectées au cas présent* ». Les juges du fond ont également précisé les exigences relatives au contenu de la notification. Selon ces derniers il convient « *d'apprécier* in concreto *si l'hébergeur a eu une connaissance effective du contenu litigieux mis en ligne, conformément aux dispositions de l'article 6, I, 5 de la LCEN* […] *ces dispositions sont impératives pour respecter la liberté de l'information circulant sur le réseau internet, afin d'éviter des suppressions de contenus non*

[1198] « *La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants* », LCEN, art. 6, I, 5°.
[1199] Civ. 1ère, 17 février 2011, n° 09-13.202 : *Bull. civ.* I, n° 31 ; *Légipresse* 2011 n° 281, p. 145.
[1200] TGI Paris, 4 décembre 2015, Goyard St-Honoré c/ LBC France.
[1201] TC Paris, 17ème ch., 13 octobre 2008, RG n° 08/98771, *Bachar K.* a. c/20 minutes (SAS) a. : *JCP* G 2008, 646, obs. E. DERIEUX ; *RLDI*, 2008 n° 43, n° 1424, obs. L. COSTES ; *RLDI*, 2008, n° 44, n° 1454, note J.-L. FANDIARI.

nécessaires »[1202]. La Cour d'appel de Paris a relevé dans ce sens que : « *le courrier adressé au prestataire de services ne renseigne aucunement sur les contenus querellés et ne saurait, par voie de conséquence, être regardé comme valant notification au sens de dispositions de la LCEN qui requièrent du notifiant une description et une localisation précises des faits litigieux de manière à permettre au service d'hébergement de reconnaître, dans la masse des documents stockés, les contenus contestés* »[1203]. La Cour d'appel de Bordeaux a de son côté rappelé l'obligation d'identifier avec précision la victime concernée par la notification. En l'occurrence, la victime n'était « *identifié(e) ni par sa profession, ni par son domicile, ni par sa nationalité, ni par ses date et lieu de naissance* »[1204].

459. Le principe de subsidiarité entourant la procédure. Mais surtout, il est imposé à l'auteur de la notification de faire état de « *la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté* ». La procédure de notification de contenu illicite est en conséquence soumise au principe de subsidiarité qui impose à l'auteur de la notification d'avoir au préalable contacté l'auteur du propos problématique pour lui demander de le corriger. Ce principe tend ainsi à ce que les situations problématiques soient réglées de préférence entre les utilisateurs eux-mêmes avant de faire appel au pouvoir de modération des hébergeurs. Ce mécanisme permet alors à la plateforme de se concentrer uniquement sur les cas les plus graves sans être retardée par des litiges pouvant être résolus par les utilisateurs eux-mêmes[1205].

460. Infraction de notification abusive de contenu. En outre, la LCEN prévoit la sanction de toute notification ou signalement abusif de contenus : « *Le fait, pour toute personne, de présenter […] un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende* »[1206]. Cette sanction est

[1202] TGI Paris, 3ème ch., 3ème sect., 13 mai 2009, Temps noir et autres c/ Youtube, Google Inc, Dailymotion : *Légipresse* 2009, n° 263.
[1203] Paris, pôle 5, ch. 1, 13 octobre 2010, R. Magdane C/ Dailymotion : *Légipresse* 2011, n° 277-19.
[1204] Bordeaux, 1ère ch., sect. B., 10 mai 2012, Amen c/ M. K. – sur renvoi : Civ. 1ère, 17 février 2011, n° 09-15.857, *Bull. civ.* I, n° 32, Amen c/ M. K. ; *D.* 2011. 2164, obs. P. SIRINELLI. *D.* 2012. 2836, obs. P. SIRINELLI ; *CCE* 2011, comm. 32, note C. CARON ; Gaz. Pal. 23 avril 2011, n° 113, Chron. 27.
[1205] La *Quadrature du Net* illustre cette idée par l'exemple suivant : une personne cite sur Twitter un propos haineux pour le dénoncer. Ce propos choque toutefois un tiers qui n'est pas certain s'il s'agit d'un propos original ou d'une citation critique. Il serait dès lors plus efficace que ce dernier contacte de lui-même l'auteur du tweet afin de dissiper la confusion et qu'il corrige son message initial de manière à le rendre moins ambigu. « PPL Avia, refusez les mesures inutiles et dangereuses », *La Quadrature du Net*, analyse juridique de la loi « contre la haine en ligne », le 17 juin 2019.
[1206] LCEN, art. 6, I, 4.

indispensable pour rendre le système de notification pérenne. Une responsabilisation tant du notifiant que du prestataire technique est essentielle pour maintenir un équilibre dans ce système de régulation.

461. Il résulte que seule une demande opérant une identification claire de la victime et du contenu litigieux de façon à permettre à l'opérateur de les reconnaître dans la masse des informations qu'il héberge est de nature à faire cesser la mise en ligne de ce contenu. Les internautes s'estimant lésés par un contenu mis en ligne doivent en conséquence faire preuve d'une rigueur particulière dans la procédure de notification du contenu illicite sous peine de nullité de la notification. L'hébergeur soumis à cette procédure doit de son côté supprimer uniquement les contenus revêtant un caractère manifestement illicite.

§2. Le critère central de contenu manifestement illicite

462. La difficile détermination du contenu manifestement illicite. L'article 6 de la LCEN conditionne l'engagement de la responsabilité pénale de l'hébergeur au prompt retrait « *de l'activité ou de l'information illicites* » qui lui a été notifiée. La loi justifie donc le retrait d'un contenu en raison de son caractère illicite qui doit être apprécié par l'hébergeur lui-même dans le cadre de son pouvoir régulateur. La notion d'illicéité est cependant diffuse et peut revêtir un très large spectre. Il est important d'en saisir le sens afin d'apprécier à sa juste valeur le devoir de modération des hébergeurs. Sur ce point, la notion de « *contenu manifestement illicite* », critère central du système de responsabilité mis en place par la LCEN, est censée apporter une neutralité optimale dans le devoir d'interprétation des prestataires techniques (A). Ce critère soulève toutefois des difficultés d'interprétation (B).

A. La notion de contenu manifestement illicite

463. La notion de contenu illicite. La mise en œuvre du pouvoir de régulation de l'opérateur d'un réseau social se justifie selon la LCEN dès lors que le contenu dont il a eu connaissance est illicite. Cette notion doit alors être précisée de manière à prendre la mesure de l'étendue du pouvoir conféré aux hébergeurs. Sur ce point, l'illicéité peut se définir en premier lieu par référence à la conception civiliste de la faute selon laquelle, aux termes de l'article 1382 du Code Napoléon, désormais l'article 1240 depuis l'ordonnance du 10 février 2016, « *tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer* ». Selon cette définition la faute est d'abord « *une*

notion morale, saisie par l'évidence, immédiatement ressentie par tous, sauf dans des cas limites ou pour des consciences tordues »[1207]. L'illicéité est plus large que l'illégalité, autrement dit, ce qui est illégal est forcément illicite alors que ce qui est illicite n'est pas automatique illégal. L'existence d'une règle de droit n'est pas nécessaire pour reconnaître le caractère illicite d'un comportement selon la conception civiliste. Dans cette hypothèse, le juge considère qu'il y a faute lorsque le comportement adopté n'était pas celui qu'aurait adopté dans les mêmes circonstances un homme normal et raisonnable, il s'agit d'une appréciation *in abstracto* catégorielle. Plus largement, l'aspect objectif caractérisant la faute civile, consiste, non seulement en la méconnaissance, intentionnelle ou non, des devoirs imposés par la loi ou les règlements mais plus généralement, en la transgression d'obligations non retranscrites dans des règles écrites. Certains auteurs décrivent ainsi l'illicéité en la méconnaissance d'une norme fondamentale de comportement ou encore d'une norme générale de civilité[1208].

464. La largesse de la conception civile de l'illicéité impose cependant de circonscrire cette notion dans un cadre plus étroit correspondant davantage aux exigences du droit pénal. Sur ce point, André Vitu distinguait l'illicéité pénale de l'illicéité civile par rapport au degré d'anormalité qu'elles suggèrent. L'illicéité est conçue en droit pénal et en droit civil, comme une transgression d'une norme générale de comportement, ces deux notions ne s'opposent donc pas dans leur nature mais davantage dans leur gravité. Le droit pénal se soucie du respect de l'ordre public et non, du moins directement, de l'indemnisation des victimes. L'illicéité pénale est en conséquence plus sévère que l'illicéité civile, elle témoigne de la gravité du comportement incriminé, qui porte plus profondément atteinte aux valeurs protégées. Cette notion se caractérise donc par le « *dépassement d'un certain seuil de tolérance sociale, au-delà duquel le législateur estime nécessaire l'infliction d'une peine* »[1209]. L'illicéité pénale s'observe alors à partir du moment où le caractère inadmissible de la transgression commise nécessite une réaction sociale forte destinée à rétablir la suprématie de la ou des valeurs sociales qui ont été méconnues. Suivant ces remarques, André Vitu définissait la notion d'illicéité pénale comme « *la transgression, en matière pénale, de la norme générale de civilité* ». Plus précisément encore, il s'agit de « *la transgression,*

[1207] P. MALAURIE, L. AYNES, P. STOFFEL-MUNCK, *Droit des obligations*, LGDJ, 9ème éd., 2017, p. 41, n° 47.
[1208] V. par exemple : J. DARBELLAY, *Théorie générale de l'illicéité*, 1955 ; M. PUECH, *L'illicéité dans la responsabilité civile extra-contractuelle*, 1973, p. 50 et suiv.
[1209] A. VITU, « De l'illicéité en droit criminel français », rapport présenté à l'occasion des 2èmes journées franco-helléniques de droit comparé à Nancy, Bull. de la société de législation comparé 1984, p. 127.

manifestée par l'un des agissements définis par une disposition législative ou réglementaire, de la norme de civilité, envisagée à travers l'un ou l'autre des biens juridiques que les pouvoirs publics ont retenus comme dignes de la protection pénale »[1210].

465. La notion de contenu manifestement illicite. La notion d'illicéité, même prise dans sa conception pénaliste, octroie à l'hébergeur une trop grande marge d'appréciation dans son pouvoir de régulation. Cela revient à lui délivrer le pouvoir de définir et de choisir les contenus conformes aux valeurs fondamentales défendues par nos sociétés. Le risque encouru est que, par crainte du non-respect de son obligation, l'hébergeur censure de façon automatique les contenus qui lui sont notifiés en raison de la largesse intrinsèque de cette notion. Face à ce constat, le Conseil constitutionnel a émis dans sa décision du 10 juin 2004[1211] une réserve d'interprétation portant sur l'article 6, I, 2° et 3°. Selon le considérant 9 de la décision, « *les 2 et 3 du I de l'article 6 de la loi déférée ont pour seule portée d'écarter la responsabilité civile et pénale des hébergeurs dans les deux hypothèses qu'ils envisagent ; que ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge* ». Le Conseil constitutionnel, conscient du flou entretenu par l'emploi du seul terme illicite apporte une précision notable en émettant une réserve qui tranche en faveur d'une interprétation restrictive des cas de mise en œuvre de la responsabilité du prestataire. Selon les sages, l'information litigieuse doit apparaître comme constituant ostensiblement un comportement contraire au droit. Cette réserve d'interprétation introduit davantage d'objectivité dans l'appréciation de la notion d'illicéité, le caractère ostensible du contenu doit en effet apparaître de manière certaine pour l'hébergeur. À ce titre plusieurs catégories de contenus apparaissent comme ostensiblement contraires au droit et forment ainsi des domaines particuliers dans lesquels la restriction d'accès aux contenus doit s'exercer de manière privilégiée.

466. Notion de contenus « *odieux* » ou « *sensibles* ». La réserve d'interprétation proposée par le Conseil constitutionnel le 10 juin 2004 ne résout donc pas toutes les interrogations.

[1210] *Ibid.*

[1211] Cons. Const., 10 juin 2004, DC n° 2004-496 : *JO* 22 juin 2004, p. 11182 ; *AJDA* 2004, 1534, note J. ARRIGHI de CASANOVA ; *AJDA*, 1385, tribune P. CASSIA ; *AJDA*, 1497, tribune M. VERPEAUX ; *AJDA*, 1537, note M. GAUTIER et F. MELLERAY, note D. CHAMUSSY ; *AJDA*, 2261, Chron. J.-M. BELORGEY, S. GERVASONI et C. LAMBERT ; *D.* 2005, p. 1125, obs. V. OGIER-BERNAUD et C. SEVERINO ; *RFDA*, 2004, 651, note B. GENEVOIS ; *JCP G* 2004, II, 10117, note P. BLANCHETIEr ; *CCE* 2004, ét. n° 32, note G. DECOCQ ; *LPA* 18 juin 2004, n° 122, p. 10, note J.-E. SCHOETTL.

Certes, elle est source d'une plus grande sécurité juridique mais la qualification d'un contenu illicite, même si l'illicéité doit être manifeste, soulève toujours certains questionnements. Il est ainsi communément admis que cette notion vise principalement les contenus d'une gravité avérée et dont le caractère illicite ne semble pas discutable[1212]. Certains contenus disposent alors par leur nature d'un caractère manifestement illicite. Ces derniers correspondent aux infractions énumérées à l'article 6, I, 7° de la LCEN[1213] formant les dérives les plus graves justifiant un retrait automatique. À l'origine, cette liste d'infractions permettait de distinguer deux principales catégories de trouble à l'ordre public. D'un côté les troubles à l'ordre public résultant d'un discours à savoir : l'apologie de crimes de guerre et des crimes contre l'humanité[1214] ; la diffusion de contenus provoquant à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap[1215] ; des provocations et apologies du terrorisme[1216]. D'un autre côté, les troubles à l'ordre public résultant de la diffusion d'une image ou d'une vidéo comprenant : la diffusion d'images pédopornographiques[1217] ; la diffusion de messages violents, pornographiques ou de nature à porter gravement atteinte à la dignité humaine ou à inciter les mineurs à se livrer à des jeux les mettant physiquement en danger accessibles aux mineurs, lorsque ces contenus sont susceptibles d'être vus ou perçus par un mineur[1218]. Cette liste n'est cependant pas demeurée figée et plusieurs lois sont venues y ajouter des infractions. La loi n° 2016-444 du 13 avril 2016[1219] a ainsi ajouté l'article 225-4-1 du Code pénal luttant contre la traite des êtres humains et les articles 225-5 et 225-6 du Code pénal en matière de proxénétisme. Plus récemment, la loi n° 2018-703 du 3 août

[1212] Concernant l'interprétation des infractions relevant de la catégorie du manifestement illicite v. : L. THOUMYRE, « les hébergeurs en ombres chinoises. Une tentative d'éclaircissement sur les incertitudes de la LCEN », *RLDI*, 2005, n° 5, p. 58 ; L. THOUMYRE, « Comment les hébergeurs français sont devenus juges du manifestement illicite », Juriscom.net, 28 juillet 2004 ; L. THOUMYRE, « Valse constitutionnelle à trois temps sur la responsabilité des intermédiaires techniques », *Légipresse* 2004, nº 214, p. 129 et suiv. ; M. VIVANT, « Entre ancien et nouveau - une quête désordonnée de confiance pour l'économie numérique », *Cahiers Lamy droit de l'informatique et des réseaux*, juillet 2004, nº 171, p. 2.

[1213] Cet article précise que : « *compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième, septième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 222-33, 225-4-1, 225-5, 225-6, 227-23 et 227-24 et 421-2-5 du code pénal* ».

[1214] L. 29 juillet 1881, art. 24, al. 5.

[1215] L. 29 juillet 1881, art. 24, al. 8.

[1216] C. pén., art. 421-2-5.

[1217] C. pén., art. 227-23.

[1218] C. pén., art. 227-24.

[1219] L. n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées, *JORF* n° 0088, 14 avril 2016, art. 1er.

2018[1220] a complété la liste par le délit de harcèlement sexuel prévu à l'article 222-33 du Code pénal. Ces contenus dits « *sensibles* » ou « *odieux* » entraînent une obligation de retrait immédiat et volontaire de l'hébergeur indépendamment d'une décision judiciaire[1221]. La Cour d'appel de Paris rappelle dans ce sens « *qu'à l'exception de certaines diffusions expressément visées par la loi relative à la pornographie enfantine, l'apologie des crimes contre l'humanité, et à l'incitation à la haine raciale que l'hébergeur doit, sans attendre une décision de justice, supprimer, l'hébergeur n'est pas tenu de retirer les contenus non manifestement illicites* »[1222]. Ces infractions, forment ainsi les bases de l'ordre public à l'échelle numérique que les intermédiaires techniques se doivent de protéger.

B. La difficile interprétation de la notion de contenu manifestement illicite

467. Si la catégorie des contenus « *odieux* » semble introduire une référence stable et précise au critère de « *contenu manifestement illicite* », le travail d'interprétation du juge en matière de discours haineux démontre toutefois la difficile appréhension de ce type particulier d'infractions (1), entraînant dès lors un risque de suppression conservatoire des contenus notifiés (2).

1) La difficile appréhension des discours de haine

468. La fine délimitation entre discours haineux pénalement sanctionné et liberté d'opinion. Si l'article 6, I, 7° de la LCEN fait entrer les délits de diffamation raciale et de provocation à la haine dans la catégorie des contenus manifestement illicites l'étude de la jurisprudence relative à ces infractions révèle en réalité le « *travail d'orfèvre* » et le « *numéro d'équilibriste* »[1223] réalisé par le juge au moment de la qualification de ces infractions. En effet, le législateur ne réprime pas un discours dès lors qu'il revêt un caractère raciste ou discriminatoire. Ce dernier sanctionne un propos qui, entrant sous une qualification pénale précise, devient préjudiciable. En dehors des cas décrits par les incriminations de diffamation, injure ou de provocation à la haine raciale, la parole est libre même si elle peut apparaître choquante ou intolérable. Ce principe est clairement rappelé par la Cour EDH selon laquelle

[1220] L. n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, *JORF* n° 0179, 5 août 2018, art. 11.
[1221] Ce principe a été rappelé par les juges du fond, v. notamment : TGI Paris, ord. Réf., 9 janvier 2008, RG n° 07/58913, R. Mezrahi a. c/ YouTube Inc.
[1222] Paris, pôle 1, ch. 2, 4 avril 2013, RG n° 12/12001, B. Rose c/ JFG Networks.
[1223] N. DROIN, « L'appréhension des discours de haine par les juridictions françaises : entre travail d'orfèvre et numéro d'équilibriste », *RevDH*, n° 14, 21 juillet 2018.
<http://journals.openedition.org/revdh/4302> (dernière consultation le 9 octobre 2019).

la liberté d'expression couvre également « *les idées qui heurtent, choquent ou inquiètent l'État ou une fraction quelconque de la population* »[1224]. Dès lors la limite entre d'un côté, la liberté d'opinion autorisant certains discours houleux et de l'autre, la pénalisation de certaines formes d'expression strictement encadrée par des textes d'incriminations, n'est pas toujours évidente à établir.

469. La stigmatisation d'une personne ou d'un groupe de personnes. Pour apprécier, le plus objectivement possible, la concordance du propos aux éléments constitutifs du délit, le juge se livre à une lecture stricte et neutre du texte d'incrimination, tout en prenant également en considération le contexte dans lequel le propos a été diffusé[1225]. Ainsi, les délits prévus aux articles 32 alinéas 2 et 3, 33 alinéas 3 et 4, et 24 alinéas 7 et 8 de la loi sur la liberté de la presse doivent viser une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, ou, à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap. Les incriminations exigent donc une victime ou un groupe de victimes identifié ou identifiable pris dans sa globalité. Par exemple, Éric Zemmour fut poursuivi du chef de diffamation raciale prévu au deuxième alinéa de l'article 32 de la loi du 29 juillet 1881 pour avoir tenu à la radio les propos suivants : « *Les Normandes, les Huns, les Arabes, les grandes invasions d'après la chute de Rome sont désormais remplacés par les bandes de Tchétchènes, de Roms, de Kosovars, de Maghrébins, d'Africains qui dévalisent, violentent ou dépouillent* ». Ce dernier fut cependant relaxé par un jugement de première instance confirmé en appel le 22 juin 2016[1226]. Les juges du fond justifièrent leur relaxe au motif qu' « *aussi excessifs, choquants ou provocants que ces propos puissent paraître* », ils ne s'appliquent « *qu'à une fraction des communautés visées et non à celles-ci dans leur ensemble* ». De même, l'écrivain Michel Houellebecq fut poursuivi pour avoir tenu les propos suivants : « *La religion la plus con, c'est quand même l'Islam* ». Ce dernier fut toutefois relaxé au motif que les propos en cause visent un système de pensées et non des personnes à raison de leur appartenance religieuse[1227]. Dans la même dynamique, la Cour de cassation a estimé en 2018

[1224] CEDH, *Handyside c. Royaume-Uni*, 7 décembre 1976, n° 5493/72, n° 49.
[1225] N. DROIN, « L'appréhension des discours de haine par les juridictions françaises : entre travail d'orfèvre et numéro d'équilibriste », *op. cit.*, p. 8.
[1226] Paris, Pôle 2, Chambre 7, 22 juin 2016, E Zemmour et autres contre Licra et autres : *Légipresse* n° 341, p. 460.
[1227] TGI Paris, 17ème ch., 22 octobre 2002, *Légipresse*, 2003, n° 198-I, p. 12.

que l'inscription « *Fuck church* » peinte sur la poitrine dénudée de plusieurs Femen ne constituait pas le délit d'injure envers la communauté catholique[1228].

470. L'imputation d'un fait déterminé en matière de diffamation. Par ailleurs, pour que les délits de la loi sur la liberté de la presse soient constitués il doit être démontré un comportement préjudiciable. La seule teneure raciste ou ségrégationniste d'un discours ne rassemble pas nécessairement l'ensemble des éléments constitutifs de l'infraction. Ainsi, le délit de diffamation raciale impose l'imputation d'un fait déterminé portant atteinte à l'honneur ou à la considération de la personne ou d'un groupe de personne à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée[1229]. Suivant ces remarques, il a été jugé que constituait le délit de diffamation le fait d' « *imputer aux personnes de confession juive de se livrer, plus que toute autre communauté, à l'inceste, constitue bien une affirmation à la fois précise, ce point pouvant faire l'objet d'un débat argumenté, et attentatoire à l'honneur et à la considération de la communauté visée* »[1230]. Le même jugement a cependant considéré que l'affirmation selon laquelle les juifs « *travestiraient systématiquement la vérité afin de se faire passer pour des victimes* » ne manifeste que « *l'expression d'une opinion qui ne saurait faire l'objet d'un débat probatoire* ».

471. Les incertitudes entourant la définition du délit de provocation. Concernant le délit de provocation à la discrimination, à la haine et à la violence prévu aux alinéas 7 et 8 de l'article 24 de la loi sur la liberté de la presse, les juges doivent établir l'existence d'une provocation, « *se traduisant par un acte positif d'incitation manifeste à la discrimination, à la haine ou à la violence* »[1231]. La Cour de cassation rappelle ainsi que toute publication choquante n'est pas assimilable à une provocation à la discrimination, à la haine ou à la violence et que la provocation ne se conçoit que par l'incitation ou l'exhortation. Autrement dit, un discours raciste ou xénophobe n'est pas nécessairement une provocation : une idée peut être outrageante sans entrer dans le champ d'application des provocations[1232]. Malgré ces précisions, la délimitation de la frontière de la définition pénale de l'acte de provocation reste soumise à interprétation y compris en doctrine. D'un côté le Professeur Emmanuel Dreyer

[1228] Crim., 23 janvier 2018, n° 17-80.524 : inédit ; *Légipresse* 2018, p. 154, note E. DREYER ; Gaz. Pal. 30 avril 2018, n° 16, p. 52, obs. S. DETRAZ.
[1229] L. 29 juillet 1881, art. 32, al. 2.
[1230] TGI, 17ème ch., 15 décembre 2016, n° 13059000638 : *Légipresse*, 2017, n° 346, p. 71.
[1231] Crim., 7 juin 2017, n° 16-80.322 : *Légipresse*, 2017, p. 1814, note C. BIGOT ; *AJ Pénal*, 2017, p. 398, obs. J.-B. THIERRY. *Adde* : N. DROIN, « L'appréhension des discours de haine par les juridictions françaises : entre travail d'orfèvre et numéro d'équilibriste », *op. cit.*, p. 10.
[1232] J.-B. THIERRY, « Choquer n'est pas provoquer », *AJ Pénal*, 2017, p. 398.

justifie une interprétation extensive du délit de provocation « *afin de permettre la sanction de publications contenant une provocation déguisée à la haine, à la discrimination ou à la violence* ». Ce dernier précise alors qu'en adoptant une conception trop stricte du présent délit, « *la haute juridiction prive les parquets d'un moyen de poursuite efficace contre les propos ségrégationnistes* »[1233]. À l'inverse, Madame Nathalie Droin privilégie le choix d'une appréciation stricte des éléments constitutifs du délit pour plusieurs raisons : « *d'une part, car elle est davantage conforme à la lettre même de l'article 24 alinéas 7 et 8 […]et par voie de conséquence, au principe d'interprétation stricte de la loi pénale, […] ; d'autre part, car elle permet de distinguer le champ d'application du délit d'injure, qui vise le propos outrageant, le terme de mépris, et le délit de provocation qui, lui, serait circonscrit à l'appel à commettre un acte de haine, de discrimination ou de violence ; enfin, car une telle interprétation paraît davantage en phase avec la loi sur la presse elle-même qui entend sanctionner des comportements précis* »[1234]. Ces hésitations démontrent au final toute la difficulté d'apprécier l'illicéité d'un propos revêtant par apparence l'aspect du délit de provocation à la discrimination, à la haine et à la violence prévu aux alinéas 7 et 8 de l'article 24 de la loi sur la liberté de la presse.

472. La difficile délimitation des discours négationnistes. L'appréhension du caractère manifestement illicite d'un contenu ne se limite toutefois pas aux seuls propos appartenant à la catégorie des contenus « *odieux* ». Le délit de négationnisme prévu à l'article 24 *bis* de la loi du 29 juillet 1881 pourrait apparaître de prime abord comme facilement identifiable par les hébergeurs, son analyse juridique révèle cependant une complexité d'interprétation. L'affaire ayant opposé le Comité de défense de la cause arménienne (CDCA) à France Télécom le 15 novembre 2004[1235] illustre le propos. En l'espèce, le Comité reprochait au Consul de Turquie d'avoir mis en ligne des propos négationnistes qui contestaient l'existence du génocide arménien. Ce message aurait pu être légitimement considéré par un profane comme manifestement illicite alors que sa réalité juridique est bien plus nuancée. En effet, le tribunal de grande instance de Paris a suivi la position de l'hébergeur en écartant la qualification de contenu manifestement illicite pour les messages concernés. Selon la juridiction le génocide arménien ne fait pas partie des crimes dont la contestation est punissable et la loi du 29 janvier 2001, reconnaissant l'existence du génocide arménien de 1915, ne crée pas pour autant un

[1233] Obs. E. Dreyer sous Crim. 14 novembre 2017, n° 16-84.945 : inédit ; *D.*, 2018, p. 213.
[1234] N. DROIN, « L'appréhension des discours de haine par les juridictions françaises : entre travail d'orfèvre et numéro d'équilibriste », *RevDH*, n° 14, 21 juillet 2018, p. 10.
[1235] TGI Paris, 15 novembre 2004, Comité de défense de la cause arménienne c/ M. Aydin A. et Sté France Télécom : <www.legalis.net>.

délit de contestation de ce génocide et n'entre dès lors pas dans les prévisions de l'article 24 *bis* de la loi du 29 juillet 1881[1236]. Ainsi, la pénalisation du négationnisme démontre également la difficulté de déterminer si un contenu se révèle illicite ou si, à l'inverse, il s'avère totalement licite. L'infraction de négationnisme est présente à l'échelle européenne mais certaines divergences de principe existent entre les États et soulèvent de nombreuses difficultés dans la définition de ses contours[1237]. Partant du constat que la définition même de l'infraction divise les juges[1238] et mobilise la doctrine[1239], l'identification d'un propos entrant effectivement sous la qualification pénale du négationnisme s'avère être une entreprise délicate pour l'hébergeur.

2) Le risque de suppression conservatoire des contenus notifés

473. L'Affaire WikiLeaks : le refus du juge de se positionner à la place de l'hébergeur. Les difficultés entourant l'appréciation de l'illicéité de certains contenus amène alors les hébergeurs à se tourner vers l'appréciation d'un juge. C'est le comportement qu'a précisément adopté la société OVH lorsqu'elle s'est vue demander le retrait du site Wikileaks qu'elle hébergeait. Les publications litigieuses concernaient la mise en ligne sur le site Wikileaks d'indiscrétions relatives à des échanges d'informations de services diplomatiques étrangers[1240]. L'hébergeur devait alors déterminer si ces informations révélées par le site d'information revêtaient un caractère manifestement illicite et s'il était en conséquence tenu de les supprimer. Or, le caractère illicite des contenus diffusés ne souffrait pas d'une certitude implacable compte tenu de l'étendue transnationale de leur diffusion et de la nature des messages concernés qui impliquait une mise en balance délicate entre d'un côté le droit à

[1236] TGI Paris, 15 novembre 2004, Comité de défense de la cause arménienne c/ M. Aydin A. et Sté France Télécom : <www.legalis.net>.
[1237] F. DUBUISSON, « Les restrictions à l'accès au contenu d'internet et le droit à la liberté d'expression », *in* : *Internet et le droit international*, société française pour le droit international, colloque de Rouen, Éd. A. Pedone, p. 156.
[1238] Concernant les difficultés de qualification du discours négationniste par le juge V. : F. DUBUISSON, « les ambivalences du rôle du juge pénal belge et français dans le répression du négationnisme réflexion à partir de l'affaire Assabyle », *in* J. ALLARD et O. CORTEN, *La vérité en procès le juge et la vérité politique*, Actes du colloque de l'ULB/ARC, 8-9 septembre 2011, LGDJ, p. 143 et suiv.
[1239] V. R. BADINTER, « De la nécessaire répression du négationnisme en France », *in Mélanges en l'honneur de Jean-Claude Colliard*, Dalloz, Avril 2014, p. 51 et suiv.
[1240] V. notamment sur la question : M. DOUEIHI, « La nouvelle fracture numérique. La fuite de documents secrets... », Le Monde, 7 décembre 2010 ; Y. EUDES, « WikiLeaks, contrebandier de l'info », Le Monde, 3 juin 2010 ; C. FOUREST, « La fuite et la victoire du filtre », Le Monde, 4 décembre 2010 ; B. FRAPPAT, « Révélations et civilisation », La Croix, 4 décembre 2010 ; B. GUETTA, « La presse et la transparence informatique », Libération, 1er décembre 2010 ; S. KAUFFMANN, « Les rapports secrets du département d'État. Pourquoi et comment publier ces documents ? », Le Monde, 30 novembre 2010.

l'information et de l'autre le droit au secret[1241]. C'est pourquoi, les fournisseurs d'hébergement français s'en sont remis aux juges, par voie d'ordonnance sur requête, pour que ceux-ci déterminent, sans dangers, la ligne de conduite à tenir. Les juges du tribunal de grande instance de Paris[1242] et de Lille[1243] ont cependant refusé de statuer sur ce point, renvoyant la société requérante face à ses incertitudes, au risque d'engager sa responsabilité pour n'avoir pas adopté le comportement adéquat[1244]. Ne voulant pas risquer un engagement de leur responsabilité, les hébergeurs ont alors développé une pratique tendant à la suppression conservatoire des contenus qui leur seraient notifiés.

474. La suppression conservatoire des contenus validée par la jurisprudence. Dans le but de préserver leur responsabilité, certains hébergeurs choisissent de supprimer d'office tout contenu « *problématique* » qui leur serait notifié au risque de censurer un contenu ne revêtant pas *in fine* un caractère illicite[1245]. L'affaire ayant opposé Roselyne Bosh, la réalisatrice du film *La Rafle* à la société JFG Networks spécialisée dans la gestion de sites internet illustre ce propos[1246]. La réalisatrice reprochait à la société de ne pas avoir supprimé après notification le contenu d'un blog qui apparaissait attentatoire à sa réputation alors que selon elle « *presque tous les hébergeurs ayant reçu notification conforme aux dispositions de l'article 6 de la […] LCEN, ont décidé le retrait sauf deux* ». Ainsi, la quasi-totalité des hébergeurs avait fait droit en dehors de toute procédure judiciaire à la demande de suppression du contenu litigieux alors même que les juges de la Cour d'appel de Paris ont finalement considéré que le propos incriminé ne dépassait pas le cadre admissible de l'exercice de la liberté d'expression[1247]. Une autre affaire concernait la suppression par le réseau social Facebook de la page « *Plus belle la vie* » qui visait à rassembler et renseigner les fans de la série. La société productrice de l'émission ordonna sur requête la suppression de cette page au motif d'une violation de ses droits de marque portant sur la dénomination « *plus belle la vie* ». Le réseau social s'exécuta d'office. L'animatrice de la page litigieuse engagea alors une action judiciaire pour réclamer le rétablissement de sa page. Le juge du TGI de Paris[1248] fit droit à sa demande en relevant

[1241] E. DÉRIEUX, « Droit à l'information et droit au secret : pour un équilibre des droits », *Légipresse* 2011, nº 279, p. 3-4.
[1242] TGI Paris, ord. req., 6 décembre 2010, Société OVH : *RLDI*, 2011, n° 67.
[1243] TGI Lille, ord. req., 6 déc 2010, Société OVH : *RLDI*, 2011, n° 67.
[1244] E. DERIEUX, « Responsabilité des services de communication au public en ligne. Appréciation des contenus hébergés. Prendre la décision de colmater les fuites ? », *RLDI*, 2011, n° 68.
[1245] F. DUBUISSON, « Les restrictions à l'accès au contenu d'internet et le droit à la liberté d'expression », *op. cit.*, p. 139.
[1246] Paris, Rose B. c. JFG Networks, 4 avril 2013, www.legalis.net.
[1247] F. DUBUISSON, « Les restrictions à l'accès au contenu d'internet et le droit à la liberté d'expression », *op. cit.*, p. 139.
[1248] TGI Paris, Laurence c. / Telfrance Serie, Facebook France, 28 novembre 2013, <www.legalis.net>.

que la page en question ne relevait pas de « *la vie des affaires* » et ne poursuivait aucune finalité commerciale. Toutefois, le juge estima que la société Facebook ne devait pas être mise en cause du fait que la demande de la société Telfrance série qui était titulaire du droit de la marque « *Plus belle la vie* » « *pouvait apparaître fondée pour la société Facebook France, tenue d'intervenir rapidement* ». Dans d'autres circonstances encore, les juridictions ont retenu une interprétation extensive du terme manifestement illicite pour justifier le retrait par les hébergeurs des contenus qui leur sont notifiés. Par exemple, dans certaines affaires, elles n'ont pas hésité à juger que l'injure et la diffamation publiques « *constituent un trouble manifestement illicite qui justifie le retrait des textes litigieux* »[1249]. Ces exemples sont révélateurs de la tendance de la jurisprudence à favoriser, dans le cadre du régime de responsabilité des intermédiaires, la suppression conservatoire de contenus, dont l'illicéité n'est pourtant pas manifeste.

475. Un déséquilibre entre sauvegarde de l'ordre public et préservation des libertés. Selon le Professeur Benoît Frydman, pour que la régulation fonctionne il est nécessaire que les intermédiaires techniques bénéficiant d'un statut privilégié ne puissent voir leur responsabilité engagée dans l'hypothèse où ils supprimeraient un contenu qu'ils pensaient illicite mais qui s'avèrerait *in fine* légal. Autrement dit, pour que le système de responsabilité de *notice and take down* mis en place fonctionne et que la régulation des contenus notamment haineux soit effective, il est primordial de ne pas reprocher à un intermédiaire technique un excès de zèle suite à une notification d'un contenu pouvant apparaître comme illicite[1250]. Le Professeur Benoît Frydman souligne alors que ce principe est reconnu en droit américain dans une clause appelée « *The Good Samaritan provision* »[1251]. Ce point de vue s'oppose cependant à la décision du Conseil constitutionnel du 10 juin 2004[1252] précisant que l'hébergeur ne peut exercer son pouvoir de modération si le contenu qui lui est notifié ne présente pas manifestement un caractère illicite ou si son retrait n'a pas été ordonné par un

[1249] Paris, Ch. 14, sect. B, 21 janvier 2005, n°04/14975.
[1250] B. FRYDMAN, I. RORIVE, « Regulating Internet Content through Intermediaries in Europe and the USA », *Zeitschrift für Rechtssoziologie* (revue de l'Institut Max Planck de Cologne), 2002, vol. 23 (1), p. 41-59.
[1251] Selon cette clause : « *No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected* ». CDA 47 U.S.C. § 230 (c) (2) (A). <https://www.law.cornell.edu/uscode/text/47/230>
[1252] Cons. const., 10 juin 2004, DC n° 2004-496, *JO* 22 juin 2004, p. 11182 ; *AJDA* 2004, 1534, note J. ARRIGHI de CASANOVA ; *AJDA*, 1385, tribune P. CASSIA ; *AJDA*, 1497, tribune M. VERPEAUX ; *AJDA*, 1537, note M. GAUTIER et F. MELLERAY, note D. CHAMUSSY ; *AJDA*, 2261, chron. J.-M. BELORGEY, S. GERVASONI et C. LAMBERT ; *D.* 2005, p. 1125, obs. V. OGIER-BERNAUD et C. SEVERINO ; *RFDA*, 2004, 651, note B. GENEVOIS ; *JCP G* 2004. II. 10117, note P. BLANCHETIER ; *CCE* 2004, ét. n° 32, note G. DECOCQ ; *LPA* 18 juin 2004, n° 122, p. 10, note J.-E. SCHOETTL.

juge. Plus généralement, la pratique systématique de la suppression conservatoire de contenus tendrait vers une situation dangereuse pour la liberté d'opinion et entraînerait un déséquilibre certain entre l'objectif de protection de l'ordre public à l'échelle numérique et l'exercice des droits et libertés.

476. Conclusion de la Section 1. Si le pouvoir de régulation accordé aux hébergeurs est encadré par la loi et contrôlé par la jurisprudence, la pratique de ce dernier se détache toutefois des prévisions textuelles. Le régime de *notice and take down* confie à des acteurs privés la possibilité de déterminer le caractère licite ou non d'un contenu qui est porté à leur connaissance. De plus, le critère de contenu manifestement illicite sensé évincer les incertitudes relatives au caractère licite ou non du contenu et restreindre le pouvoir de modération aux contenus les plus « *odieux* » et « *sensibles* » se révèle en réalité difficile à interpréter, amenant le risque d'être appliqué au-delà de ses prévisions. Ainsi, les contenus rendus inaccessibles ne relèvent pas nécessairement du « *manifestement* » illicite, voire, de l'illicite. En la matière, la justice manifeste son accord à cette pratique en ne sanctionnant pas l'hébergeur qui a voulu se montrer diligent par rapport à ses obligations. Cependant, le juge ne joue pas pleinement son rôle lorsque, saisi par l'hébergeur faisant face à une difficulté d'interprétation, il refuse de se prononcer sur la licéité d'un contenu. Dès lors, les hébergeurs sont incités à réaliser une suppression conservatoire des signalements de contenus apparaissant comme un discours haineux. Une telle pratique serait nécessairement néfaste du point de vue de la liberté d'expression et plus précisément du principe selon chaque individu dispose de la liberté d'exprimer des opinions qui heurtent, choquent ou inquiètent. Au final, l'ensemble de ces mécanismes juridiques tendent vers la situation décriée par le rapporteur spécial des Nations Unies Franck Larue selon lequel un pouvoir de modération est délégué à une entité privée qui s'arroge le droit au travers ses conditions générales d'utilisation de supprimer de façon discrétionnaire les contenus qui lui sont soumis[1253].

Il s'agit dès lors de mettre en évidence la pratique de la régulation des contenus menée par les opérateurs des réseaux sociaux et de démontrer son incohérence avec le régime de responsabilité mis en place par la LCEN.

[1253] F. LARUE, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, Assemblée générale des Nations Unies, Conseil des droits de l'homme, 17ème session, 16 mai 2011, p. 13, n° 43.

Section 2 : Un système de régulation privé de l'expression insatisfaisant

477. Une régulation privée de l'expression menaçant les standards européens. L'encadrement du pouvoir de régulation des sites de réseaux sociaux par la procédure de notification de contenus illicites ne permet pas d'assurer un traitement satisfaisant des contenus. Bien loin de pratiquer une suppression conservatoire des contenus notifiés, les opérateurs des réseaux sociaux privilégient en réalité leurs propres critères, autrement dit, leurs conditions générales d'utilisations (CGU). Ceci est d'autant plus problématique au vu de l'importance acquise par les sites de réseaux sociaux dans la circulation de l'information. Cette régulation des contenus par des opérateurs privés menace la sécurité juridique du traitement des contenus en ligne dans la mesure où leurs règles internes ne coïncident pas toujours avec les contours de l'ordre public européen. Ainsi, la modération des contenus pratiquée par les opérateurs des réseaux sociaux (**§1**) permet de mettre en avant le conflit entre ce système de régulation privée et certains standards juridiques européens (**§2**).

§1. La pratique de la modération des contenus par les opérateurs des réseaux sociaux

478. Les opérateurs des réseaux sociaux, maîtres de leur politique de modération. Lorsqu'un contenu est signalé ou notifié, la décision finale de suppression du contenu revient au seul hébergeur. Les opérateurs des réseaux sociaux effectuent en conséquence des qualifications juridiques et décident en fonction si le contenu à vocation à être modéré. L'interprétation autonome des contenus indésirables (A) et les moyens de régulation opaques mis en œuvre (B) permettent d'aboutir à une critique du système de régulation exercé par les opérateurs des réseaux sociaux.

A. Une interprétation autonome des contenus indésirables

479. Un pouvoir de modération s'affranchissant du critère du contenu manifestement illicite. La capacité technique des hébergeurs à agir sur les contenus diffusés sur leurs plateformes leurs confèrent le pouvoir de mettre en place une politique de modération de contenus. Chaque réseau social applique alors ses propres règles édictées dans ses conditions générales d'utilisation, acceptées par les utilisateurs au moment de leur inscription. Cette relation d'ordre contractuel régit cependant des comportements pouvant revêtir des qualifications pénales. Pour ce faire, chaque plateforme définit de manière autonome les

standards de sa communauté et les comportements qu'elle considère comme illicites[1254]. Ces interdictions rejoignent peu ou prou les principales qualifications pénales figurant en droit interne et notamment celles relevant de la catégorie des contenus manifestement illicites. Cependant, l'autonomie laissée aux opérateurs des réseaux sociaux dans l'interprétation de leurs conditions générales d'utilisation révèle les libertés prises par ces derniers dans l'interprétation de ce critère pourtant central dans le système de *notice and take down*. Se dessine une opposition entre une modération souple des discours (1) et une modération stricte de l'image (2) révélant la liberté d'action de ces plateformes d'échange dans la régulation des contenus qui y transitent.

1) Une modération souple des discours

480. Une faible réactivité des opérateurs en matière de discours haineux. Bien que l'interprétation d'un discours haineux pénalement sanctionné s'avère être une entreprise délicate[1255], la prolifération de ce type de discours sur les sites de réseaux sociaux est une réalité problématique qui ne saurait être contestée[1256]. Plus encore, les caractéristiques et le fonctionnement des sites de réseaux sociaux favorisent la multiplication de ce type de discours. Par exemple, l'anonymat offert par ces plateformes suscite chez certains individus un sentiment d'impunité amenant ainsi la parole à se délier favorisant l'apparition des discours violents. Or, en parallèle de ce constat, les contenus haineux ne sont que faiblement modérés alors même qu'ils sont de nature à relever de qualifications pénales. Ce faible taux de modération a été mis pour la première fois en évidence dans un communiqué de presse

[1254] Par exemple, Facebook proscrit dans ces standards les contenus suivants : Standards Facebook : « *Discours incitant à la haine* » ; « *Contenu violent et explicite* » ; « *Nudité et activités sexuelles chez les adultes* » ; « *Violence crédible* » ; « *Individus et organismes dangereux* » ; « *Promotion de crime* » ; «*Violence organisée* » ; « *Marchandises réglementées* » ; « *Suicide et automutilation* » ; « *Nudité et exploitation sexuelle des enfants* » ; « *Exploitation sexuelle des adultes* » ; « *Intimidation* » « *Harcèlement* » ; « *Violations de la vie privée et droit à la confidentialité des images* » ; « *Discours incitant à la haine* » ; « *Contenu violent et explicite* » ; « *Nudité et activités sexuelles chez les adultes* » ; « *Sollicitation sexuelle* » ; « *Cruel et indélicat* » ; « *Contenu indésirable* » ; « *Représentations frauduleuses* » ; « *Fausses informations* » ; « *Commémoration* » ; « *Propriété intellectuelle* » ; Twitter interdit quant à lui les contenus suivants : « *Violence et blessures* » « *Comportement inapproprié et conduite haineuse* » « *Informations privées et médias intimes* » « *Usurpation d'identité* » « *les abus techniques et le spam* ».

[1255] V. *supra* n° 468 et suiv.

[1256] De nombreux rapports, études, avis ou ouvrages s'accordent à reconnaître la prolifération des discours haineux sur internet et les sites de réseaux sociaux en particulier, parmi lesquels : K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018 ; M. KNOBEL, *L'internet de la haine*, Berg International Éditeurs, 2012 ; *Dalloz IP/IT*, dossier « La haine sur Internet », 2017 p. 562 à 583 ; CE, *Le numérique et les droits fondamentaux*, étude annuelle 2014, p. 215 ; Recommandation n° R(97)20 du comité des Ministres aux Etats membres, sur le « discours de haine » adoptée le 30 octobre 1997 ; Communiqué de presse du Conseil national du numérique, *Le CNNum exprime ses interrogations sur la proposition de loi visant à lutter contre la haine sur Internet*, le 21 mars 2019, p. 3 ; A. JOMNI, « Du discours de haine en ligne au cyberterrorisme : quelles régulations possibles ? », *Dalloz IP/IT* 2017, p. 563.

publié le 15 mai 2016, des associations UEJF, SOS Racisme et SOS homophobie[1257]. Pour ce faire, les associations ont organisé entre le 31 mars et le 10 mai 2016 une opération de *testing* visant les trois principales plateformes numériques à savoir les sociétés Facebook, Twitter et YouTube. Cette opération a entrainé le signalement de 586 contenus racistes, antisémites, négationnistes, homophobes ou encore faisant l'apologie du terrorisme ou de crimes contre l'humanité. Sur les 586 contenus signalés, seuls 4 % ont été supprimés sur Twitter[1258], 7% sur YouTube[1259] et 34% sur Facebook[1260]. Ce constat d'inertie dans la réactivité des opérateurs des réseaux sociaux a également été observé en Allemagne par le ministère fédéral de la Famille et le Ministère fédéral de la Justice et de la protection des consommateurs qui ont réalisés une série de signalements, plusieurs centaines au total, à ces trois mêmes acteurs. YouTube a démontré pour sa part une réactivité satisfaisante avec un taux de plus de 90% de suppression mais concernant Facebook le chiffre n'est plus que de 39% alors que pour Twitter le chiffre n'est plus que de 1%[1261]. Dans une étude publiée en mars 2010[1262], le Centre Simon Wiesenthal observait une hausse de 20% des propos à teneur terroriste et raciste diffusés principalement sur les réseaux sociaux Facebook et Twitter. Le rapport a mis en évidence que les sites de réseaux sociaux sont de plus en plus utilisés pour véhiculer des messages de haine particulièrement à destination du jeune public. Le Centre a ainsi identifié en 2009 10 000 sites, forums ou comptes twitter réputés « *problématiques* » car faisant la promotion de l'antisémitisme, de l'homophobie ou du terrorisme, puis environ 11 550 en 2010[1263]. Face à ce constat, la politique extrêmement permissive des principaux réseaux sociaux concernant les vidéos, images ou textes incitant à la haine ou à la violence fait l'objet de vives critiques. Il est notamment reproché à ces plateformes leur manque de coopération dans la lutte contre la

[1257] Communiqué de Presse de l'UEJF, SOS Racisme et SOS homophobie, « L'UEJF, SOS Racisme et SOS homophobie portent plainte contre Twitter, YouTube et Facebook pour non-respect de leurs obligations de modération », le 15 mai 2016.
<https://www.sos-homophobie.org/article/l-uejf-sos-racisme-et-sos-homophobie-portent-plainte-contre-twitter-youtube-et-facebook-pour> (dernière consultation le 9 octobre 2019).
[1258] Sur les 205 contenus haineux signalés à Twitter, seuls 8 ont été supprimés.
[1259] Sur les 225 contenus haineux signalés à YouTube, 16 ont été supprimés.
[1260] Sur les 156 contenus haineux signalés à Facebook 53 ont été supprimés.
[1261] Monsieur Emmanuel Netter précise toutefois que ces chiffres résultent de signalements réalisés par un utilisateur ordinaire. Les résultats sont différents lorsque le signalement est effectué par un compte dont l'identité est vérifiée ou encore lorsque le signalement est effectué par courrier électronique. Ainsi, « *pour Twitter on distingue un taux de 1% de suppression après signalement ordinaire, puis 63% après un signalement par un compte vérifié, et enfin 36% après l'envoi d'un courriel. Concernant YouTube, les chiffres sont respectivement de 90%, 7% et 3%. Facebook se distingue en laissant 7% de contenus illicites en ligne même après l'emploi de toutes les méthodes de signalement* ». E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, p. 195, n° 62.
[1262] Centre Simon Wiesenthal, « Digital Terrorism and Hate », 2011.
<http://www.wiesenthal.com/about/news/hate-in-the-digital-age.html> (dernière consultation le 9 octobre 2019).
[1263] Chiffres cités *in* : M. KNOBEL, *L'internet de la haine*, Berg International Éditeurs, 2012, p. 138.

haine[1264]. Cette absence de rigueur des réseaux sociaux dans leur pouvoir de modération s'explique en réalité par l'absence d'intérêt de ces sites à censurer outre mesure ce type de contenu, les discours haineux et sulfureux générant un maximum d'interactions et contribuant ainsi à entretenir le modèle économique de ces sites[1265].

Si les réseaux sociaux sus mentionnés font preuve d'une particulière souplesse dans la modération des discours y compris ceux de nature à présenter un caractère « *odieux* » ou « *sensibles* » au sens de l'article 6, I, 7 alinéa 3 de la LCEN, à l'inverse, ils opèrent une modération particulièrement stricte de l'image, allant au-delà du champ restrictif de la notion de contenu manifestement illicite.

2) Une modération stricte de l'image

481. Une modération stricte de la nudité. L'autonomie des opérateurs des réseaux sociaux dans la définition et la gestion des contenus illicites peut entraîner une modération outrancière de certains contenus. Dans cette hypothèse, les contenus supprimés ne revêtent pas un caractère manifestement illicite, pis encore, l'illicéité même des contenus est discutable. Le pouvoir de modération devient alors un instrument de censure dont la légitimité est discutable. Ce propos peut être illustré par la politique de modération de la nudité sur le réseau social Facebook. En l'occurrence, ce réseau social interdit la nudité sur sa plateforme :

« *Nous limitons l'affichage de scènes de nudité et d'activités sexuelles, car certaines personnes au sein de notre communauté peuvent être sensibles à ce type de contenu. En outre, nous supprimons par défaut les images de nature sexuelle pour empêcher le partage de contenus montrant des actes non consentis ou des mineurs. Les restrictions sur l'affichage d'activité sexuelle s'appliquent également au contenu créé numériquement, sauf si le contenu est publié à des fins pédagogiques, humoristiques ou satiriques* »[1266].

482. Cette disposition a conduit Facebook à opérer une politique de censure quasi automatique des contenus représentant de la nudité. Ce manque de filtres dans la modération de ce type de contenu a fait l'objet de nombreuses critiques. Certains contenus relevant du domaine artistique ont été supprimés de la plateforme et les comptes de leurs utilisateurs bloqués pour non-respect des conditions générales d'utilisation. C'est ainsi que le tableau

[1264] A. JOMNI, « Du discours de haine en ligne au cyberterrorisme : quelles régulations possibles ? », *Dalloz IP/IT* 2017, p. 563.
[1265] V. *infra* n° 516.
[1266] Standards de la communauté Facebook n° 14 : « *Nudité et activités sexuelles chez les adultes* », al. 1er. <https://www.facebook.com/communitystandards/objectionable_content> (dernière consultation le 9 octobre 2019).

L'origine du monde de Gustave Courbet représentant un sexe féminin[1267] mais également *La Vénus de Willendorf*, figurine considérée comme un chef-d'œuvre de l'art paléolithique[1268], ont été censurés par le réseau social Facebook. Par ailleurs, certains contenus présentant un intérêt historique ont également été supprimés du réseau social Facebook à l'image de la célèbre photographie de Nick Ut *La fillette au Napalm* présentant en son centre une fillette nue, partiellement brûlée, le visage tordu par la douleur[1269].

483. Face à ces critiques, le réseau social a cependant entrepris de modérer sa politique concernant la censure de la nudité en introduisant dans ces règles d'utilisation des tempéraments :

« *Avec le temps, nous avons adapté nos règlements relatifs à a nudité. Nous comprenons que les contenus montrant des scènes de nudité peuvent être partagés pour diverses raisons, notamment dans le cadre d'une protestation, pour sensibiliser à une cause, ou à des fins pédagogiques ou sanitaires. Par conséquent, nous acceptons les contenus respectant de tels motifs. Par exemple, alors que nous limitons certaines images de la poitrine féminine qui montrent le mamelon, nous autorisons d'autres types d'images, notamment celles illustrant des actes de protestation, des femmes défendant activement l'allaitement ou des cicatrices de mastectomie. Nous autorisons également les photos de peintures, sculptures et autres œuvres d'art illustrant des personnages nus* »[1270].

484. Suivant ces exceptions, Facebook a finalement accepté la conformité des trois précédents exemples (*L'origine du Monde*, *La Vénus de Willendorf*, *La fillette au Napalm*) à ses conditions générales. Si ces trois exemples montrent un infléchissement de la politique du réseau social ils ne démontrent pas pour autant un changement radical de sa politique. Par exemple, le tableau *Make America Great Again* de l'artiste Illma Gore représentant un dessin de Donald Trump avec un micro pénis fut censuré du réseau social Facebook après avoir été

[1267] P. SIGNORET, « Censure de "L'Origine du monde" : une faute de Facebook reconnue, mais pas sur le fond », *Le Monde*, 15 mars 2018. <https://www.lemonde.fr/pixels/article/2018/03/15/censure-de-l-origine-du-monde-une-faute-de-facebook-reconnue-mais-pas-sur-le-fond_5271666_4408996.html> (dernière consultation le 9 octobre 2019). V. également les décisions judiciaires concernant la présente affaire : Paris, 12 février 2016, n° 15/08624 : *D.* 2016, p. 422 ; *D.* 2016, p. 1045, obs. H. GAUDEMET-TALLON et F. JAULT-SESEKE ; *RTD Civ*., 2016, 310 obs. L. USUNIER ; *CCE*, 2016, Comm. 33, note G. LOISEAU.

[1268] « Facebook présente ses excuses après la censure d'une Vénus paléolithique », *Le Monde* avec *AFP*, 1er mars 2018.
<https://www.lemonde.fr/pixels/article/2018/03/01/une-venus-paleolithique-censuree-sur-facebook_5264174_4408996.html> (dernière consultation le 9 octobre 2019).

[1269] M. UNTERSINGER, « Après avoir censuré une photo de la guerre du Vietnam, Facebook fait machine arrière », *Le Monde*, 9 septembre 2016.
<https://www.lemonde.fr/pixels/article/2016/09/09/censure-le-plus-grand-journal-norvegien-attaque-facebook_4995029_4408996.html> (dernière consultation le 9 octobre 2019).

[1270] Standards de la communauté Facebook n° 14 : « *Nudité et activités sexuelles chez les adultes* », alinéa 2nd.

partagé plus de 50 millions de fois[1271]. Dans une autre affaire Facebook a supprimé la mise en ligne d'une photographie d'art de Laure Albin Guillot, représentant une femme à moitié dénudée. En l'occurrence, suite à la publication de la photographie sur la page Facebook du Musée du Jeu de Paume le réseau social avait pris l'initiative de désactiver le compte du musée en application des « *standards de la communauté Facebook* »[1272].

485. En tout état de cause, le critère du contenu manifestement illicite, fondement du pouvoir de modération des hébergeurs, est largement dépassé en pratique. Le simple caractère illicite de certains contenus censurés étant lui-même contestable. Les opérateurs des réseaux sociaux dépassent ainsi largement leurs obligations légales et s'arrogent le droit de censurer des contenus qui ne présentent pas manifestement un caractère illicite. Ce pouvoir de modération conféré aux réseaux sociaux est d'autant plus critiquable que les moyens de régulation qu'ils mettent en œuvre manquent de transparence.

B. Des moyens de régulation opaques

486. Des moyens techniques et humains. Les sites de réseaux sociaux communiquent très peu sur les moyens techniques et humains qu'ils mobilisent pour réguler les contenus qui transitent sur leurs plateformes se retranchant souvent derrière le secret industriel ou le secret des affaires. La question est toutefois de première importance dans la mesure où les contenus ainsi régulés ne transitent pas par la voie judiciaire classique mais sont directement modérés en ligne. En l'occurrence, les principales plateformes modèrent les contenus soit au moyen d'algorithmes de détection (1), soit par une main d'œuvre humaine (2). Dans les deux hypothèses, les méthodes utilisées manquent de transparence et de fiabilité sur le plan juridique.

1) Les limites de l'utilisation d'algorithmes dans la détection de contenus indésirables

487. L'essor des techniques de détection algorithmique des contenus illicites. La prise de connaissance par les opérateurs des réseaux sociaux des contenus enfreignant leurs conditions générales résulte soit de leurs utilisateurs par le biais des notifications de contenus,

[1271] « Un nu intégral de Donald Trump censuré aux USA est exposé à Londres », *AFP*, le 9 avril 2016. <https://culturebox.francetvinfo.fr/arts/peinture/un-nu-integral-de-donald-trump-censure-aux-usa-est-expose-a-londres-237753> (dernière consultation le 9 octobre 2019).
[1272] G. CHAMPEAU, « Musée du Jeu de Paume : Facebook assume la censure », *Numerama*, 6 mars 2013. <https://www.numerama.com/magazine/25307-musee-du-jeu-de-paume-facebook-assume-la-censure.html> (dernière consultation le 9 octobre 2019).

soit de systèmes automatisés chargés de détecter les contenus contraires à leurs standards[1273]. Or, les logiciels de détection automatique se sont beaucoup développés et affinés surtout concernant les contenus multimédias[1274]. Certaines plateformes de partage de vidéos ont mis en place à leur propre initiative des systèmes de marquage numérique de vidéos permettant d'identifier de façon automatisée des contenus illicites. Parmi ces logiciels, certains ont vocation à détecter la mise en ligne par un internaute d'une vidéo ou d'une chanson protégée par le droit d'auteur afin d'en bloquer la diffusion. Le meilleur exemple étant le logiciel *Content ID* utilisé par le site YouTube depuis 2007. Ce robot compare les vidéos postées chaque jour sur la plateforme de partage aux empreintes numériques de musiques ou films fournies par les ayants droit. YouTube dispose ainsi d'un partenariat avec 9 000 studios de cinéma et labels, qui lui offrent une base de données de plus de 80 millions d'œuvres[1275]. Lorsqu'une correspondance est décelée, une partie des revenus générés par la vidéo revient automatiquement aux auteurs de l'œuvre identifiée, qui peuvent aussi exiger le blocage du contenu[1276].

488. Les difficultés posées par les techniques de détection des contenus contrefaisants. Si l'utilisation de tels logiciels assure *a priori*, par le système de l'empreinte numérique, une détection neutre et objective d'une violation du droit d'auteur, cette méthode pose en réalité de nombreuses difficultés pratiques. Au sein de l'espace numérique les limites du système de détection automatique des contenus contrefaisant sont particulièrement mises en relief avec la problématique des œuvres transformatives[1277]. Cette notion pourrait se rapprocher en droit français de celle d'œuvre composite ou dérivée désignant « *l'œuvre nouvelle à laquelle est incorporée une œuvre préexistante sans la collaboration de l'auteur de cette dernière* »[1278]. Si cette pratique existe depuis des millénaires[1279], le numérique a démultiplié les possibilités des

[1273] Par exemple, dans ces conditions générales Facebook précise : « *nous développons des systèmes automatisés pour améliorer notre capacité à détecter et à supprimer les activités abusives et dangereuses qui pourraient porter atteinte à notre communauté et à l'intégrité de nos Produits* ».

[1274] Nous entendons ici les contenus basés sur de l'image, du son ou de la vidéo.

[1275] <https://siecledigital.fr/2018/11/12/les-auteurs-de-videos-sur-youtube-mieux-remuneres-depuis-content-id> (dernière consultation le 9 octobre 2019).

[1276] V. sur le sujet la vidéo de présentation de Content ID : <https://www.youtube.com/watch?time_continue=21&v=9g2U12SsRns> (dernière consultation le 9 octobre 2019).

[1277] V. sur le sujet : P. LEGER, *La recherche d'un statut de l'œuvre transformatrice. Contribution à l'étude de l'œuvre composite en droit d'auteur* (dir. P. SIRINELLI), LGDJ, 2018.

[1278] CPI, art. L. 113-2., alinéa 2.

[1279] Les exemples sont nombreux en la matière : du point de vue littéraire on pense à Montaigne connu pour ses nombreuses insertions de textes classique dans ses *Essais*, ou encore La Fontaine dont les fables sont largement inspirées d'Esope. Du point de vue musical, on peut préciser qu'au sein de son œuvre les *Contes d'Hoffmann* de 1881, Offenbach a repris des lignes mélodiques d'un autre opéra, celui de *Don Giovanni* de Mozart.

usages transformatifs[1280]. Les œuvres transformatives offrent une gamme particulièrement larges de potentialités créatrices allant « *de l'insignifiant au sublime* »[1281]. Il n'est d'ailleurs pas pertinent d'établir une liste des pratiques rencontrées sur le web tant elle est en continuelle évolution. Quelques exemples peuvent toutefois être cités tels que : les *mash-up*[1282], *remix*[1283], *prequel*[1284], *fanvid*[1285], *spin-off*[1286], *lip dub*[1287], *supercuts*[1288]. Si de telles pratiques reprennent ou s'inspirent d'œuvres préexistantes elles ne constituent pas pour autant une violation automatique du droit d'auteur, de nombreuses limites ou tempéraments étant portés à ce droit. C'est le cas lorsque l'œuvre composite ne fait que reprendre une petite partie de l'œuvre originale non représentative de sa globalité[1289]. De même, aucune violation du droit d'auteur ne peut être déduite lorsque la reprise de l'œuvre est indirecte, incidente ou fortuite au travers, par exemple, de simples éléments de décors[1290]. Enfin, selon l'exception de citation prévue au Code de propriété intellectuelle, l'auteur ne peut interdire « *les analyses et courtes citations justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées* »[1291]. Plus largement, les études préconisent

---

[1280] V.-L. BENABOU et F. LANGROGNET, *Rapport de la mission du CSPLA sur les « œuvres transformatives*, 24 décembre 2014, p. 7.

[1281] P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *CCE* n° 4, Avril 2016, étude 8.

[1282] « *Collage hétérogène d'œuvres différentes ou, inversement, forme de fusion de deux œuvres dans une troisième* ». P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit.*

[1283] Traitement nouveau d'une œuvre, le plus souvent musicale ou audiovisuelle. P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit.*

[1284] « *Œuvre dont l'histoire précède chronologiquement celle de l'œuvre préexistante* ». P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit.*

[1285] « *Vidéo de fan d'une œuvre préexistante en rapport avec cette œuvre* ». P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit.*

[1286] « *Œuvre reprenant un personnage de fiction d'une œuvre préexistante* ». P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit.*

[1287] « *Reconstitution créative d'une chanson, c'est-à-dire une œuvre audiovisuelle où une musique préexistante est parée d'une vidéo nouvelle* ». P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit.*

[1288] « *Assemblages de scènes de films similaires* ». P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit.*

[1289] CJUE, *Infopaq International A/S c./ Danske Dagblades Forening*, 16 juillet 2009, C-5/08, §45 *:* « *S'agissant des éléments de telles œuvres sur lesquels porte la protection, il convient de relever que celles-ci sont composées de mots qui, considérés isolément, ne sont pas en tant que tels une création intellectuelle de l'auteur qui les utilise. Ce n'est qu'à travers le choix, la disposition et la combinaison de ces mots qu'il est permis à l'auteur d'exprimer son esprit créateur de manière originale et d'aboutir à un résultat constituant une création intellectuelle* ». Cité *in* : E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, n° 221, p. 278.

[1290] Civ. 1ère., 12 mai 2011, n° 08-20.651 : *Bull. civ.* I n° 87. *Adde* : E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, n° 221, p. 278.

[1291] CPI, art. L. 122-5, 3, a).

l'adoption d'une exception au droit d'auteur spécifique en matière d'œuvre transformative[1292] certains y voyant « *une pratique sociale que le droit doit encourager* »[1293]. Cependant, loin des subtilités de ce débat juridique, les plateformes de partage ont tendance à supprimer de façon conservatoire les œuvres dites transformatives par volonté de préserver leur responsabilité. Un paradoxe peut alors être identifié : « *alors que les œuvres transformatives envahissent la toile […] elles peuvent aussi vite en ressortir, parfois sans préavis, sans explication, alors même qu'elles ne seraient pas nécessairement des contrefaçons, dans un mouvement de balancier parfois ressenti avec violence de part et d'autre. Une tension se crée sur la ligne de démarcation entre la possibilité de créer et diffuser une œuvre transformative et la contrefaçon supposée ou avérée d'une œuvre préexistante* »[1294]. En définitive, l'utilisation de logiciels de détection automatique de contenus contrefaisant n'emporte pas l'unanimité tant les résultats proposés par ces technologies sont encore loin de la finesse juridique qui anime le débat de la protection des droits d'auteurs sur les plateformes de partage. Le système de détection réalisé à partir d'un système d'empreintes numériques à l'image du logiciel *Content ID* sur YouTube ne permet ainsi pas d'en déduire une analyse juridique satisfaisante de la problématique du droit d'auteur tant les critères utilisés sont opaques.

489. Les limites des algorithmes de détection concernant les images de violences. L'efficacité des logiciels de détection automatique est également remise en cause concernant la diffusion d'images de violences sur les sites de réseaux sociaux. Sur ce point, la tuerie de Christchurch retransmise en direct sur le réseau social Facebook en est une sombre illustration. En l'occurrence, le réseau social a reconnu que la vidéo a été dupliquée plus de 1,5 millions de fois sur la plateforme d'échanges dans les 24 heures qui ont suivi l'attentat, et dans ce laps de temps, 300 000 copies auraient entièrement échappées aux outils de modération mis en place par le site Facebook[1295]. Cet exemple démontre qu'il semble impossible qu'un hébergeur puisse maîtriser le partage par ses utilisateurs d'un contenu jugé illicite et soumis à un filtrage. Nombre d'utilisateurs ont, par une simple modification de la durée, de la couleur ou du son de la vidéo, réussi à déjouer l'algorithme Facebook. Ainsi, le

[1292] V. par exemple : V.-L. BENABOU et F. LANGROGNET, *Rapport de la mission du CSPLA sur les « œuvres transformatives*, 24 décembre 2014.
[1293] C. MANARA, « Les créations transformatives », Juris art etc. n° 25/2015, p. 29.
[1294] P. HENAFF, « L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *op. cit*.
[1295] C. SONDERBY, « Update on NewZeland », *Facebook Newsroom*, 18 mars 2019.
<https://newsroom.fb.com/news/2019/03/update-on-new-zealand/> (dernière consultation le 9 octobre 2019).

système de marquage et de détection numérique des contenus audio ou vidéo présente de réelles limites dont la correction s'avère difficile d'un point de vue technique.

490. Les difficultés intrinsèques à la détection automatique des discours haineux. Partant du constat de l'efficacité limitée des algorithmes de détection pour les contenus multimédias (images, sons et vidéos), la modération des discours haineux s'avère alors être une entreprise encore plus délicate. Si théoriquement la détection et la modération des discours illicites par un algorithme est possible, l'opération de filtrage par mot clés qu'elle suggère présente toutefois des limites tenant à la subjectivité intrinsèque de l'expression[1296]. D'abord, le sens des mots clés recherchés est susceptible de changer selon le contexte mais également selon les époques[1297]. Ensuite, lorsque le terme est identifié, l'algorithme doit également être en mesure de distinguer si le propos défend un point de vue sanctionné ou si au contraire il le critique. Enfin, la faillibilité de ce système s'observe par la variabilité du contenu et des marqueurs lexicaux dans les pages illicites. Un mot neutre pouvant d'une part être récupéré et utilisé dans un contexte illicite et d'autre part, le phénomène linguistique de créativité lexicale rend également la tâche plus complexe[1298]. Ainsi, le filtrage de l'expression haineuse par des moyens automatisés s'avère être, en raison des difficultés d'interprétation propre à cette dernière, d'une complexité bien supérieure à celui des images ou vidéos dont l'analyse du caractère illicite est par nature plus objective.

La régulation des contenus sur les réseaux sociaux peuvent être également le fruit d'une prise de décision humaine, cette dernière n'est cependant pas gage d'une plus grande qualité et transparence.

[1296] V. R. VINOT, N. GRABAR, M. VALETTE, « Application d'algorithmes de classification automatique pour la détection des contenus racistes sur l'Internet », TALN 2003, Batz-sur-Mer, 11-14 juin 2003 ; v. également : M. VALETTE, « Sémantique interprétative appliquée à la détection automatique de documents racistes et xénophobes sur Internet », *in Approches sémantiques du Document Numérique*, Actes du 7ème colloque International sur le Document Electronique, 22-25 juin 2004, Patrice Enjalbert et Mauro Gaio, éd., 2004, pp. 215-230 ; v. également : M. VALETTE et N. GRABBAR, « Caractérisation de textes à contenu idéologique : statistique textuelle ou extraction se syntagme ? L'exemple du projet PRINCIP », Journées Internationales d'Analyse statistique des Données Textuelles (JADT), 2004, Louvain-la-Neuve, Belgique, UCL-Presses Universitaires de Louvain, 2004, pp. 1106-1116.

[1297] Par exemple le mot « *nègre* » dispose d'une signification radicalement différente en fonction des expressions utilisées : l' « *art nègre* », la « *tête de nègre* », le « *nègre* » d'un écrivain ou encore le « *nègre* » tel qu'il était couramment utilisé aux XVIIIème et XIXème siècles ne revêtent pas le même sens. V. R. VINOT, N. GRABAR, M. VALETTE, « Application d'algorithmes de classification automatique pour la détection des contenus racistes sur l'Internet », TALN 2003, Batz-sur-Mer, 11-14 juin 2003.

[1298] Par exemple : l'emploi du verlan (« *rebeu* », « *feujs* »), ou la modification, volontaire ou non, de l'orthographe (« naigre » au lieu de « *nègre* »). V. R. VINOT, N. GRABAR, M. VALETTE, « Application d'algorithmes de classification automatique pour la détection des contenus racistes sur l'Internet », TALN 2003, Batz-sur-Mer, 11-14 juin 2003.

2) Le sous traitement du pouvoir de modération à un personnel étranger

491. Une délégation des pouvoir de modération. Les principales plateformes de réseaux sociaux délèguent le plus souvent la tâche de modération à une main d'œuvre humaine. Ces modérateurs n'étant pas directement rémunérés par ces plateformes mais par des sociétés sous-traitantes basées pour la plupart en Asie, en particulier à Manille aux Philippines. Ceux qui sont désignés comme les « *nettoyeurs du web* »[1299] sont chargés d'inspecter les contenus qui leur sont signalés soit par les utilisateurs de ces plateformes soit par un logiciel de détection automatique. Lorsque l'image signalée s'affiche sur leurs écrans, les modérateurs ont le choix entre ignorer (« *ignor* ») ou supprimer (« *delete* ») les contenus qui leur sont soumis. Ils peuvent également classer ces contenus dans diverses catégories à savoir : la nudité (« *nudity* »)[1300], le spam, l'automutilation (« *Self Harm* »), le suicide, la pédopornographie (« *child abuse* »), le terrorisme (« *terrorism* »)[1301], ou encore dans la catégorie menace (« *Threat* »). Au-delà de l'application du critère de l'illicéité manifeste, il s'agit donc de s'assurer de la qualité de la décision prise au regard du temps consacré à la prise de décision[1302] et aux compétences juridiques des personnes investies du pouvoir de modération. En ce sens, nombre de contenus mériteraient une analyse détaillée avant une quelconque décision concernant leur diffusion notamment lorsqu'ils touchent au domaine artistique, historique, satirique ou encore journalistique. Or, la procédure de modération pratiquée par les principaux sites de réseaux sociaux permet de douter que la prise de décision s'effectue systématiquement dans un temps de réflexion suffisant et par une personne disposant des compétences juridiques adéquates.

En définitive, la modération des contenus opérée par les principaux sites de réseaux sociaux demeure dans une « *zone grise de censure privée* »[1303]. Il en résulte qu'un certain nombre d'infractions prévues par le Code pénal ne sont plus sanctionnées et même, pire

---

[1299] V. sur la question le documentaire : *Les Nettoyeurs du Web (The Cleaners)*, de Hans Block et Moritz Riesewieck, Allemagne, 2018, 86mn, diffusé le mardi 28 août 2018 sur Arte.

[1300] « *La plus grosse erreur que l'on puisse faire c'est de ne pas supprimer des photos de nus, celles qui montrent la poitrine d'une femme ou les parties génitales d'un homme ne doivent en aucun cas être conservées* ». Témoignage d'un modérateur recueilli dans *Les Nettoyeurs du Web (The Cleaners)*, de Hans Block et Moritz Riesewieck, Allemagne, 2018, 86mn, diffusé le mardi 28 août 2018 sur Arte.

[1301] « *Il y a une liste de 37 organisations terroristes que nous devons bannir de la plateforme. Nous devons les mémorisées ainsi que leurs emblèmes et leurs slogans* ». Témoignage d'un modérateur recueilli dans *Les Nettoyeurs du Web (The Cleaners)*, de Hans Block et Moritz Riesewieck, Allemagne, 2018, 86mn, diffusé le mardi 28 août 2018 sur Arte.

[1302] Les nettoyeurs du web pouvant analyser jusque 25 000 contenus par jour. V. *Les Nettoyeurs du Web (The Cleaners)*, de Hans Block et Moritz Riesewieck, Allemagne, 2018, 86mn, diffusé le mardi 28 août 2018 sur Arte.

[1303] F. DUBUISSON, « Les restrictions à l'accès au contenu d'internet et le droit à la liberté d'expression », *in* : *Internet et le droit international*, société française pour le droit international, colloque de Rouen, Éd. A. Pedone, p. 141.

encore, plus poursuivies. Ce manque d'effectivité du régime de responsabilité propre aux hébergeurs mis en œuvre par la LCEN favorise alors la mise en place d'une régulation globale de l'expression selon les règles édictées dans les conditions générales des sites de réseaux sociaux qui ne coïncident pas systématiquement avec les exigences posées par la loi.

§2. Une régulation privée des contenus en conflit avec certains standards juridiques européens

492. L'expression sur les réseaux sociaux, point de friction entre l'idéologie libertarienne et les standards européens. Les grandes plateformes de réseaux sociaux, principalement basées dans la région de San Francisco et la Silicon Valley, véhiculent une conception de la vie en société qui s'exporte dans tous les grands centres urbains si bien que selon la sociologue Monique Dagnaud : « *aucune société avancée ne saurait échapper à la force transformatrice de l'utopie californienne* »[1304]. Plus précisément, les principaux réseaux sociaux basent leur modèle sur l'idéologie libertarienne. Cette dernière revêt une importance majeure dans la mesure où elle guide la politique de modération exercée par les opérateurs de réseaux sociaux (A). Cependant, au vu du système de régulation privée des contenus, la doctrine libertarienne portée par les réseaux sociaux est en position de concurrencer, voire d'affaiblir certains standards européens tel que le principe de liberté d'expression (B).

A. La consécration par les réseaux sociaux de l'idéologie libertarienne

493. Les fondements de l'idéologie libertarienne. Dans un premier temps, le modèle libertarien trouve ses sources aux origines des États-Unis et notamment dans la forme d'esprit antiétatique qui animait ses pères fondateurs[1305]. Plus précisément, cette défiance de l'État se retrouve à travers les doctrines du libéralisme classique[1306] et de l'anarchisme

[1304] M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, Odile Jacob, 2016, p. 13.
[1305] V. É. MARIENSTRAS, *Les mythes fondateurs de la nation américaine. Essai sur le discours idéologique aux États- Unis à l'époque de l'indépendance (1763-1800)*, Paris, François Maspero, 1976, p. 48 ; v. également l'étude de J. APPLEBY, « Liberalism and the American Revolution », *The New England Quarterly*, Vol. 49, n° 1, Mars, 1976, pp. 3-26.
[1306] Cette doctrine portée par Thomas Jefferson selon laquelle, l'individu est constitué de droits inaliénables. Les principaux sont la vie, l'égalité naturelle, l'autogouvernement et la libre quête du bonheur. Pour ce faire, les libéraux prônent une intervention réduite de l'État limitée à sa seule sphère régalienne. V. T. JEFFERSON, *On Democracy*, éd. Saul K. Padover, New York, Penguin Books, 1946 ; J. APPLEBY, T. BALL, *Thomas Jefferson. Political Writings*, New York, Cambridge University Press, 1999 ; D. BERGERON, « Thomas Jefferson et la réflexion sur l'Autochtone. Conception d'une nature au fondement d'un projet humain », *Revue française de science politique*, vol. 67, n° 3, 2017, pp. 497-519.

individualiste[1307]. Le libertarisme regroupe justement ces différentes théories dans un système théorique cohérent qui associe la défense des libertés économiques, des libertés individuelles et condamne l'impérialisme[1308]. Ainsi, le discours libertarien classique dresse la liberté et les droits individuels en pivot essentiels de la vie en société mais aussi de l'activité politique et économique[1309]. Cette idéologie se retrouve notamment en filigrane dans la déclaration d'indépendance américaine de 1776, mais aussi dans la Constitution des États-Unis de 1787 qui sont perçus comme les textes de référence absolue en la matière[1310]. Particulièrement le premier amendement de la constitution américaine qui pose le droit du « *freedom of speech* » assurant une liberté d'expression totale[1311].

494. Dans un second temps l'idéologie libertarienne a trouvé un nouvel essor dans la Californie des années 1960 à l'aube de la révolution technologique. La sociologue Monique Dagnaud[1312] impute ce nouvel élan à la jeunesse californienne et à deux types d'acteurs en particuliers. D'un côté, les hackeurs décrits comme de « *jeunes bidouilleurs qui s'agitent dans les couloirs des universités* »[1313] utilisant de manière plus ou moins clandestine les premières versions d'ordinateurs[1314]. De l'autre, la contre-culture californienne des années 1960-1970 et notamment le mouvement hippie qui a grandement influencé à travers son imaginaire la construction d'internet notamment dans son mode de vie en communauté comparable aux prémices du réseau internet[1315]. Cependant, alors qu'à partir des années 1970 les communautés hippies vont progressivement se disloquer, une élite « *indépendante et*

[1307] Il s'agit d'un courant de l'anarchisme qui défend la liberté des choix individuels face à ceux imposés par un groupe social. Les anarchistes individualistes américains préconisent la libre circulation et s'opposent aux révolutions violentes. Par exemple Benjamin Tucker défend le droit à la création de coopératives indépendantes fonctionnant sur le système du libre-échange, le refus de payer l'impôt ainsi que la mise en place d'un système bancaire affranchi de l'emprise étatique. Dans ce même courant d'idée, Lysander Spooner défendait pour sa part la justice naturelle. Selon lui, les actes de coercition à l'encontre des individus et de leurs propriétés sont illégaux. Il condamne en conséquence tout positivisme juridique, au profit des droits naturels de l'individu. Enfin, d'autres philosophes appartenant à ce mouvement ont quant à eux expérimentés la vie en autarcie comme Henri David Thoreau. V. H. D. THOREAU, *Walden; or, Life in the Woods*, Ticknor and Fields, 1854 ; plus généralement : v. V. BASCH, *L'individualisme anarchiste*, Paris, 1904, F. Alcan, réédition en 1928 et en 2008.

[1308] S. CARE, « Racines théoriques du libertarianisme américain », *Cités*, vol. 46, n° 2, 2011, p. 133.

[1309] M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, Odile Jacob, 2016, p. 9.

[1310] O. ITEANU, *Quand le digital défie l'État de droit*, Eyrolles, 2016, p. 26.

[1311] V. *infra* n° 500.

[1312] M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, *op. cit.*, p. 32 et suiv.

[1313] *Ibid*.

[1314] Pour une analyse complète du mode de vie et de l'éthique des Hackers V. : S. LEVY, *Hackers : Heroes of the Computer Revolution*, New York, Delta, 1984 ; P. HIMANEN, *L'Éthique hacker et l'Esprit de l'ère de l'information*, Saint-Élie-de-Caxton (Québec), Exils, 2001.

[1315] V. F. TURNER, *Aux sources de l'utopie numérique. De la contre-culture à la cyberculture, Stewart Brand, un homme d'influence*, Caen, éd. C. & F., 2012.

créative »[1316] émerge de cette forme de vie en société et pose les bases idéologiques de la révolution technologique[1317].

495. Le contenu de l'idéologie classique libertarienne. Selon l'idéologie classique libertarienne, il existe un fossé entre « *l'homme potentiellement libre et l'individu réellement libéré de toutes ses chaînes, autrement dit entre une liberté négative formelle et une liberté positive substantielle* »[1318]. Les libertariens se placent en opposition par rapport aux autres philosophies politiques qui voient dans ces intervalles l'espace d'une intervention étatique légitime alors que les libertariens y décèlent une occasion offerte à l'individu d'accomplir par lui-même ses aspirations[1319]. Le mouvement libertarien revendique en conséquence une limitation extrême des pouvoirs et des fonctions de l'État central au nom de la liberté. Cependant, la liberté revendiquée par les libertariens est protéiforme et reflète des aspects bien divers. Les libertariens sont dans un premier temps *jusnaturalistes* : ils prônent une liberté individuelle totale et pour ce faire, défendent les droits naturels[1320] des individus. Selon ces derniers, seuls les droits qui préexistaient avant la formation de l'État sont légitimes à recouvrir une force obligatoire. Dès lors le droit positif doit correspondre peu ou prou aux droits naturels des individus sans que l'État n'intervienne au-delà[1321]. Ces droits font partie de l'essence de la déclaration des droits de l'homme et du citoyen de 1789 et sont explicitement mentionnés à son article 2 comme : « *la liberté, la propriété, la sûreté, et la résistance à l'oppression* »[1322]. Mais cette liberté de l'individu n'est pas la seule revendiquée par le courant libertarien qui milite également pour une entière liberté économique souhaitant projeter la logique du marché dans tous les domaines de la société. Le libéralisme économique constitue dans un second temps l'autre point essentiel de l'idéologie libertarienne, l'État devant s'abstraire de tout interventionnisme en la matière de manière à favoriser le libre

[1316] M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, *op. cit.*, p. 36.
[1317] Un des exemples les plus connus est celui du catalogue américain de contre-culture : le *Whole Earth Catalog* publié par Steward Brand entre 1968 et 1972. Il s'agit d'un catalogue proposant toutes sortes de produits à la vente souvent associés à la contre-culture et au mouvement hippie. On y trouve par exemple des livres, des engins mécaniques, des kits variés utiles pour un style de vie créatif et autosuffisant, du matériel pour vivre dans la nature, des tenues hippies. Les lecteurs pouvant eux-mêmes commenter les produits et en conseiller d'autres. Un autre exemple se trouve dans le magazine *Wired* lancé en 1993 et s'inscrivant ouvertement dans l'idéologie libertarienne, c'est d'ailleurs Kevin Kelly, ancien rédacteur en chef du *Whole Earth Catalog* qui devient son directeur de publication. V. M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, Odile Jacob, 2016, p. 38.
[1318] S. CARE, « Racines théoriques du libertarianisme américain », *Cités*, vol. 46, n° 2, 2011, p. 138.
[1319] *Ibid*.
[1320] Juridiquement le droit naturel est une « *règle considérée comme conforme à la nature (de l'homme ou des choses) et à ce titre reconnue comme de droit idéal* », Association H. CAPITANT, *Vocabulaire juridique*, G. CORNU (dir.), PUF, 12ème éd., 2018, *V°* Naturel.
[1321] J. RIVERO et H. MOUTOUH, *Liberté publiques*, Tome 1, 9ème éd., 2003, Thémis Droit public, p. 30, n° 46.
[1322] Art. 2, DDHC : « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression* ».

marché. Le libéralisme économique doit dans cette hypothèse être compris comme une nouvelle raison gouvernementale : le marché incarnerait un lieu de formation de la vérité justifiant une autorégulation totale et indépendante[1323].

496. Par ailleurs, l'intensité de l'exercice de ces libertés varie également en fonction des différents courants du libertarianisme. Monsieur Sébastien Caré distingue ainsi « *la variété des horizons d'attentes auxquels les libertariens destinent la société* »[1324]. La forme la plus extrême de cette doctrine est l'utopie anarcho-capitaliste préconisant un système de propriété privée intégrale même pour ce qui relève des pouvoirs régaliens de l'État. Cette doctrine propose de soumettre l'ensemble des domaines de la vie en société au marché y compris la police, les tribunaux, les prisons et la défense nationale[1325]. Moins extrême, l'utopie minarchiste ne reconnaît à l'État qu'une fonction régalienne consistant à assurer la sécurité des individus contre les crimes et les attaques extérieures[1326]. Enfin, une dernière tranche de la doctrine libertarienne reconnaît à l'État de nombreuses fonctions concernant le maintien de l'ordre public mais également la distribution de biens et de services collectifs qui ne pourraient pas être assurés par le marché[1327].

497. L'idéologie libertarienne appliquée à internet. Les libertariens voient la technique et la technologie d'internet comme les gardiens de la liberté totale qu'ils revendiquent. Ils considèrent qu'un réseau ouvert et décentralisé serait libérateur pour la société. Une telle forme de réseau serait également susceptible de s'autoréguler en étant laissé à lui-même. En conséquence, toute ingérence extérieure, en particulier celle de l'État, est considérée comme illégitime[1328]. La déclaration d'indépendance du cyberespace en date du 8 février 1996 fait figure de texte de référence en la matière[1329]. En reprenant le ton de la Déclaration d'indépendance des États-Unis, son rédacteur John P. Barlow affirme la soustraction du cyberspace à l'autorité des États : « *Gouvernements du monde industriel, géants fatigués de chair et d'acier, je viens du cyberespace, nouvelle demeure de l'esprit. Au nom de l'avenir, je*

[1323] B. LOVELUCK, « Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux*, vol. 192, n° 4, 2015, p. 244.
[1324] S. CARE, « Racines théoriques du libertarianisme américain », *Cités*, vol. 46, n° 2, 2011, p. 137.
[1325] V. par exemple : D. FRIEDMAN, *Vers une société sans État*, Paris, Les Belles Lettres, 1992, 2ème éd. (1ère éd. 1973).
[1326] V. par exemple : R. NOZICK, *Anarchie, État et utopie*, Paris, PUF, 1974.
[1327] V. par exemple : F. Hayek, *La route de la servitude*, Paris, PUF, coll. « Quadrige », 2010.
[1328] B. LOVELUCK, « Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux*, vol. 192, n° 4, 2015, p. 249.
[1329] J. P. BARLOW, « Déclaration d'indépendance du cyberespace », *in* O. BLONDEAU, *Libres enfants du savoir numérique. Une anthologie du "Libre"*. Editions de l'Éclat, 2000, p. 51. Ce texte fut rédigé en marge du sommet de Davos et en réaction au *Communications Decency Act* (CDA) qui proposait la création de mesures de censure contre les contenus obscènes et violents jugées inadaptées et liberticides.

vous demande, à vous qui êtes du passé, de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez aucun droit de souveraineté sur nos lieux de rencontre »[1330].

498. De l'idéologie libertarienne à l'idéologie de la *Silicon Valley*. L'économie collaborative est devenue le vecteur essentiel de la doctrine libertarienne. Sur internet, ce modèle idéologique repose sur trois piliers fondamentaux : une autonomie des individus sublimée par la technologie ; une liberté de circulation sans limites des flux d'informations ; un partage désintéressé des contenus dans le but de favoriser la diffusion de la culture et de l'information[1331]. L'économie du partage, le système du *peer-to-peer*, sont dans l'espace numérique les modèles de référence de cette idéologie[1332]. Selon la sociologue Monique Dagnaud, « *Les valeurs de la contre-culture, progressivement, se sont fondues dans la pensée du* new age, *démarche tout à fait compatible avec celles des entreprises postindustrielles et, d'ailleurs, généreusement accueillie par elles* »[1333]. Le système de l'économie collaborative trouve son point d'ancrage dans le modèle développé par les sites de réseaux sociaux et plus généralement dans le groupe des « *entreprises de la Silicon Valley* » identifié par Monsieur Olivier Iteanu[1334]. Ces grandes entreprises partagent avec les libertariens leur défiance vis-à-vis des États, cependant, à la différence de ces derniers, elles défendent davantage le principe du marché total que celui de la liberté totale[1335]. L'idéal de la doctrine libertarienne se dissout en conséquence dans la politique économique de ces plateformes. L'idéologie libertarienne se mue progressivement en idéologie de la *Silicon Valley* où la liberté économique supplante les libertés individuelles. Ce nouveau rapport de force conduisant inexorablement à un affaiblissement des standards juridiques européens.

B. L'affaiblissement de la notion européenne du droit à la liberté d'expression

499. Les fondements idéologiques libertariens se retrouvent par essence dans la doctrine du *freedom of speech*, cependant, par l'effet du numérique, le concept du *freedom of speech* se

[1330] J. P. BARLOW, « Déclaration d'indépendance du cyberespace », *op. cit.*, p. 51.
[1331] M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, *op. cit.*, p. 9.
[1332] O. ITEANU, *Quand le digital défie l'État de droit*, Eyrolles, 2016, p. 25.
[1333] M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, *op. cit.*, p. 41.
[1334] Selon Monsieur Olivier Iteanu ces entreprises constituent un groupe et une idéologie à part entière qui se distingue de celle des libertariens classiques. Il précise également que la dénomination « *entreprise de la Silicon Valley* » regroupe en réalité des entreprises localisées ailleurs telles que Uber ou Airbnb. V. O. ITEANU, *Quand le digital défie l'État de droit*, *op. cit.*, p. 26.
[1335] V. A. SUPIOT, *La gouvernance par les nombres*, Fayard, 2015, p. 22.

substitue au concept européen de liberté d'expression alors même qu'il s'agit de deux doctrines bien différentes.

500. Concept américain du *freedom of speech*. En droit américain le *freedom of speech* revêt un caractère absolu ce qui insinue qu'aucune entrave d'ordre économique, politique ou sociétale ne doit aller à son encontre. Ce principe est consacré avec force et symbolisme au premier amendement de la constitution américaine démontrant ainsi le degré d'implantation de la doctrine libertarienne dans la culture juridique américaine. Le droit au *freedom of speech* défend en effet une intervention minimaliste de l'État concernant la liberté de parole, la liberté religieuse ou encore la liberté d'association. Le législateur américain ne peut donc apporter aucune limite aux abus de la liberté d'expression. Le premier amendement apparaît rédigé comme suit :

« *Le Congrès ne fera aucune loi qui touche l'établissement ou interdise le libre exercice d'une religion, ni qui restreigne la liberté de la parole ou de la presse, ou le droit qu'a le peuple de s'assembler paisiblement et d'adresser des pétitions au gouvernement pour la réparation des torts dont il a à se plaindre* »[1336].

501. Concept européen de la liberté d'expression. À l'inverse, la liberté d'expression, dans sa conception européenne, n'est pas une liberté absolue, il s'agit au contraire d'une liberté encadrée. L'article 10 de la Convention EDH précise dans la même logique que l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789[1337] que même si la liberté d'expression est un droit fondamental, ce dernier n'est toutefois pas absolu, certains abus de la liberté d'expression pouvant être sanctionnés par la loi :

« *Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.*

L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratiques, à la sécurité nationale,

[1336] Constitution DES États-Unis du 17 septembre 1787, 1er Amendement.
[1337] Déclaration des Droits de l'Homme et du Citoyen de 1789, art 11 : « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi* ».

à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire »[1338].

502. Jurisprudence de la Cour EDH. Le juge européen opère une démarche casuistique dans son contrôle du respect du principe de liberté d'expression. Ce dernier s'intéresse aux circonstances dans lesquelles les propos ont été tenus et s'attache à ce titre à plusieurs variables : les interlocuteurs en présence, le but poursuivi par l'auteur du propos, le support utilisé et les répercussions potentielles des propos litigieux[1339]. De manière générale, les propos qualifiés de discours haineux sont reconnus comme constituant des abus de droit au regard de l'article 17 de la Convention EDH. Dans cette hypothèse le propos constitue un abus de la liberté d'expression sanctionné par le juge européen[1340]. La Cour EDH identifie une série de discours comme constituant des formes d'abus de la liberté d'expression à l'instar des propos racistes, antisémites, xénophobes, mais aussi toute forme de haine fondée sur l'intolérance, y compris celles qui s'expriment sous la forme d'un nationalisme agressif[1341].

503. Justification de la doctrine européenne. Selon la base du système de pensée européen, l'homme exerce sa liberté d'opinion à trois niveaux : en premier lieu il pense, puis il s'exprime, enfin il agit. En conséquence, l'expression est le préalable de l'action, c'est pourquoi elle doit être protégée mais également encadrée pour prévenir toute forme d'action violente. Partant de ce constat Monsieur Olivier Iteanu relève que : « *le fait d'exprimer, à l'oral comme à l'écrit, une pensée qui porte atteinte à autrui, surtout en public, à raison de la race, de la religion, de l'orientation sexuelle, notamment, ou qui rapporte des faits portant atteinte à l'honneur d'un tiers, peut logiquement dégénérer demain en un acte portant atteinte à l'intégrité physique de la ou des personnes désignées, par l'auteur de la parole ou de l'écrit ou même par un de ses auditeurs ou lecteurs* »[1342]. La vague d'attentats perpétrés en France en 2015 ont permis de soulever le rôle joué par les réseaux sociaux dans la diffusion des discours

[1338] Conv. EDH, Art. 10.
[1339] M. AFROUKH, « La liberté d'expression face aux discours haineux en ligne dans la jurisprudence de la Cour européenne des droits de l'homme », *Dalloz IP/IT* 2017, p. 575.
[1340] V. par exemple : CEDH, *M'Bala M'Bala c/ France (aff. Dieudonné)*, 20 octobre 2015, n° 25239/13 – CEDH, *Garaudy c/ France*, 24 juin 2003, n° 65831/01 – CEDH, *Ivanov c/ Russie*, 20 février 2007, n° 35222/04 – CEDH, *Norwood c/ Royaume-Uni*, 16 novembre 2004, n° 23131/03. *Adde :* M. AFROUKH, « La liberté d'expression face aux discours haineux en ligne dans la jurisprudence de la Cour européenne des droits de l'homme », *Dalloz IP/IT* 2017 p. 575.
[1341] C. DENIZEAU, « L'Europe face au(x) discours de haine », *Revue générale du droit on line*, 2015, n° 21669. *Adde* : A. JOMNI, « Du discours de haine en ligne au cyberterrorisme : quelles régulations possibles ? », *Dalloz IP/IT* 2017, p. 563.
[1342] O. ITEANU, *Quand le digital défie l'État de droit*, *op. cit.*, p. 33-34.

de haine et l'endoctrinement du jeune public. Dès lors, l'encadrement de l'expression publique a pour but de prévenir l'acte raciste et la violence jusque dans ses formes le plus extrêmes. Au final un tel encadrement joue un rôle pacificateur essentiel au sein de la société[1343]. C'est pourquoi, dans ce contexte numérique, la conception européenne de la liberté d'expression apparaît en réalité comme le plus responsable et le plus abouti de notre temps. À l'opposé, la doctrine du *freedom of speech* paraît moins en phase avec le monde digital actuel, ce principe serait même aujourd'hui « *totalement dépassé* »[1344]. Cependant, c'est bien la conception américaine du *freedom of speech* qui semble prendre le dessus sur le concept européen de liberté d'expression.

504. Application du concept du *freedom of speech* en lieu et place de la liberté d'expression. Le point de confrontation entre l'Europe et les États-Unis sur cette divergence de conception de la liberté d'expression se trouve au niveau du traitement des paroles de haine appelées également *hate speech*. En la matière, la souplesse observée dans la modération des discours[1345] démontre que les réseaux sociaux appliquent, y compris à l'égard du public européen la doctrine du *freedom of speech* mettant en péril la conception européenne de la liberté d'expression[1346]. Les affaires Yahoo![1347] ou Twitter[1348] mettent en exergue les

[1343] L'historien Jules Isaac a notamment démontré comment « *l'enseignement du mépris* » qui s'était installé depuis des siècles dans le débat public européen avait mené progressivement à la Shoah durant la décennie 1940. V. J. ISAAC, *Genèse de l'antisémitisme, essai historique,* Calmann-Levy, 1956. Cité *in* : O. ITEANU, *Quand le digital défie l'État de droit*, Eyrolles, 2016, p. 34.

[1344] O. ITEANU, *Quand le digital défie l'État de droit*, *op. cit.*, p. 60.

[1345] V. s*upra* n° 480.

[1346] Un exemple illustre parfaitement cet état de fait : à la suite d'une émission de France culture consacrée au mariage pour tous certains propos ont été publiés sur la page Facebook d'un des intervenants de l'émission, en l'occurrence Louis-Georges Tin militant des droits des homosexuels et membre du Conseil représentatif des associations noires de France (CRAN). Les propos étaient de la teneur suivante : « *Pauvre merde à la con !!! Tu mérites une grande dose de Zyklon B sale porc !!!* ». Après signalement du contenu par un membre de l'émission au réseau social, Facebook a renvoyé cette réponse : « *Nous vous remercions pour votre rapport. Nous avons soigneusement examiné la publication que vous nous avez signalée. Mais nous avons conclu qu'elle n'enfreint pas le standard de la communauté "discours incitant à la haine". Nous ne l'avons donc pas retiré* ». Propos recueillis dans l'émission : *Peut-on réguler les réseaux sociaux ?*, Émission *Du Grain à Moudre*, France culture, présentée par Hervé Garedette, 7 février 2013.

[1347] En l'espèce, le site Yahoo ! proposait sur ces pages de ventes aux enchères en ligne des objets nazis, de la littérature antisémite et la vente de Zyklon B. Or, des associations antiracistes reprochaient que ces ventes aux enchères soient notamment orientées vers le public européen. Au prix d'une longue bataille judiciaire, le juge français a finalement fait injonction à la société américaine de « *prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de vente aux enchères d'objets nazis et de tout autre site ou service qui constitue une apologie du nazisme ou une contestation des crimes nazis* ». V. TGI Paris, ordonnance de référé, 22 mai 2000, UEJF et Licra c/ Yahoo ! Inc. Et Yahoo§ France – TGI Paris, ordonnance de référé, 20 novembre 2000, UEJF et Licra c/ Yahoo ! Inc. Et Yahoo§ France.

[1348] En l'espèce, le site Twitter véhiculait des discours de haine notamment par les hashtags : *#unbonjuif #unjuifmort*. La plateforme a procédé au retrait des tweet antisémites mais a refusé de communiquer l'identité des auteurs malgré l'ordonne du TGI de Paris lui enjoignant de le faire. V. TGI Paris, ordonnance des référés, UEJF et autres c/ Twitter Inc. et Twitter France, 24 janvier 2013. Ce refus de se soumettre à la décision du juge français a été vivement critiqué par le juge du second degré qui releva notamment que Twitter ne justifiait pas « *d'une impossibilité d'exécuter celle*-ci ». V. Paris, Pôle 1, Chambre 5, ordonnance du 12 juin 2013,

difficultés du droit européen à s'appliquer face aux standards de ces grandes entreprises souvent basés sur les règles de droit américain. La problématique est la suivante : le droit au *freedom of speech* américain tolère les discours de haine alors que le concept européen de liberté d'expression les poursuit devant les tribunaux. Il n'est dans ce cas pas question de contester l'application du droit constitutionnel américain aux États-Unis mais d'exiger que cette approche de la liberté d'expression ne s'exporte pas au territoire de l'Union-Européenne par le biais des grandes plateformes numériques américaines[1349].

505. Conclusion de la Section 2. La souveraineté des opérateurs des réseaux sociaux dans la régulation des contenus qui y transitent amène à de vives critiques. D'une part, les principaux acteurs s'affranchissent des exigences développées dans la LCEN en particulier celle de son article 6 subordonnant leur responsabilité au retrait des contenus manifestement illicites. C'est ainsi que certains contenus se voient censurés par ces sites alors qu'ils revêtent un intérêt sur le plan artistique ou du droit à l'information. D'autre part, les opérateurs des réseaux sociaux, en tant que juges du respect de leurs propres conditions générales, démontrent une inertie fautive dans la modération de certains contenus contrevenant à leurs propres conditions générales et pouvant revêtir en sus un caractère manifestement illicite, c'est le cas des discours haineux. Cette politique de modération est inspirée de l'idéologie libertarienne qui a accompagné l'émergence et le développement d'internet. Cependant, les grandes entreprises de la *Silicon Valley* se sont réappropriées cette idéologie et l'ont transformée peu à peu. Au final, alors que l'idéologie libertarienne classique prône sur un pied d'égalité les libertés économiques et les libertés individuelles, l'idéologie de la *Silicon Valley* supplante les libertés individuelles au profit des libertés économiques. Si la doctrine du *freedom of speech* apparaît en premier lieu comme un droit individuel, elle est aujourd'hui utilisée dans le but de préserver le modèle économique des sites de réseaux sociaux et de justifier la défiance envers le principe européen de liberté d'expression. Ce constat condensé dans l'expression « *Buisness is law* »[1350] est également résumé par la sociologue Monique Dagnaud selon laquelle : « *En réalité, dès que la révolution Internet s'est éloignée des utopies originelles, dès qu'elle est sortie du ruisseau pour gonfler un fleuve prêt à tout balayer sur son passage, dès que les logiques capitalistes et commerciales l'ont innervée, […] dès qu'elle a cessé de concerner un petit monde d'initiés arrimés à une cause généreuse, elle a été*

UEJF c/ Twitter. L'identité des auteurs de ces hashtags fut finalement livrée par Twitter mais de manière informelle et au prix d'une longue procédure judiciaire.

[1349] V. dans ce sens : O. ITEANU, *Quand le digital défie l'État de droit*, Eyrolles, 2016, p. 35.

[1350] O. ITEANU, *Quand le digital défie l'État de droit*, *op cit.*, p. 148.

attaquée vigoureusement. […] *Au final, un débat s'est enflammé et n'a jamais cessé de brûler* »[1351].

[1351] M. DAGNAUD, *Le modèle californien. Comment l'esprit collaboratif change le monde*, Odile Jacob, 2016, p. 45.

Conclusion du Chapitre 1

506. Les opérateurs des réseaux sociaux disposent en leur qualité d'hébergeurs de la capacité, suite à un signalement ou à une notification d'un contenu, de modérer une information pouvant relever d'une qualification pénale. En l'occurrence la LCEN donne pouvoir aux opérateurs de régulation des contenus qui leur sont notifiés lorsque ceux-ci revêtent un caractère manifestement illicite. Ce critère correspond en réalité à une liste limitative d'infractions appartenant à la catégorie des contenus « *odieux* » ou « *sensibles* » pour lesquelles les opérateurs se doivent d'agir promptement sous peine d'engager leur responsabilité pénale. Toutefois, le critère de contenu manifestement illicite, censé apporter une objectivité satisfaisante dans le pouvoir de modération des opérateurs concerne des infractions dont la qualification juridique relève parfois d'un travail d'interprétation délicat établissant la limite entre les discours pénalement sanctionnés et la simple opinion dérangeante protégée par le principe de liberté d'expression. Dès lors, une modération systématique des contenus notifiés aboutirait au risque de supprimer des contenus s'avérant en réalité parfaitement licites. Cependant, loin de pratiquer une suppression conservatoire des contenus leur étant notifiés, les opérateurs des réseaux sociaux réalisent une régulation selon leurs propres conditions générales d'utilisation. Ce pouvoir de police privée des contenus revient cependant dans certains cas à méconnaître les contours de l'ordre public à l'échelle numérique, particulièrement concernant les limites posées en droit français et européen au principe de liberté d'expression. La solution serait alors de renforcer le pouvoir et la capacité de contrôle de l'autorité publique au sein de ce système de régulation de manière à réaffirmer l'État de droit et les libertés individuelles qu'il défend. Allant dans ce sens, Monsieur Emmanuel Netter constate que « *seuls des propos dont l'illégalité crève les yeux peuvent faire l'objet d'une forme de censure privée* », dès lors qu'il y a une hésitation, même infime, « *il ne peut être question d'en exiger ni même d'en admettre le retrait par quelques salariés d'une compagnie américaine. C'est au juge, doté de moyens suffisants par l'État, qu'il appartient de procéder à ces arbitrages vitaux dans une société démocratique* »[1352].

[1352] E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, n° 163, p. 196.

Chapitre 2 – Les enjeux du nouvel encadrement des opérateurs des réseaux sociaux

507. Rétablissement d'une coercition à l'égard des réseaux sociaux. Le régime de responsabilité des hébergeurs attribué aux sites de réseaux sociaux démontre son inadaptation aux problématiques soulevées par ces nouveaux acteurs. L'actuel pouvoir de régulation des contenus conféré aux prestataires techniques aboutit à un affaiblissement de certains principes fondamentaux défendus à l'échelle française et européenne, particulièrement l'application du principe de liberté d'expression. Ce mouvement est favorisé par le manque de fermeté du régime de responsabilité actuel appliqué aux opérateurs des réseaux sociaux qui organise un quasi régime d'irresponsabilité notamment en raison de la faible capacité coercitive de l'autorité judiciaire provenant de son manque de pouvoir sanctionnateur en la matière. Il s'agit alors de redéfinir le cadre juridique applicable aux opérateurs des réseaux sociaux et précisément d'adopter un régime de responsabilité *sui generis* adapté à cette catégorie particulière et singulière d'acteurs impliquant des obligations renforcées susceptibles d'aboutir sur des sanctions dissuasives. En l'occurrence, plusieurs types d'acteurs doivent jouer un rôle déterminant dans l'encadrement des sites de réseaux sociaux et assurer par là même une réelle effectivité de ce nouveau régime de responsabilité. En premier lieu, la présence d'une autorité de contrôle, collaborant avec l'autorité judiciaire, est destinée à instaurer une relation verticale avec les réseaux sociaux par son pouvoir de contrôle et de sanction à leur égard. En second lieu, le bon respect des obligations et la régulation satisfaisante des contenus est également dépendante de la collaboration de l'ensemble des acteurs des réseaux sociaux à savoir leurs utilisateurs et leurs opérateurs. Ce rapport davantage horizontal dans la régulation des contenus est un complément nécessaire à la verticalité instaurée par la présence d'une autorité de contrôle.

Un meilleur encadrement des sites de réseaux sociaux passe en l'occurrence par l'adoption d'un régime de responsabilité renforcé à l'égard de leurs opérateurs (**Section 1**) induisant l'identification de nouveaux acteurs en charge de cet encadrement (**Section 2**).

Section 1 : L'adoption d'un régime de responsabilité renforcé à l'égard des opérateurs des réseaux sociaux

508. Une responsabilisation par la création d'un nouveau statut juridique. Le régime juridique des hébergeurs affecté aux opérateurs des réseaux sociaux ne permet pas d'obtenir des résultats satisfaisants concernant la régulation des contenus publiés sur ces sites. D'une part, il introduit un système de responsabilité favorable car subordonné à la seule inaction de l'hébergeur et d'autre part ces derniers disposent d'une large marge de manœuvre leur permettant en pratique d'élaborer leur propre politique éditoriale au détriment parfois de la liberté d'expression et de la qualité de l'information y circulant. La création d'une nouvelle catégorie d'acteurs s'inscrivant entre les éditeurs de contenus et les prestataires techniques devient une nécessité (**§1**). Cette nouvelle catégorie ne se contenterait pas d'introduire un régime de responsabilité conditionné à la seule inaction du réseau social mais bien au contraire, elle impliquerait des obligations et des sanctions renforcées de manière à responsabiliser les sites de réseaux sociaux à la hauteur de leur impact sociétal (**§2**).

§1. La création d'une nouvelle catégorie d'acteurs

509. Création d'un statut *sui generis*. Au-delà du disfonctionnement observé du système d'autorégulation permis par la LCEN, les caractéristiques intrinsèques au fonctionnement des sites de réseaux sociaux justifient l'adoption d'un nouveau statut juridique pour ces derniers (A). Ceci rappelé, il est dès lors possible de déterminer les contours de ce statut (B).

A. La justification de l'adoption d'un nouveau statut pour les opérateurs des réseaux sociaux

510. Double justification. La nécessité de créer un nouveau statut juridique se justifie au regard de l'inadéquation entre le rôle actif joué par les opérateurs de réseaux sociaux sur les contenus et de la fonction purement technique attribuée à l'hébergeur (1) mais également de l'avantage économique tiré par ces derniers de l'activité de leurs utilisateurs (2).

1) La justification au regard du rôle actif des opérateurs sur les contenus

511. Le rôle actif des opérateurs inadapté à la fonction technique de l'hébergeur. Le fait d'attribuer aux opérateurs des réseaux sociaux la qualification d'hébergeurs revient à leur

reconnaître un rôle davantage technique qu'actif. Or, ces derniers possèdent justement plusieurs caractéristiques qui permettraient de déduire leur rôle actif dans la mise en ligne des contenus. Ce rôle actif peut être observé par l'utilisation du ciblage publicitaire (a) mais également, de manière plus générale, par l'utilisation d'un algorithme qui détermine la visibilité des contenus (b).

a- L'utilisation du ciblage publicitaire

512. La technique du ciblage publicitaire sur les sites de réseaux sociaux. Le ciblage publicitaire est une technique consistant à personnaliser les contenus promotionnels, en fonction du comportement des internautes et de l'identification de leurs centres d'intérêt. Ce ciblage comportemental[1353] est permis par l'utilisation des cookies présents sur l'ordinateur ou le téléphone mobile de l'individu. Cette technique publicitaire utilise notamment l'historique des pages visitées, les recherches effectuées sur les sites, les achats en ligne et plus généralement toute information susceptible de déterminer avec précision les centres d'intérêt de l'internaute. Les principaux réseaux sociaux recourent à cette technique et y fondent, à l'image de Facebook, leur modèle économique. Le site Facebook propose ainsi à des entreprises, disposant souvent de leur propre page Facebook, un service de publicité ciblée leur permettant de donner une plus grande visibilité à leur marque en fonction de critères prédéterminés. On distingue des critères de bases qui sont le ciblage géographique, le ciblage par âge et le ciblage par sexe. Outre ces premiers critères, le site Facebook propose d'atteindre « *une audience bien plus pertinente* » en ajoutant « *des options de ciblage supplémentaires en fonction des centres d'intérêt, des comportements et des données démographiques* »[1354]. Le réseau social ne se contente donc pas de mettre à disposition des espaces publicitaires, le site propose une gestion personnalisée de la publicité en l'orientant vers certains publics suggérés en amont.

513. Le rôle actif du ciblage publicitaire selon la jurisprudence. La jurisprudence s'est déjà prononcée sur la pratique du ciblage publicitaire pour en déduire une incompatibilité avec le statut d'hébergeur. Il faut en l'espèce distinguer la mise à disposition d'espaces publicitaires qui n'induit pas forcément un pouvoir d'action de l'hébergeur sur le contenu et l'utilisation d'un ciblage publicitaire qui apparaît « *de nature à exclure les dispositions*

[1353] Ce terme est également connu dans sa version anglaise : « *Behavioural targeting* ».
[1354] <https://www.facebook.com/business/learn/facebook-tips-ad-targeting> (dernière consultation le 9 octobre 2019).

applicables à l'hébergeur »[1355]. La Cour de cassation[1356] a ainsi précisé à propos de la société Tiscali que son statut d'hébergeur n'était pas remis en cause en raison de son modèle économique fondé sur la publicité ou du fait que ces publicités soient accessibles depuis des pages personnelles. La non-appartenance de la société à la catégorie des hébergeurs s'explique par sa gestion d'espaces publicitaires. De cet acte de gestion « *se déduit un ciblage publicitaire en lien avec les contenus stockés impliquant une connaissance ou un contrôle desdits contenus* »[1357]. La CJUE à quant à elle précisé que le site eBay joue un rôle actif « *quand il prête une assistance laquelle consiste notamment à optimiser la présentation des offres à la vente en cause ou à promouvoir celles-ci* »[1358]. Le Professeur Laure Marino observe alors que « *l'on ne peut pas s'abriter sous le parapluie du statut de prestataire technique si l'on bascule dans le monde de la publicité, car ce n'est plus du tout d'une simple activité neutre et technique qu'il s'agit* »[1359]. Les opérateurs des réseaux sociaux ne peuvent donc se prévaloir de leur qualité d'hébergeur concernant leur activité de ciblage publicitaire.

b- L'utilisation d'un algorithme pour le traitement des contenus

514. L'intervention de l'algorithme dans le tri des contenus. Les principaux réseaux sociaux tirent leurs revenus de la revente à des fins publicitaires des données générées par leurs utilisateurs. Ainsi, plus il y a de contenus mis en ligne et d'interactions entre les utilisateurs plus cela profite au réseau social. Partant, il est de leur intérêt de favoriser l'activité au sein de leurs plateformes d'échanges. Dans cette optique, le réseau social Facebook met tout en œuvre pour pousser l'utilisateur à livrer des informations. Cela se traduit par certaines suggestions présentes à divers endroits du profil de l'utilisateur : « *exprimez-vous* », « *qu'avez-vous fait aujourd'hui ?* », « *Cela fait longtemps que vous n'avez pas changé votre photo de profil* », etc. Le réseau social suggérant parfois lui-même la publication de contenus préfabriqués[1360]. Dans ces cas de figure c'est toujours l'utilisateur qui

[1355] A. de SAINT MARTIN, « Clarification de la qualification de service d'hébergement », *RLDI*, 2011, n° 70.
[1356] Civ. 1ère, 14 janvier 2010, n° 06-18.855.
[1357] R. HARDOUIN, « L'hébergeur et la publicité : la neutralité comme condition d'une coexistence », *RLDI*, 2010, n° 62.
[1358] CJUE, 12 juillet 2011, aff. C-324/09, L'Oréal et a. c/ eBay International et a. : *CCE* 2011, comm. 99, note C. CARON ; Propr. industr. 2011, comm. 71, note A. FOLLIARD-MONGUIRAL ; *Gaz. Pal.* 26 octobre 2011, n° 299, p. 19, note L. MARINO ; *D.* 2011, p. 1965, obs. C. MANARA ; *D.* 2011, p. 2054, point de vue P.-Y. GAUTIER ; *RTDE* 2011, p. 847, obs. E. TREPPOZ ; *RLDI*, 2011, n° 74, n° 67, note C. CASTETS-RENARD ; *RLDI*, 2011, n° 74, n° 2459, p. 61, note L. GRYNBAUM.
[1359] L. MARINO, « Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl.* Comm., Fasc. 670, août 2015 (mis à jour décembre 2017), n° 31.
[1360] Il s'agit souvent de petites vidéos relatant des relations sur le réseau social entre l'utilisateur et un de ses contacts. Le réseau social choisi souvent comme prétexte de publication une date symbolique, par exemple : « *fêtez vos cinq ans d'amitié sur Facebook* ».

a le dernier mot quant au choix de publier un contenu ou au contraire de rester inactif. De ce fait, si l'on peut considérer que le réseau social intervient dans le processus de mise en ligne du contenu il est toutefois difficile de lui reconnaître à ce stade une connaissance ou un contrôle effectif du contenu de nature à remettre en question son statut d'hébergeur. Cependant, outre la mise en place d'outils incitant les utilisateurs à publier des informations personnelles, les opérateurs des réseaux sociaux réalisent un tri des contenus mis en ligne suivant un algorithme[1361] développé en amont[1362]. En conséquence, le flux des informations visibles sur les réseaux sociaux est tout sauf une publication neutre des contenus postés par les utilisateurs. La visibilité des contenus est déterminée en fonction de leur catégorie par un algorithme. Par exemple, afin de préserver son modèle économique, Facebook a choisi un algorithme privilégiant la mise en avant des contenus qui ont une forte propension à créer des réactions ou interactions[1363]. L'algorithme classe les contenus en fonction de différents facteurs. Le premier concerne l'engagement de l'utilisateur, autrement dit, plus une personne interagit avec une page, plus Facebook aura tendance à faire apparaître sur son fil d'actualité les publications de cette page. Ensuite, les contenus sont également classés en fonction de leur performance, cela insinue que plus un contenu suscite d'interactions plus il sera visible dans le fil d'actualité. Les interactions ne sont cependant pas toutes classées sur un pied d'égalité : le partage d'un contenu aura plus de poids qu'un commentaire qui aura lui-même plus de poids qu'un simple « *Like* ». La visibilité est également fonction du type de contenu. La

[1361] Le sociologue Dominique Cardon définit l'algorithme de la manière suivante : « *Comme la recette de cuisine, un algorithme est une série d'instructions permettant d'obtenir un résultat. À très grande vitesse, il opère un ensemble de calculs à partir de gigantesques masses de données (les "big data"). Il hiérarchise l'information, devine ce qui nous intéresse, sélectionne les biens que nous préférons et s'efforce de nous suppléer dans de nombreuses tâches. Nous fabriquons ces calculateurs, mais en retour ils nous construisent* ». D. CARDON, *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, Seuil, 2015, p. 7. Le ministère de l'économie, de l'industrie et du numérique définit pour sa part l'algorithme comme « *une succession finie et bien définie d'opérations ou d'instructions qui permettent de résoudre un problème ou d'obtenir un résultat. En général, l'algorithme utilise des données d'entrée, les traite suivant des instructions précises et fournit un résultat* ». Ministère de l'économie de l'industrie et du numérique, *Modalités de régulation des algorithmes de traitement des contenus*, rapport à Mme la Secrétaire d'État chargée du numérique, 13 mai 2016, p. 57.

[1362] Concernant l'algorithme du réseau social Facebook v. : T. FELLE, « Changement d'algorithme sur Facebook : moins de contenus "médias", plus de recettes publicitaires », *The conversation*, 25 janvier 2018. <https://theconversation.com/changement-dalgorithme-sur-facebook-moins-de-contenus-medias-plus-de-recettes-publicitaires-90660> (dernière consultation le 9 octobre 2019) ; N. PIGNARD-CHEYNEL, J. RICHARD ET M. RUMIGNANI, « Au-delà du mur : l'algorithme de Facebook mis à l'épreuve », *The conversation*, 25 septembre 2017, mis à jour le 15 janvier 2018. <https://theconversation.com/au-dela-du-mur-lalgorithme-de-facebook-mis-a-lepreuve-84295> (dernière consultation le 9 octobre 2019).

[1363] Facebook explique son choix éditorial dans sa page d'aide « *comment fonctionne le fil d'actualité ?* », il précise notamment que « *les publications qui s'affichent en premier sont sélectionnées en fonction de votre activité et de vos contacts sur Facebook. Une actualité peut également apparaître plus haut dans votre fil d'actualité en fonction du nombre de commentaires, de mentions J'aime et de réactions qu'elle reçoit, ainsi que de sa nature (par exemple, s'il s'agit d'une photo, d'une vidéo ou d'un nouveau statut)* ». <https://www.facebook.com/help/1155510281178725> (dernière consultation le 9 octobre 2019).

capacité d'un contenu à être visible dans le fil d'actualité sera différente s'il s'agit d'un simple texte, d'un lien, d'une image, d'une vidéo ou d'un live. Par exemple, le réseau social Facebook privilégie les contenus vidéos hébergés directement sur sa plateforme et particulièrement les « *Facebook Live* »[1364]. Les images ont alors un moins fort potentiel de visibilité que la vidéo ; les liens et les textes ont quant à eux un moins fort potentiel de visibilité que les images ou vidéos. Enfin, la récence du contenu agira sur sa visibilité, plus le contenu posté est ancien, moins il apparaîtra, à moins bien sûr que ce dernier suscite beaucoup d'interactions !

515. L'algorithme, une intervention sur le fond ou la forme ? Il revient de s'interroger sur la nature du rôle joué par l'algorithme : ce dernier manifeste-t-il une réelle intervention sur le fond du contenu de nature à justifier une remise en cause du statut d'hébergeur ou ne constitue-t-il qu'une mesure de rationalisation n'agissant que sur la forme du contenu et n'impactant donc aucunement le statut d'hébergeur ? Une première analyse pourrait conclure que la classification du contenu ne traduit en aucun cas un quelconque indice pouvant justifier une requalification du statut d'hébergeur. Le tri des contenus participerait alors de la même dynamique que l'architecture du site, la présentation du site, l'interface de visualisation ou encore le formatage des contenus. La jurisprudence a ainsi listé dans l'arrêt Dailymotion[1365] plusieurs interventions du site de streaming sur la forme du contenu qui n'étaient pas de nature à remettre en cause son statut d'hébergeur. Selon les juges de la Cour de cassation, « *le réencodage* », le « *formatage* », ou la « *mise en place de cadres de présentation et la mise à disposition d'outils de classification des contenus* » sont, selon la Cour « *des opérations techniques qui participent de l'essence du prestataire d'hébergement et qui n'induisent en rien une sélection par ce dernier des contenus mis en ligne* ». L'activité de fournisseur d'hébergement implique nécessairement une structuration des informations stockées[1366]. Il apparaît alors justifié que le critère du rôle actif dégagé par la jurisprudence s'analyse au regard du fond du contenu et non de la forme de ce dernier qui n'est pas un critère déterminant dans l'établissement du statut juridique de l'intervenant[1367].

[1364] Nouvelle fonctionnalité Facebook permettant de transmettre une vidéo en direct sur le réseau social.

[1365] Civ. 1ère, 17 février 2011, n° 09-67.896 : *Bull. civ.* I n° 30 ; *CCE* 2011, comm. 32, note C. CARON ; *JCP* G 2011, 520, note A. DEBET ; *Gaz. Pal.* 23 juin. 2011, p. 20, note L. MARINO ; Resp. civ. et assur. 2011, étude 8, L. MARINO ; Propr. intell. 2011, n° 39, p. 197, note A. LUCAS ; *D.* 2011, p. 1113, note L. GRYNBAUM ; RLDI, 2011, n° 69, n° 2258, note C. CASTETS-RENARD ; *Légipresse* 2011, n° 283, p. 297, note V. VARET.

[1366] Sénat, Rapport d'information n° 296 sur l'évaluation de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon, 9 février 2011, p. 47.

[1367] Selon A. ST MARTIN : « *Il nous semble conséquemment acquis que l'intervention sur le contenu susceptible d'écarter la qualification d'hébergeur doit nécessairement avoir pour siège le fond du contenu, par*

516. Il serait cependant réducteur de cantonner l'action de l'algorithme à une simple mesure de classement et de rationalisation ne relevant en conséquence que d'une intervention purement technique sur la forme du contenu. À ce sujet, la CJUE[1368] a rappelé que le pouvoir d'intervention d'un site sur le fond du contenu se mesure au regard de sa connaissance ou de son pouvoir de contrôle des données stockées. En l'occurrence, la mise en place d'un algorithme révèle une intervention bien plus sophistiquée qu'une simple rationalisation de l'information, susceptible de déterminer un véritable pouvoir de contrôle du fond de l'information. Par exemple, le réseau social Facebook joue un véritable rôle actif dans la mise en ligne des contenus en sélectionnant ces derniers de manière à entretenir la pérennité de son modèle économique. Il a ainsi été observé que : « *la plateforme est devenue le plus grand site de partage d'informations au monde, et contrôle au niveau individuel ce que deux milliards de personnes voient quotidiennement sur leurs fils d'actualités* »[1369]. Ce pouvoir d'intervention du réseau social sur le contenu est donc d'une importance particulière et pourtant, la politique algorithmique mise en place est dangereuse à deux niveaux. Dans un premier temps, elle favorise la visibilité des contenus au fort potentiel de viralité, autrement dit les contenus suscitant beaucoup de débats et de commentaires. Or ces informations correspondent le plus souvent aux contenus véhiculant des messages de haine, de violence ou d'indignation. Les « *Fake news* » bénéficient également d'une très forte visibilité, particulièrement lors des campagnes présidentielles française de 2017 et américaine de 2016, en raison de leur concordance avec la logique de son algorithme[1370]. Le réseau social Facebook contribue ainsi à mettre en avant des contenus qui pourraient exposer leurs auteurs à d'éventuelles poursuites pénales. Dans un second temps, les algorithmes sont à l'origine d'un phénomène appelé « *bulle de filtres* »[1371] selon lequel l'utilisateur s'enferme peu à peu dans un cercle de publications de même nature entretenant une réalité alternative loin de constituer une source d'information exhaustive et donc fiable. Le fonctionnement est similaire

---

opposition à sa forme, laquelle peut être modifiée sans contrôle du fond pour des motifs techniques », *RLDI*, 2011, n° 70.

[1368] CJUE, *Sté Google c/ Sté Louis Vuitton Malletier*, 23 mars 2010, aff. C-236/08 à C-238/08 : *JCP* G 2010, note 642, L. MARINO ; *JCP* G 2011, 1175, doctr. F. TERRÉ ; *CCE* 2010, comm. 88, note P. STOFFEL-MUNCK ; *CCE* 2010, comm. 70, note C. CARON ; *CCE* 2010, étude 12, G. BONET ; *D.* 2010, p. 885, obs. C. MANARA ; *RTDE* 2010, p. 939, obs. E. TREPPOZ ; *CCC* 2010, comm. 132, note M. MALAURIE-VIGNAL ; *RLDI*, 2010, n° 60, n° 1980, note L. GRYNBAUM ; *RLDI*, 2010, n° 61, n° 1999, note C. CASTETS-RENARD ; *Légipresse* 2010, n° 274, p. 158, note C. MARECHAL ; *Propr. industr.* 2010, comm. 31, note P. TREFIGNY-GOY.

[1369] T. FELLE, « Changement d'algorithme sur Facebook : moins de contenus "médias", plus de recettes publicitaires », *The conversation*, 25 janvier 2018.

[1370] *Ibid*.

[1371] E. PARISER, *The filter bubble: how the new personalized web is changing what we read and how we think*, Penguin books, 2012.

sur Twitter, son système de tendances et de hashtags aboutit mécaniquement à « *canaliser et à uniformiser une parole "mainstream" autour de grands centres d'intérêt* »[1372]. Plus encore, le fonctionnement de ce site basé sur des messages courts et sur un mécanisme de renvoie favorise « *l'invective, le buzz, le conflit, tout en rendant quasiment impossibles les propos d'apaisement et de compréhension qui peuvent rarement se tenir en 280 caractères* »[1373]. Ces observations valent également pour l'algorithme de la plateforme de partage de vidéos Youtube qui favorise les contenus agressifs, diffamants, choquants ou complotistes alors même que 70 % des contenus visionnés sur le site de partage de vidéos le sont sur recommandation de son algorithme[1374]. Au final, les sites de réseaux sociaux favorisent un appauvrissement général de la qualité de l'information, la parole est à la fois « *creuse et uniforme* » mais également « *virulente et éruptive* »[1375]. Monsieur Emmanuel Netter résume ce constat de la manière suivante : « *Ces plateformes ne se contentent pas de relayer de manière neutre et exhaustive les contenus proposés par les utilisateurs : à l'aide d'algorithmes, elles les filtrent pour complaire à ceux qui compulsent leurs fils d'actualité, au risque d'offrir aux internautes une vision excessivement personnalisée, et donc biaisée, du monde qui les entoure* »[1376].

517. Suivant ces constatations il semble alors difficile d'affirmer que les opérateurs des réseaux sociaux ne jouent pas un rôle actif sur les contenus et qu'ils ne sont pas en mesure de les contrôler. Cette intervention dépasse de loin une simple classification des contenus relevant d'une intervention sur la forme. L'algorithme agît sur le fond en ce qu'il détermine des tendances propres à entretenir le modèle économique des sites de réseaux sociaux et favorisant en outre une prolifération de messages à fort taux d'interaction. Ce mode de fonctionnement révèle alors l'existence d'un choix éditorial dans la mise en ligne des contenus permettant de remettre en cause le statut d'hébergeur du site[1377]. Dès lors il est

[1372] R. LE GUNEHEC, « Twitter et la vie d'avant : les réseaux sociaux changent-ils tout ? », *Légipresse* n° 355, décembre 2017, p. 600.
[1373] « PPL Avia, refusez les mesures inutiles et dangereuses », *La Quadrature du Net*, analyse juridique de la loi « contre la haine en ligne », le 17 juin 2019.
[1374] J. E. SOLSMAN, « YouTube's AI is the puppet master over most of what you watch », *Cnet*, 10 janvier 2018. <https://www.cnet.com/news/youtube-ces-2018-neal-mohan> (dernière consultation le 9 octobre 2019).
[1375] R. LE GUNEHEC, « Twitter et la vie d'avant : les réseaux sociaux changent-ils tout ? », *op. cit.*
[1376] E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, n° 178, p. 220.
[1377] Dans une ordonnance de référé en date du 26 mars 2008, le juge du fond a condamné l'hébergeur Fuzz.fr au motif qu'en publiant un lien vers un site au contenu litigieux, il devait être considéré comme un « *site d'information original* ». Selon le juge la publication de ce lien opérait un choix éditorial en tant qu'il marquait la volonté de mettre le public en contact avec des messages de son choix. Dès lors, cela justifie que le site revêt la qualité d' « *éditeur* » au sens de la loi pour la confiance dans l'économie numérique concernant le contenu en cause. V. TGI Paris, ordonnance de référé, 26 mars 2008, Olivier M. / Bloobox Net. < https://www.legalis.net>.

justifié d'envisager une requalification du statut des opérateurs des réseaux sociaux fonctionnant sur ce modèle.

2) La justification au regard de l'avantage économique tiré par les réseaux sociaux

518. Application de la théorie du risque. Par ailleurs, Le Professeur Tristan Azzi propose de justifier l'adoption d'un régime de responsabilité plus stricte pour les grandes plateformes numériques par le biais de la théorie du risque[1378], cette notion de droit civil[1379] ayant permis de proposer des principes de responsabilité satisfaisant à nombre de progrès technique[1380]. Son postulat est simple : il revient à la personne à l'origine d'une activité à risque, d'autant plus lorsqu'elle en tire un profit, d'en assumer la responsabilité[1381]. Cette théorie répond ainsi à l'adage : « *Ubi emolentum, ibi onus* »[1382] et justifie une approche plus sévère en matière de responsabilité à l'égard de ces nouvelles plateformes numériques dans la mesure où elles tirent un avantage économique émanant directement de l'activité de leurs utilisateurs. Ces dernières se montrent cependant réticentes et opposent une série d'arguments en faveur d'une responsabilité plus modérée, le Professeur Tristan Azzi nuance cependant ces arguments[1383] :

Dans la même logique, la Cour d'appel de Paris a considéré à propos de la société eBay que son rôle ne « *se limitait pas à classer et à faciliter la lisibilité des offres et des demandes mais consiste à les promouvoir activement et à les orienter pour optimiser les chances qu'elles aboutissent à des transactions effectives sur le montant desquelles il percevra une commission dont le taux est fonction du niveau du prix auquel la vente a été conclue* ». V. Paris, pôle 5, ch. 2, 3 septembre 2010, n° 08/12821, eBay Inc, eBay International c/ Christian Dior Couture.

[1378] T. AZZI, « La responsabilité des nouvelles plates-formes : éditeurs, hébergeurs ou autre voie ? », *in* : *Contrefaçon sur Internet. Les enjeux du droit d'auteur sur le WEB 2.0*, LexisNexis, coll. IRPI, 2009, n° 33, p. 69.

[1379] La « *théorie du risque* » provient à l'origine de l'impossibilité de fonder la réparation des accidents du travail provoqués par des machines sur la notion de faute. La notion de « *risque* » vient alors pallier l'absence de faute objective génératrice de responsabilité. Raymond Saleilles développa cette théorie en faisant d'abord référence au « *risque professionnel* » ou au « *risque industriel* », avant d'en déduire la « *théorie du risque* » de manière à part entière. V. R. SALEILLES, *Les accidents du travail et la responsabilité civile : essai d'une théorie objective de la responsabilité délictuelle*, 1897, éd. A. Rousseau ; V. également la note écrite par l'auteur au *D.* 1897, p. 433, préc. p. 438 ; ainsi que le texte de la conférence qu'il a présentée à la Société d'économie sociale le 14 février 1898, *La réforme sociale*, 1898 , p. 634 et suiv. Louis Josserand joignit également son analyse à celle de Raymond Saleilles, il est ainsi considéré comme cofondateur de la théorie du risque. V. L. JOSSERAND, *De la responsabilité du fait des choses inanimées*, Éd. A. Rousseau, 1897.

[1380] L'influence de la théorie du risque est certaine. Certains régimes spéciaux de responsabilité ont été construits autour d'elle, en particulier le régime de réparation des accidents du travail (Loi n° 85-677 du 5 juillet 1985 tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation), la loi du 5 juillet 1985, relative à l'indemnisation des victimes d'accidents de la circulation (Loi n° 85-677 du 5 juillet 1985 tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation) ou encore la loi du 4 mars 2002, relative aux risques sanitaires (Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé). MM. F. TERRÉ, P. SIMLER et Y. LEQUETTE, *Droit civil. Les obligations*. Dalloz, 11ème éd. 2013, n° 684.

[1381] G. VINEY, *Traité de droit civil. Introduction à la responsabilité*, LGDJ, 2ème éd., p. 82, n° 49.

[1382] « *Où est le profit, là est la charge* ». H. ROLAND et L. BOYER, *Adages du droit français*, 1999, Litec, nº 452.

[1383] T. AZZI, « La responsabilité des nouvelles plates-formes : éditeurs, hébergeurs ou autre voie ? », *op. cit.*

519. Argument économique. Le premier argument soulevé par les opérateurs des réseaux sociaux est économique. Accroître leur responsabilité diminuerait leur rentabilité et freinerait ainsi le développement de l'économie numérique[1384]. Cet argument ne saurait l'emporter dans la mesure où d'éventuelles condamnations financières ne menaceraient pas véritablement leur prospérité économique. Mais surtout, la condamnation d'une activité doit intervenir indépendamment de toute considération économique, seul son caractère répréhensible doit en dépendre.

520. Argument concernant la création des contenus. Un deuxième argument tient au fait que ces nouvelles plateformes ne sont pas à l'origine des contenus illicites qui y sont générés et qu'il serait injuste de les en tenir responsables. Ce à quoi il est répondu que ces sites ne sont certes pas créateurs des contenus mais jouent néanmoins un rôle actif dans l'administration de ces contenus. Le fort pouvoir d'influence des opérateurs des réseaux sociaux *via* leurs algorithmes sur les contenus est alors de nature à justifier un engagement plus strict de leur responsabilité sans toutefois les assimiler à des éditeurs de contenus.

521. Argument de l'impossibilité d'un contrôle généralisé. Enfin, le troisième argument avancé revient au fait qu'il serait particulièrement difficile pour les sites de réseaux sociaux, au regard de leur nombre d'utilisateurs, de contrôler l'ensemble des informations qui y transitent, et qu'une condamnation systématique ne serait pas justifiée. Ce contrôle généralisé serait dangereux en ce qu'il introduirait une modération *a priori* des contenus revenant à un régime de *notice and stay down* et favorisant ainsi un système de censure privée. Ce constat vaut d'autant plus que par excès de zèle certaines plateformes pourraient avoir une interprétation trop large de leurs obligations et auraient alors tendance à censurer des contenus parfaitement licites. Il s'agit en l'occurrence d'une véritable limite à ne pas franchir dans la détermination d'une responsabilité renforcée à l'égard des opérateurs de réseaux sociaux. Cependant, l'adoption d'un statut juridique plus engageant que celui actuellement prévu pour les hébergeurs n'implique pas automatiquement l'adoption d'une obligation générale de surveillance, l'interdiction d'une telle obligation doit même être rappelée avec vigueur au sein de ce nouveau statut juridique.

[1384] Le développement de l'économie numérique est un argument souvent utilisé par le législateur dans l'adoption de nouvelles réformes. Cela a par exemple été le cas pour la directive « commerce électronique » (Dir. 2000/31/CE, 8 juin 2000, art. 14). En l'espèce, les considérations économiques sont majeures. L'absence d'obligation de surveillance décharge les prestataires des coûts qu'induiraient les contrôles, l'allégement de la responsabilité les dégrève des coûts qu'engendreraient les condamnations. V. L. MARINO, *Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement*, *J.-Cl.* Comm., Fasc. 670, 30 août 2015 (dernière mis à jour 1er décembre 2017), n° 3.

522. Dès lors que les réseaux sociaux mettent en place un système de communication favorisant des activités illicites, ces derniers créent un risque dont ils doivent en assumer la responsabilité. La théorie du risque doit cependant être utilisée avec nuance pour ne pas être soumise à de vives critiques[1385]. À ce titre, ce nouveau système de responsabilité doit être cohérent avec les capacités réelles des opérateurs des réseaux sociaux à gérer les flux de données gravitant sur leurs plateformes. Il apparaît donc nécessaire de mettre en œuvre un système de responsabilité accru mais pragmatique pour les grandes plateformes numériques. L'enjeu consiste alors à déterminer du point de vue de la technique juridique quelle forme pourrait revêtir un tel modèle de responsabilité.

B. La détermination du statut juridique applicable aux opérateurs des réseaux sociaux

523. Un nouveau statut pour de nouveaux acteurs. La distinction classique posée par la LCEN entre éditeurs de services et prestataires techniques ne correspond plus à la réalité de tous les acteurs du web actuel, les opérateurs des réseaux sociaux constituent assurément un acteur intermédiaire (1) auquel il convient d'accorder un statut spécifique (2).

1) Les opérateurs des réseaux sociaux, un acteur intermédiaire

524. Une qualification distributive privilégiée par la jurisprudence. L'activité d'un site de réseau social est potentiellement très diversifiée et peut revêtir à ce titre plusieurs qualifications en fonction du rôle qu'il a concrètement joué sur la mise en ligne et la diffusion d'un contenu. Selon cette approche, la détermination de la qualité d'hébergeur dépend de son activité analysée non pas dans son ensemble mais uniquement au regard du contenu qui s'avère litigieux. La jurisprudence a pris cette orientation en privilégiant une application distributive de la qualification d'hébergeur pour appliquer ensuite le système de responsabilité qui en découle[1386]. Par exemple, la plateforme de marché en ligne eBay est considérée comme éditeur lorsqu'elle met en relation le vendeur et l'acheteur en proposant la création de liens pour promouvoir les ventes. À l'inverse, elle est assimilée à un hébergeur lorsqu'elle se livre à

[1385] Notons que la théorie du risque fut décriée par une partie de la doctrine. Marcel Planiol émît des critiques envers la théorie du risque dans deux chroniques. Prenant le parti de la faute comme critère central de la responsabilité l'auteur affirme que « *tout cas de responsabilité sans faute, s'il était réellement admis, serait une injustice sociale* ». Marcel Planiol préfère alors privilégier une conception large de la faute pour favoriser l'indemnisation des victimes plutôt qu'une responsabilité basée sur le risque créé. M. PLANIOL, « Études sur la responsabilité civile, *Rev. Crit.*, 1905, p. 277 et 1906, p. 80. D'autres auteurs à l'origine favorables à la théorie du risque se rallièrent finalement aux idées de Planiol à l'instar de Georges Ripert et Maurice Hauriou. V. G. RIPERT, *La règle morale dans les obligations civiles*, n[os] 112 et suiv. et M. HAURIOU, notes *S.* 1095, III, 113 et 1918-1919, III, 25.

[1386] A. SAINT MARTIN, « Clarification de la qualification de service d'hébergement », *RLDI*, 2011, n° 70.

un stockage d'annonces qui n'inclut pas de services complémentaires[1387]. De même pour Dailymotion qui est un hébergeur pour les vidéos mises en ligne par les internautes et un éditeur pour les vidéos où la plateforme possède les licences d'exploitation[1388]. Cette qualification distributive permet d'être au contact de la réalité complexe des sites de réseaux sociaux. Le Professeur Laure Marino considère par exemple que Facebook pourrait être qualifié « *d'hébergeur pour son activité de réseau social, et d'éditeur pour ses activités marchandes de type E-commerce ou pour sa régie publicitaire* »[1389]. Cette approche ne prend cependant pas en compte le rôle actif des réseaux sociaux dans la détermination des contenus.

525. Le réseau social : ni hébergeur, ni éditeur de contenus. Partant du constat que l'opérateur d'un réseau social de type Facebook ou Twitter contrôle la visibilité des contenus qu'il diffuse selon leurs caractéristiques, l'analyse sur le statut juridique d'un site de réseau social peut également être construite au regard de l'ensemble de son activité. Plus largement, le statut d'hébergeur accordé au réseau social pour son activité relative à la mise en ligne de contenus peut être contesté dans l'hypothèse où il organise une diffusion d'informations orientée et donc dépourvue de neutralité. Le tribunal de grande instance de Paris a reconnu que le régime de responsabilité favorable des hébergeurs ne trouve pas à s'appliquer lorsque « *les activités sont générées ou induite par le prestataire lui-même* »[1390]. En conséquence, l'activité de l'opérateur d'un réseau social pourrait alors se rapprocher de la qualification d'éditeur de contenus dans la mesure où il « *réunit des contenus, sélectionne ceux qu'il souhaite publier, les modifie, les mets en forme et donne l'ordre de publication* »[1391]. Cependant, le critère déterminant du statut d'éditeur de contenus demeure l'intervention dans la création même des contenus[1392]. Or, bien qu'il soit admis que les opérateurs des réseaux sociaux jouent un rôle actif sur les contenus mis en ligne, leur rôle ne peut être assimilé pour l'ensemble de leur activité à celui de créateur de contenus. Le statut d'éditeur revient en l'occurrence principalement à leurs utilisateurs qui jouent véritablement ce rôle créateur. La situation semble d'apparence insoluble : les opérateurs des réseaux sociaux ne permettent pas de répondre, dans le cadre de leur activité principale, aux critères définissant les hébergeurs

[1387] Reims, ch. civ., 1ère sect., 20 juillet 2010, n° 08/01519, eBay France et International c/ Hermès International et a. – Paris, pôle 5, ch. 2, 3 septembre 2010, n° 08/12821, eBay Inc, eBay International c/ Christian Dior Couture.
[1388] TGI Paris, 4ème sect., 13 septembre 2012, n° 09/19255, TF1 et a. c/ Dailymotion : *CCE* 2012, comm. 122, note A. DEBET ; *RLDI*, 2012, n° 88, note B. VANDEVELDE.
[1389] L. MARINO, « Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl.* Comm., fasc. 670, août 2015 (mis à jour décembre 2017), n° 25.
[1390] TGI Paris, 13 juillet 2007, Christian C. c/ Dailymotion, Propr. Intell. 2008. 364, obs. J. Passa ; *CCE* 2007, com. 143, obs. C. CARON ; *RIDA* octobre 2007, n° 214, p. 293, obs. P. SIRINELLI.
[1391] L. THOUMYRE, « Les notions d'éditeurs et d'hébergeurs dans l'économie numérique », *D.* 2010, p. 837.
[1392] M. QUÉMÉNER, Y. CHARPENEL, *Cybercriminalité, Droit pénal appliqué*, Économica, 2010, p. 45.

mais également à ceux définissant les éditeurs. Leur intervention sur les contenus est trop importante pour leur reconnaître un rôle essentiellement technique, mais l'activité de création de contenus ne relève pas de leur fait. La solution revient alors à leur reconnaître un statut intermédiaire organisant un système de responsabilité en adéquation avec leur véritable rôle joué, c'est-à-dire, plus souple que celui des éditeurs de contenus mais plus engageant que l'actuel statut des hébergeurs.

2) Les opérateurs des réseaux sociaux, un statut spécifique

526. Proposition du Sénat : la nouvelle catégorie des « *éditeurs de services* ». Le Sénat a proposé dans un rapport du 9 février 2011 la création d'une catégorie *sui generis* d'intervenants nommée les « *éditeurs de services* »[1393]. Selon le Sénat, la distinction entre éditeur et hébergeur de contenus, pensée dans les années 1990, ne correspond plus à la réalité actuelle des activités sur internet et du web 2.0 particulièrement. Les hébergeurs ne forment plus une catégorie homogène caractérisée par la seule fourniture de prestations purement techniques et adopteraient une démarche de plus en plus active notamment en « *publiant eux-mêmes des informations ; vendant des espaces publicitaires et tirant des recettes qui dépendent du succès des contenus hébergés* »[1394]. Le terme « *éditeur de service* » n'est en réalité pas nouveau[1395], ce dernier étant actuellement confondu avec la notion d' « *éditeur de contenus* »[1396]. Il est alors proposé de donner à cette notion une existence à part entière au sein des acteurs de la communication au public en ligne revenant à distinguer l' « *éditeur de services* » de l' « *éditeur de contenu* » et du « *fournisseur d'hébergement* ». Pour l'heure, l'article 6, III de la LCEN considère les éditeurs comme la personne qui « *édite un service de communication au public* », à titre professionnel ou non, autrement dit, l'éditeur est la personne qui crée ou rassemble du contenu. Cette définition légale ne distingue toutefois pas les « *éditeurs de contenus* » des « *éditeurs de services* ». Un critère de qualification permettant de dissocier clairement les « *éditeurs de services* » des autres prestataires techniques doit alors être établi. Sur ce point, le rapport préconise l'utilisation de « *l'avantage économique direct retiré de la consultation des contenus* » comme critère principal de

[1393] Sénat, Rapport d'information n° 296 sur l'évaluation de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon, 9 février 2011, p. 44.
[1394] *Ibid*.
[1395] V. par exemple : E. DERIEUX, *Droit des médias. Droit français, européen et international*, 7ème éd., LGDJ, p. 232., n° 823.
[1396] Tristan AZZI parle d'un « *système qui manque cruellement de clarté* » à propos des « *éditeurs de services* » et des « *éditeurs de contenus* », T. AZZI « La responsabilité des nouvelles plates-formes : éditeurs, hébergeurs ou autre voie ? », *in Contrefaçon sur Internet. Les enjeux du droit d'auteur sur le WEB 2.0*, LexisNexis, coll. IRPI, 2009, p. 72, n° 20. V. *supra* n° 417.

l'application de ce nouveau statut. Ce critère permettrait ainsi d'appliquer un régime de responsabilité spécifique plus contraignant que celui des hébergeurs. Ce régime de responsabilité pourrait se construire au regard de celui existant actuellement pour l'hébergeur de contenus. La catégorie des « *éditeurs de services* » se définirait en conséquence au regard de celle plus large des prestataires techniques et non au regard de celle des « *éditeurs de contenus* ». Cependant, le choix de partir d'une notion préexistante pour définir une nouvelle catégorie d'acteurs ne paraît en l'espèce pas opportun, pis encore, est de nature à obscurcir la distinction entre les différents régimes de responsabilité applicables. Il est ainsi préférable d'associer à cette nouvelle catégorie intermédiaire d'acteurs une nouvelle notion et définition.

527. Proposition de création de la catégorie des « *accélérateurs de contenus* ». Plus récemment, le rapport d'une mission relative à la lutte contre le racisme et l'antisémitisme publié le 20 septembre 2018 a proposé pour sa part de définir un statut d'« *accélérateur de contenus* »[1397] pour appréhender juridiquement des opérateurs « *dont l'activité consiste à mettre en avant, référencer ou hiérarchiser des contenus en ligne - et qui ne sont donc ni de simples hébergeurs, ni des éditeurs* »[1398]. Ce statut spécifique s'appliquerait ainsi aux grandes plateformes numériques et viserait en particulier les principaux sites de réseaux sociaux mais également les moteurs de recherche. Ceci se justifie du fait que ces acteurs majeurs offrent à leurs utilisateurs un potentiel de diffusion et d'interaction inégalé permettant de caractériser ce trouble à l'ordre public numérique. Ceci permettrait notamment de préserver les autres opérateurs mettant en œuvre des plateformes relationnelles de plus modeste taille qui ne peuvent caractériser un tel trouble. Certains invitent alors à cibler les plateformes « *en position dominante* » ou encore « *les grands acteurs structurant pour l'économie numérique* »[1399]. Le Conseil national du numérique propose pour sa part de créer une catégorie de plateformes « *dotées de la plus forte capacité de nuisance* »[1400] qui justifierait l'application de règles spécifiques. Les critères de définition de ces plateformes doivent être les plus objectifs possibles afin de réduire au maximum les divergences d'interprétation. À ce titre, le critère de l'audience ou de la fréquentation de la plateforme est d'une particulière

[1397] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018, p. 19, n° 114.
[1398] M. QUEMENER, « Haine sur internet : quelles nouvelles préconisations ? », *RLDI*, 2018, n° 154.
[1399] C. FÉRAL-SCHUHL, *Cyberdroit. Le droit à l'épreuve de l'internet*, 7ème éd., Dalloz, 2018-2019, p. 1449, n° 626.131.
[1400] C. PAUL et C. FERAL-SCHUL, *Numérique et libertés : un nouvel âge démocratique*, Rapport d'information sur le droit et les libertés à l'âge du numérique n° 3119, 8 octobre 2015.

objectivité. La loi allemande *NetzDG*[1401] a mis en avant ce critère en prévoyant des obligations et sanctions renforcées pour tous les sites de réseaux sociaux dont le nombre d'utilisateurs est supérieur à deux millions. Sur la base de ces énonciations, la proposition de loi visant à lutter contre la haine sur internet[1402] consacre ce nouveau type particulier d'acteurs au sein d'un nouvel article 6-2 de la LCEN. Le législateur définit en l'occurrence ces acteurs comme : « *les opérateurs de plateforme en ligne au sens du I de l'article L. 111-7 du code de la consommation qui proposent un service de communication au public en ligne reposant sur la mise en relation de plusieurs parties en vue du partage de contenus publics ou sur le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus proposés ou mis en ligne par des tiers et dont l'activité sur le territoire français dépasse des seuils déterminés par décret* ». Ce nouveau régime juridique concerne principalement deux catégories d'acteurs. Dans un premier temps, « *les services de communication au public en ligne reposant sur la mise en relation de plusieurs parties en vue du partage de contenus publics* », à savoir les plateformes de partage et les plateformes relationnelles[1403] dont les réseaux sociaux font partie mais aussi les plateformes collaboratives[1404]. Dans un second temps, « *les sites reposant sur le sur le classement ou le référencement, au moyen d'algorithmes informatiques* », faisant référence aux moteurs de recherche[1405]. Il s'agit dès lors de mettre en évidence le nouveau régime de responsabilité spécifique qui se dessine à l'égard de ces acteurs dominants de l'économie numérique.

§2. La définition d'un régime de responsabilité renforcé

528. Une responsabilisation dans l'intérêt des utilisateurs. Responsabiliser les opérateurs des réseaux sociaux implique de leur attribuer un statut juridique plus contraignant que celui des hébergeurs. Cela passe notamment par la création d'obligations à la charge de cette nouvelle catégorie d'acteurs. Les obligations instaurées doivent cependant avant tout servir l'intérêt des utilisateurs et ne pas entraîner un affaiblissement de leurs droits et libertés fondamentales notamment la liberté d'expression et le droit à l'information de ces derniers. En l'occurrence, le législateur se basant sur le rapport « *renforcer la lutte contre le racisme et*

[1401] Loi *Netzwerkdurchsetzungsgesetz*, ou *NetzDG*, entrée en vigueur le 1er janvier 2018. Consultable sur <https://www.gesetze-im-internet.de/netzdg/index.html> (dernière consultation le 9 octobre 2019).
[1402] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019.
[1403] Principalement les plateformes de type : Youtube, Facebook, Twitter.
[1404] Ces plateformes équivalent aux sites de type : Le Bon Coin, TripAdvisor, Wikipédia.
[1405] Par exemple : Google, Yahoo!, Bing, Qwant, Ecosia.

l'antisémitisme »[1406] propose d'instaurer au sein de la LCEN un régime de responsabilité renforcé à l'égard de la catégorie des « *accélérateurs de contenus* » (A). Ce nouveau statut devrait être également accompagné d'une obligation de loyauté associée aux algorithmes de traitement (B).

A. L'émergence d'obligations renforcées au regard du statut classique d'hébergeur

529. Une responsabilisation renforcée et mesurée. La création d'un nouveau régime de responsabilité visant les grandes plateformes numériques poursuit l'objectif de contenir la multiplication des discours de haine observés sur ces dernières. Pour ce faire, le législateur propose d'instaurer un régime de responsabilité renforcé à l'égard de la catégorie des « *accélérateurs de contenus* » dont les opérateurs des réseaux sociaux font partie. Cette réforme tend alors à lutter contre les contenus haineux en obligeant les opérateurs de ces plateformes à « *retirer ou* […] *rendre inaccessible dans un délai de 24 heures après la notification par un ou plusieurs utilisateurs* »[1407] certains contenus revêtant un caractère manifestement illicite en référence à certaines catégories particulières d'infractions. L'objectif est donc d'imposer notamment aux opérateurs des réseaux sociaux des obligations renforcées au regard du régime de responsabilité des hébergeurs prévu à l'article 6 de la LCEN. Ce nouveau régime de responsabilité ne doit cependant pas aboutir à une sur-responsabilisation de ces plateformes au risque d'entraîner une régulation trop intensive de l'expression nécessairement néfaste pour les libertés des utilisateurs. Ceci implique de définir un régime d'obligations équilibré entre sauvegarde de l'ordre public à l'échelle numérique et protection des libertés des utilisateurs (1) et d'appliquer ce dernier à une liste limitative d'infractions (2).

1) Un régime d'obligation équilibré entre sauvegarde de l'ordre public à l'échelle numérique et protection des libertés des utilisateurs

530. Une obligation de surveillance renforcée. Le nouveau régime de responsabilité prévoit une obligation pour les plateformes de réseaux sociaux d'adopter une politique de lutte active au regard de l'intérêt général attaché au respect de la dignité humaine et à la lutte

[1406] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018.
[1407] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 1er, futur article 6-3 de la LCEN.

contre les contenus haineux publiés sur internet[1408]. Si une obligation de surveillance générale doit être proscrite, en revanche une surveillance particulière de certains contenus peut être envisagée. Cette possibilité figure dans le considérant 47 de la Directive du 8 juin 2000 selon lequel : « *l'interdiction pour les États membres d'imposer aux prestataires de services une obligation de surveillance ne vaut que pour les obligations à caractère général. Elle ne concerne pas les obligations de surveillance applicables à un cas spécifique et, notamment, elle ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale* ». Par ailleurs, en plus de cette obligation les opérateurs de plateformes sont également tenus de mettre en œuvre les moyens appropriés pour empêcher la rediffusion des contenus haineux[1409]. Il s'agirait dès lors d'une obligation positive à la charge des plateformes visées par ce nouveau statut de rechercher activement par des moyens humains ou automatisés les contenus visés par cette obligation. Ce nouveau régime de responsabilité équivaut dès lors à une obligation de filtrage spécifique à certains contenus et non temporaire.

531. Les dangers d'un filtrage généralisé au regard des libertés fondamentales. L'introduction de ce nouveau régime de responsabilité ne doit pas pour autant justifier un assouplissement de l'interdiction d'une obligation générale de surveillance. Un devoir de filtrage généralisé des contenus porte nécessairement atteinte à certaines libertés fondamentales qui jouent ici le rôle de « *garde-fous* »[1410] face au mouvement de responsabilisation des plateformes de stockage. Ainsi, une telle obligation qui impliquerait nécessairement l'installation d'un « *système informatique complexe, coûteux, permanent et à ses seuls frais* »[1411] entrerait nécessairement en opposition avec la liberté d'entreprise reconnue à l'article 16 de la charte des droits fondamentaux de l'Union européenne. Mais surtout, un tel système serait en réalité néfaste pour les utilisateurs eux-mêmes. Dans les arrêts SABAM[1412], la Cour de justice constate que l'injonction de mettre en place un système de filtrage permanent et automatique de tous les contenus implique *a fortiori* une analyse systématique de tous les contenus ainsi que la collecte et l'identification des adresses IP des

[1408] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 1er, futur article 6-2 de la LCEN.
[1409] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 2, futur article 6-3 5° *bis*, de la LCEN.
[1410] C. CASTETS-RENARD, « Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet », *D.* 2012, p. 817.
[1411] *Ibid*.
[1412] CJUE, *Scarlet c/ SABAM*, 3ème ch., 24 novembre 2011, aff. C-70/10 : *Gaz. Pal.* 16 février 2012, p. 20, note L. MARINO ; *CCE* 2012, comm. 63, note A. DEBET – CJUE, *SABAM c/ Netlog*, 3ème ch., 16 février 2012, aff. C-360/10 : *Gaz. Pal.* 1er août 2012, p. 18, note L. MARINO ; *CCE* 2012, comm. 63, note A. DEBET.

utilisateurs. Cette pratique porterait nécessairement une atteinte disproportionnée aux données personnelles de leurs utilisateurs protégées par l'article 8 de la charte des droits fondamentaux. Enfin, un tel filtrage pourrait aboutir, en raison de son caractère préventif et généralisé, à la suppression de contenus qui seraient en réalité parfaitement licites ce qui porterait à la fois atteinte à la liberté d'information des utilisateurs n'ayant pas eu accès au contenu censuré et à la liberté d'expression de l'internaute à l'origine du contenu censuré. Il est en conséquence nécessaire que l'obligation de filtrage des contenus haineux se restreigne à un nombre limité d'infractions formant le noyau dur de l'ordre public numérique[1413]. Il est également indispensable que cette obligation ne soit qu'une obligation de moyens et non de résultat afin de ne pas inciter les plateformes à une suppression conservatoire de contenus et préserver ainsi un juste équilibre avec la liberté d'expression de leurs utilisateurs. Le respect de cette obligation serait alors jugé sur la base du rapport de transparence[1414] remis par le réseau social chaque année faisant notamment état des moyens qu'il développe pour mener à bien cette obligation spécifique.

532. Les dangers d'un délai de réaction raccourci. Le nouveau statut juridique applicable aux sites de réseaux sociaux prévoit par ailleurs l'adoption d'un délai de réaction raccourci des plateformes numériques suite à un signalement d'un contenu illicite. Sur ce point, le législateur français propose de calquer ce délai sur celui proposé par la loi allemande *NetzDG*[1415] destinée à sanctionner les contenus haineux sur les sites de réseaux sociaux. Selon ses dispositions, les sites de réseaux sociaux comptant plus de deux millions d'utilisateurs inscrits en Allemagne doivent supprimer localement tout contenu « *dont l'illégalité est évidente* » dans les 24 heures qui suivent son signalement. Dans le cas où l'illégalité du contenu ne serait pas manifeste, le délai est rallongé à sept jours pour que le réseau social prenne une décision. Ce délai peut encore être étendu dans certains cas exceptionnels, notamment si l'auteur du contenu est amené à s'expliquer ou si la décision revient à une institution d'autorégulation réglementée[1416]. En France, le rapport « *renforcer la lutte contre le racisme et l'antisémitisme* » préconise de suivre l'exemple allemand et d'imposer aux

[1413] V. *infra* n° 536.
[1414] V. *infra* n° 535.
[1415] La loi Netzwerkdurchsetzungsgesetz, ou NetzDG, entrée en vigueur le 1er janvier 2018.
Consultable sur : <https://www.gesetze-im-internet.de/netzdg/index.html> (dernière consultation le 9 octobre 2019).
[1416] Pour une explication de la supression de contenu en vertu de la loi NetzDG v. : <https://transparencyreport.google.com/netzdg/youtube?hl=fr> (dernière consultation le 9 octobre 2019).

grandes plateformes un délai de 24 heures pour retirer les contenus manifestement illicites[1417]. Le rapport précise en outre que l'opérateur du réseau social doit faire preuve d'une réactivité extrême lorsque le contenu notifié est constitutif d'une apologie du terrorisme ou d'une provocation au terrorisme[1418]. Dans ces deux hypothèses et lorsque le contenu est manifestement constitutif de l'une de ces qualifications pénales, le rapport propose un délai de réaction d'une heure à l'opérateur du réseau social pour retirer ou du moins bloquer l'accès à ce contenu[1419]. La proposition de loi adoptée par l'Assemblée nationale le 9 juillet 2019 ne reprend toutefois que le délai de réaction de 24 heures à la charge des opérateurs des grandes plateformes numériques[1420]. Ce délai de réaction extrêmement court fait l'objet de vives critiques[1421]. Ce délai a ainsi été jugé « *contre-productif* » en ce qu'il est susceptible de provoquer d'importantes restrictions de libertés en raison du sur-blocage des contenus qu'il induirait[1422]. En effet, ce délai de réaction imposerait aux plateformes visées par ce régime de responsabilité de traiter tous les signalements dans un même et unique délai ce qui les empêcherait de prioriser la modération des contenus les plus graves ou les plus partagés. Le récent exemple de la tuerie de Christchurch retransmise en direct sur le réseau social Facebook démontrant l'incapacité de ce dernier à contenir la propagation de la vidéo sur son réseau[1423] vient d'autant plus nuancer la pertinence de ce délai de réaction de 24 heures. Plus encore, un tel délai de réaction ignore les difficultés d'interprétation intrinsèques aux délits de presse sanctionnant les discours de haine[1424].

533. La nécessaire possibilité de contester la mesure. Il est également nécessaire d'introduire de manière systématique la possibilité pour l'utilisateur visé par le signalement ou pour l'auteur du signalement de faire un recours contre la décision de modération prise à l'encontre du contenu. Ceci implique dans un premier temps d'informer sans délai l'utilisateur et l'auteur de la notification de la décision prise à l'égard du contenu et des motifs ayant

[1417] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018, recommandation n° 1, p. 16.
[1418] Comportements prévus à l'article 421-2-5 C. pén.
[1419] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, *op. cit.*, p. 19, n° 118.
[1420] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 1er, futur art. 6-2, I de la LCEN.
[1421] V. notamment : « PPL Avia, refusez les mesures inutiles et dangereuses », *La Quadrature du Net*, analyse juridique de la loi « contre la haine en ligne », le 17 juin 2019 ; B. NICAUD, « Proposition de loi contre la "cyberhaine" adoptée à l'Assemblée ou l'enfer pavé de bonne (?) intentions », Lexbase Pénal Edition n° 18, 18 juillet 2019.
[1422] « PPL Avia, refusez les mesures inutiles et dangereuses », *La Quadrature du Net*, analyse juridique de la loi « contre la haine en ligne », le 17 juin 2019.
[1423] V. *supra* n° 489.
[1424] V. *supra* nos 468 et suiv.

conduits à ce choix. Il est ainsi prévu d'ajouter un nouvel article 6-3 à la LCEN[1425] prévoyant notamment que les opérateurs des plateformes en ligne « *informent le notifiant et, lorsqu'ils disposent des informations permettant de le contacter, l'utilisateur à l'origine de la publication du contenu notifié, de la date et de l'heure de la notification, des suites données à la notification ainsi que des motifs de leurs décisions* ». Chaque partie doit dès lors pouvoir contester la mesure prise à l'encontre du contenu signalé, cette contestation étant soumise au réexamen du réseau social. Pour ce faire, le nouveau régime de responsabilité impose aux plateformes numériques de mettre en œuvre un dispositif permettant de contester la décision prise lorsqu'ils décident de retirer ou rendre inaccessible un contenu notifié ou lorsqu'ils décident de ne pas faire cesser le référencement du contenu notifié[1426]. Lorsque l'auteur du contenu notifié ou l'auteur de la notification n'est toujours pas satisfait de la décision prise à l'égard du contenu, y compris après réexamen du réseau social, ce dernier doit être en mesure de porter sa contestation à une autorité de contrôle. Enfin, lorsque le contenu en cause est potentiellement constitutif d'une infraction pénale, il est toujours possible d'engager des poursuites à l'encontre de l'auteur du contenu, la modération en ligne du contenu n'effaçant ni la commission l'acte infractionnel, ni la responsabilité pénale de son auteur.

534. Obligation de coopération avec l'autorité judiciaire. L'obligation de coopération avec l'autorité judiciaire est déjà présente dans le régime de responsabilité classique de l'hébergeur, cette obligation prenant la forme d'une obligation de conservation et de transmission de données d'identification. Il s'agit alors de réaffirmer mais également de renforcer cette obligation concernant le nouveau statut juridique applicable aux opérateurs des réseaux sociaux. Si les dispositions de la LCEN comportent d'ores et déjà une obligation de coopération, force est de constater la difficulté des démarches judiciaires pour lever l'anonymat d'auteurs d'infractions, particulièrement lorsque l'opérateur est installé à l'étranger[1427]. En réaction à cette complexe coopération, la solution serait d'imposer aux opérateurs des grandes plateformes numériques de disposer d'un représentant légal en France auprès duquel effectuer ces réquisitions judiciaires plus efficacement. Le nouvel article 6-3 de la LCEN prévoirait ainsi l'obligation pour les opérateurs des plateformes d'échange de désigner « *un représentant légal, personne physique située sur le territoire français exerçant*

[1425] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 2, futur article 6-3 2° de la LCEN.
[1426] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 2, futur article 6-3 5° a) et b) de la LCEN.
[1427] V. *supra* n[os] 378 et 379.

les fonctions d'interlocuteur référent sur le territoire français pour l'application de l'article 6-2 et du présent article. Ce représentant légal est chargé de recevoir les demandes de l'autorité judiciaire en vertu de l'article 6 de la présente loi et les demandes du Conseil supérieur de l'audiovisuel en vertu de l'article 17-3 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication »[1428].

535. Transparence, corollaire essentiel de la surveillance. Outre une surveillance renforcée à l'égard des contenus haineux et une meilleure coopération avec l'autorité judiciaire, cette nouvelle catégorie d'acteur implique en complément une obligation de transparence sur la politique de lutte contre les contenus illicites mise en œuvre. Le législateur propose en l'occurrence au nouvel article 6-3 de la LCEN une série d'obligations de transparence à la charge des opérateurs des grandes plateformes numériques. Ces derniers doivent notamment mettre à disposition une information publique, claire et détaillée, facilement accessible et visible permettant d'informer leurs utilisateurs sur les dispositifs de recours, internes et judiciaires, ainsi que sur les délais impartis pour ces recours dont disposent les victimes de contenus haineux[1429]. Ce devoir d'information porte également sur les sanctions que leurs utilisateurs encourent en cas de publication de contenus haineux[1430]. Mais surtout, ce nouveau régime de responsabilité instaure un devoir d'information des opérateurs sur les modalités générales du dispositif qu'ils mettent en place dans leur activité de modération des contenus. Sur ce point, il leur est imposé de rendre compte des moyens humains et technologiques qu'ils mettent en œuvre et des procédures qu'ils adoptent pour se conformer à leur obligation de modération des contenus[1431]. Afin de compléter cette dernière obligation, il est prévu que les opérateurs des plateformes numériques remettent un rapport annuel de transparence sur la lutte contre les contenus illicites et sur le traitement des signalements et notifications reçues. Cette obligation se justifie du fait de la nature de l'obligation de surveillance qui ne serait qu'une obligation de moyens. Ce compte-rendu

[1428] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 3, futur article 6-3 10° de la LCEN.
[1429] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, futur art. 6-3 a) de la LCEN.
[1430] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, futur art. 6-3 b) de la LCEN.
[1431] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, futur art. 6-3 c).

aurait notamment pour but de contrôler le respect de l'obligation de surveillance demandée aux opérateurs des principaux réseaux sociaux[1432].

2) Des obligations visant une liste limitative d'infractions

536. Une nécessaire liste restreinte d'infractions. La sauvegarde de l'ordre public admet des restrictions aux libertés uniquement dans la mesure où celles-ci sont indispensables à la coexistence des droits et libertés. Ainsi, la régulation à l'échelle numérique ne doit pas organiser un déséquilibre entre la préservation de l'ordre public et des libertés en restreignant au-delà du strict nécessaire l'exercice de droits ou libertés[1433]. En l'occurrence, de manière à rendre l'ensemble de ces obligations à la fois réalisables pour les plateformes numériques et également respectueuses du droit à la liberté d'expression, il est indispensable de circonscrire de la manière la plus restrictive possible les contenus visés par ce nouveau régime de responsabilité. Seules certaines infractions particulièrement graves prévues par le Code pénal ou par la loi sur la liberté de la presse doivent entrer dans ce régime de responsabilité renforcé. Ce *corpus* d'infractions définirait en l'occurrence les contours du noyau dur de l'ordre public numérique justifiant un pouvoir régulateur en matière d'expression à la charge des grandes plateformes numériques.

537. L'identification des infractions visées par le nouveau régime de responsabilité. Dans le souci d'apporter une cohérence d'ensemble à la LCEN, le nouveau système de responsabilité applicable aux « *accélérateurs de contenus* » reprend comme socle du régime d'obligation renforcées, les infractions définies à l'article 6, I, 7° de la loi. Sont alors comprises dans ce nouveau système de responsabilité, les infractions sanctionnant les troubles à l'ordre public résultant soit d'un discours[1434], soit de la diffusion d'images ou de vidéos[1435],

[1432] Le rapport « *Renforcer la lutte contre le racisme et l'antisémitisme* » précise une série d'éléments pouvant relever *a minima* de cette obligation : « *La description des mécanismes de notification des contenus et les critères appliqués pour décider s'il faut informer les autorités publiques compétentes d'un contenu ou d'une activité illicite ; Le nombre de retraits de contenus et de blocage à leur accès selon les mêmes critères d'origine, de motifs, et de durées ; Le nombre de notifications effectuées dans le 12 derniers mois en fonction de l'origine de la notification (utilisateurs, plateformes, associations), les motifs des notifications, et la durée de traitement des notifications par la plateformes ; Le nombre d'activités illicites portées à connaissance de l'autorité publique, selon les mêmes critères d'origine, de motifs et de durée ; Des informations portant sur l'organisation des unités traitant des signalements, le nombre de personnes qui y sont affectées, les formations juridiques et en langue et culture française qui leur sont le cas échéant dispensées, le mode de recours à des spécialistes en expertise linguistique, la mise à disposition de supports techniques ; le nombre de contenus retirés par des moyens d'intelligence artificielle, ainsi que le taux de faux-positifs* ». K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, *op. cit.*, recommandation n° 3, p. 18.

[1433] P. GERVIER, « L'ordre public et le numérique », *Politeia* n° 31, *Les métamorphoses des droits fondamentaux à l'ère du numérique*, 2017, p. 187.

[1434] Pour rappel : l'apologie de crimes de guerre et des crimes contre l'humanité (L. 29 juillet 1881, art. 24, al. 5) ; la diffusion de contenus provoquant à la discrimination, à la haine ou à la violence à l'égard d'une

mais également les infractions rajoutées à la liste des contenus « *odieux* » par les lois du 13 avril 2016[1436] et du 3 août 2018[1437] autrement dit, les infractions de lutte contre la traite des êtres humains[1438] et contre le proxénétisme[1439] ainsi que le délit d'harcèlement sexuel[1440]. En plus du renvoi aux infractions définies à l'article 6, I, 7° le législateur a également choisi d'étendre le régime des obligations renforcées aux injures aggravées mentionnées aux troisième et quatrième alinéas de l'article 33 de la loi du 29 juillet 1881 sur la liberté de la presse[1441].

538. Un champ d'application trop étendu. Ce champ d'application dépasse en réalité largement les seuls discours haineux. Ce nouveau régime d'obligation vise un ensemble hétéroclite d'infractions protégeant des valeurs sociales bien différentes. Fait ainsi partie du champ d'application le délit prévu à l'article 227-24 du Code pénal visant principalement les « *messages à caractère violent, incitant au terrorisme, pornographie ou de nature à porter gravement atteinte à la dignité humaine […] lorsque ce message est susceptible d'être vu par un mineur* ». Cette infraction ne relève ni de la pédopornographie, ni du discours de haine, elle ne sanctionne pas non plus la publication de contenus illicites mais davantage les conditions de leur diffusion. La présence de cette infraction dans le champ d'application du système de responsabilité mis en place à l'encontre des grandes plateformes numériques risque alors « *de vider internet des contenus licites pour le majeur au nom de l'impératif de protection du mineur* »[1442]. De même, nombre d'infractions, très loin de viser des discours haineux stigmatisant des groupes d'individus, sanctionnent en réalité des atteintes particulières à des personnes déterminées tels que les délits de proxénétisme ou d'harcèlement sexuel.

---

personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap (L. 29 juillet 1881, art. 24, al. 8) ; les provocations et apologies du terrorisme (C. pén., art. 421-2-5).

[1435] Pour rappel : la diffusion d'images pédopornographiques (C. pén., art. 227-23) ; la diffusion de messages violents, pornographiques ou de nature à porter gravement atteinte à la dignité humaine ou à inciter les mineurs à se livrer à des jeux les mettant physiquement en danger accessibles aux mineurs, lorsque ces contenus sont susceptibles d'être vus ou perçus par un mineur (C. pén., art. 227-24).

[1436] L. n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées, *JORF* n° 0088, 14 avril 2016.

[1437] L. n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, *JORF* n° 0179, 5 août 2018.

[1438] C. pén., art. 225-4-1.

[1439] C. pén., art. 225-5 et 225-6.

[1440] C. pén., art. 222-33.

[1441] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, futur art. 6-2, I.

[1442] B. NICAUD, « Proposition de loi contre la "cyberhaine" adoptée à l'Assemblée ou l'enfer pavé de bonne (?) intentions », Lexbase Pénal Édition n° 18, 18 juillet 2019.

539. Une nécessaire restriction du champ d'application de la loi. Ce manque de cohérence de l'ensemble des infractions visées par ce nouveau régime d'obligation contribue à sur-responsabiliser les opérateurs des sites de réseaux sociaux au risque d'entraîner une suppression conservatoire des contenus qui leur seraient signalés. De manière à donner une véritable portée aux obligations renforcées conférées aux grandes plateformes numériques, il est nécessaire de restreindre la liste des infractions aux seules infractions venant réprimer des discours haineux, véritables épicentre de la réforme engagée. Selon le Conseil des ministres du Conseil de l'Europe la notion de discours haineux recouvre « *toutes formes d'expression qui propagent, incitent à, promeuvent ou justifient la haine raciale, la xénophobie, l'antisémitisme ou d'autres formes de haine fondées sur l'intolérance, y compris l'intolérance qui s'exprime sous forme de nationalisme agressif et d'ethnocentrisme, de discrimination et d'hostilité à l'encontre des minorités, des immigrés et des personnes issues de l'immigration* »[1443]. Partant de cette définition, Madame Nathalie Droin considère que les discours de haine regroupent « *les propos racistes et antisémites, mais également d'autres discours, discriminatoires ou ségrégationnistes, tels les propos sexistes, homophobes ou encore handiphobes* »[1444]. D'un point de vue pénal, l'auteur en déduit dès lors que ces discours correspondent aux délits de diffamations[1445], injures[1446] et provocations[1447] à la discrimination, à la haine et à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée mais également à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap. Par ailleurs, au vu de l'objectif de préservation de l'ordre public numérique et par là même, de la paix sociale poursuivi par le législateur, il serait également légitime d'inclure dans cette liste exhaustive d'infractions, les provocations et apologies du terrorisme[1448] ainsi que l'apologie de crimes de guerre et des crimes contre l'humanité[1449]. Cette restriction du champ d'application de la loi aurait le mérite de focaliser l'attention des opérateurs sur une liste plus restreinte de comportements nécessitant un devoir de vigilance particulier et une prompte réaction. Ceci ne

[1443] Conseil de l'Europe, Comité des ministres, Du comité de ministres aux États membres sur le « discours de haine », Recommandation n° R(97)20 adoptée le 30 octobre 1997, p. 107.
[1444] N. DROIN, « L'appréhension des discours de haine par les juridictions françaises : entre travail d'orfèvre et numéro d'équilibriste », *RevDH*, n° 14, 21 juillet 2018.
[1445] L. 29 juillet 1881 sur la liberté de la presse, art. 32, al. 2 et 3.
[1446] L. 29 juillet 1881 sur la liberté de la presse, art. 33, al. 3 et 4.
[1447] L. 29 juillet 1881 sur la liberté de la presse, art. 24, al. 7 et 8.
[1448] C. pén., art. 421-2-5.
[1449] L. 29 juillet 1881, art. 24, al. 5.

résoudrait toutefois pas la problématique liée à la difficulté d'appréciation du caractère illicite ou non de ce type d'infractions.

B. Une nécessaire obligation de loyauté associée aux algorithmes de traitement

540. Justification d'une telle obligation. L'encadrement des algorithmes apparaît aujourd'hui comme une nécessité bien que certains arguments s'y opposent, notamment l'idée selon laquelle il ne faut pas entraver l'innovation par un système de normes inadaptées à un univers fondamentalement nouveau. Le risque est d'imposer des règles qui se révéleraient nécessairement inadaptées et vouées à être rendues rapidement caduques en raison de l'évolution rapide de ces nouvelles technologies. Toutefois, il est une chose que le droit ne freine pas l'évolution technologique, il en est une autre que l'évolution technologique se fasse dans le respect des droits et libertés fondamentaux. Sur ce point, l'autogestion accordée à des opérateurs privés a déjà démontré les carences et limites qu'elle impliquait[1450]. Le caractère particulièrement sensible de certains secteurs tels que le secteur militaire, la justice ou le secteur médical justifie même une réflexion sur l'interdiction des algorithmes et de l'intelligence artificielle. La problématique de l'usage d'algorithme dans la mise en avant de contenus par des plateformes de réseaux sociaux apparaît cependant d'une sensibilité moins évidente que les domaines précités. Cela n'empêche pas certains observateurs de prendre position pour une interdiction de telle pratiques y compris dans ce domaine[1451]. N'allant pas jusque dans une telle démarche qui serait contreproductive à l'égard de l'avancée technologique, il est question de proposer non pas une interdiction mais un encadrement de l'usage des algorithmes applicable à cette nouvelle catégorie juridique d'acteurs. Cet encadrement visant à favoriser un développement des sites de réseaux sociaux respectueux des droits et libertés fondamentaux. Le Conseil National du Numérique a rappelé à ce sujet qu'« *il s'agit de prévenir l'asphyxie du système face aux phénomènes oligopolistiques de multinationales dont le poids s'approche ou dépasse celui d'un État, mais dont les valeurs ne*

[1450] V. *supra*, Partie 2, Titre 2, Chapitre 1, Section 2.

[1451] V. notamment les propos de Monsieur Serge Tisseron qui défend une interdiction du ciblage personnalisé dans le domaine publicitaire et culturel. Propos recueillis *in* : « Les publicités ciblées, c'est la bêtise assurée, interdisons-les ! », *Huffington Post*, 26 septembre 2017.
<http://www.huffingtonpost.fr/serge-tisseron/les-publicites-ciblees-cest-la-betise-assuree-interdisons-les_a_23220999/> (dernière consultation le 9 octobre 2019).

comprennent pas nécessairement des impératifs d'intérêt général ni des conditions de maintien de soutenabilité »[1452].

541. Les dispositions contenues dans la loi informatique et libertés et reprises dans le RGPD. La loi informatique et libertés a textualisé dès 1978 un certain nombre de dispositions de nature à encadrer les algorithmes qui sont dorénavant reprises dans le RGPD. La première disposition apparaît sous forme de principe général énoncé à l'article premier de la loi informatique et liberté : « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». Selon ce principe, l'informatique doit en tout état de cause s'exercer dans l'intérêt et le respect des droits du citoyen. Cette règle générale induit une série de sous-principes[1453]. Le premier concerne non pas le traitement algorithmique en tant que tel mais l'encadrement de l'utilisation des données personnelles nécessaires au fonctionnement des algorithmes. Autrement dit, il s'agit de l'encadrement des conditions dans lesquelles sont collectées les données, cela fait référence aux principes de finalité, de proportionnalité, de sécurité et de limitation de la durée de conservation des données. Selon un deuxième principe, un traitement automatisé de données ne peut prendre seul, c'est-à-dire sans intervention humaine, des décisions affectant de manière significative les personnes[1454]. Enfin, un troisième principe érige le droit pour les personnes d'obtenir, auprès de celui qui en est responsable, des informations sur la logique de fonctionnement de l'algorithme[1455].

542. Les dispositions de la loi pour la République numérique. La loi du 7 octobre 2016 est venue rajouter une disposition dans le Code de la consommation selon laquelle : « *Tout*

[1452] CNNum, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, ministère de l'économie du redressement productif et du numérique, mai 2014, p. 19.

[1453] V. CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017, p. 45.

[1454] Ce principe se retrouve d'une part à l'article 10 de la loi informatique et libertés selon lequel : « *Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage* ». Ce principe se retrouve également à l'article 22 du RGPD qui dispose : « *La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ».

[1455] L'article 39 5° de la loi informatique et libertés consacre ainsi le droit pour toute personne physique d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : « *les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé* ». Dans la même logique l'article 15.1 (h) du RGPD précise que la personne concernée a le droit d'obtenir du responsable du traitement l'accès aux informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur : 1° les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ; 2° l'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne »[1456]. Ainsi, depuis cette réforme, les plateformes qui utilisent des algorithmes dans le classement ou le référencement de leurs contenus ont l'obligation de procéder par eux-mêmes à la révélation des principaux facteurs influant sur leur sélection de l'information[1457]. Plus encore, la loi pour la République numérique prévoit que les codes sources des algorithmes utilisés par l'administration sont des informations qui doivent désormais figurer en open source[1458]. Cette transparence totale n'a cependant été envisagée que pour certaines administrations, le secteur privé n'étant pas concerné par cette obligation.

543. Les récentes réformes viennent conforter les dispositions préexistantes, à l'image des dispositions de la loi informatique et libertés retranscrites dans le RGPD mais également, proposer de nouvelles obligations entourant l'utilisation des algorithmes. Afin de développer cet encadrement juridique encore embryonnaire, il est opportun de proposer le développement d'une obligation de loyauté applicable aux traitements algorithmiques mis en œuvre par les opérateurs des réseaux sociaux. Dans son étude annuelle de 2014 le Conseil d'État a formulé un principe de « *loyauté* » applicable aux plateformes numériques mettant en œuvre des algorithmes dans le traitement de leurs contenus[1459]. Ce principe ensuite été repris par la CNIL comme un principe fondateur devant entourer le développement des algorithmes et de

[1456] Art. L. 111-7 C. conso. dans sa rédaction issue de la loi n° 2016-1321 du 7 octobre 2016.
[1457] E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, p. 212, n° 173.
[1458] La loi n° 2016-1321 du 7 octobre 2016 a notamment créé l'article L312-1-3du Code des relations entre le public et l'administration selon lequel : « *Sous réserve des secrets protégés en application du 2° de l'article L. 311-5, les administrations mentionnées au premier alinéa de l'article L. 300-2, à l'exception des personnes morales dont le nombre d'agents ou de salariés est inférieur à un seuil fixé par décret, publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles* ».
[1459] Selon le Conseil d'État : « *Les plateformes, qui constitueraient une nouvelle catégorie juridique, seraient quant à elles soumises à une obligation de loyauté, consistant à assurer de donne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs* ». CE, *Le numérique et les droits fondamentaux*, étude annuelle 2014, p. 26.

l'intelligence artificielle[1460]. Le législateur n'a toutefois pas suivi cette dynamique et ne prévoit pour l'heure aucune obligation particulière en la matière. Il serait pourtant opportun de proposer deux obligations à la charge des grandes plateformes numériques : d'une part une obligation de transparence sur le fonctionnement de l'algorithme (1) et d'autre part, l'obligation de mettre en œuvre un algorithme défendant l'intérêt de l'utilisateur (2).

1) La transparence sur le fonctionnement de l'algorithme

544. Une obligation positive d'information des utilisateurs. De manière générale les informations concernant l'algorithme doivent être fournies de manière loyale et le comportement de l'algorithme doit y correspondre. Loi informatique et libertés concevait pour sa part l'information sur le fonctionnement de l'algorithme comme un droit pouvant être éventuellement mobilisé par les utilisateurs. La logique est aujourd'hui différente, il ne s'agit plus d'accorder un droit de regard aux utilisateurs mais davantage une obligation positive d'information à la charge des plateformes. L'information doit ainsi d'emblée être diffusée à destination de la communauté des utilisateurs.

545. Un rapport de transparence remis à l'autorité de contrôle. Selon l'obligation actuelle établie par la loi pour la République numérique, les plateformes sont tenues de préciser les critères de fonctionnement de leurs algorithmes. Cependant, seule une partie des éléments entrant en jeu dans la sélection des contenus mis en avant est connue. Les algorithmes des principales plateformes internet demeurent alors « *de grands mystères* »[1461]. En réalité, il est impossible de s'assurer de la neutralité de l'algorithme par rapport au fond des messages qu'il manipule dès lors que leur code source reste inconnu[1462]. Il s'agirait dans ce cas d'imposer aux plateformes numériques une obligation de transparence étendue en y incluant le devoir de remettre à l'autorité chargée de leur contrôle, un rapport concernant le fonctionnement de leurs algorithmes. Cela permettrait ainsi d'exercer une surveillance de leur politique éditoriale sans pour autant imposer la divulgation au grand public des secrets de fabrication de leurs algorithmes relevant du secret industriel.

[1460] CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, rapport de synthèse du débat public sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, décembre 2017, p. 48.

[1461] F. ROPARS, « Comment fonctionne l'algorithme Facebook ? », *Blog du modérateur*, 3 mai 2017. <https://www.blogdumoderateur.com/algorithme-facebook-fonctionnement> (dernière consultation le 9 octobre 2019).

[1462] E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, p. 208, n° 170.

2) La mise en œuvre de l'algorithme dans l'intérêt des utilisateurs

546. La notion d' « *intérêt des utilisateurs* ». Il n'est pas suffisant que l'algorithme « *dise ce qu'il fasse et fasse ce qu'il dise* » pour parvenir à un traitement loyal de l'information, il est également essentiel que l'algorithme agisse dans « *l'intérêt des utilisateurs* »[1463]. Selon le Conseil d'État, « *la loyauté consiste à assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs* »[1464]. Le principe de loyauté limite en conséquence la liberté que le responsable de l'algorithme a de déterminer les critères de fonctionnement de ce dernier. La notion d'intérêt des utilisateurs doit en l'occurrence être entendue dans un sens large. Il ne s'agit pas de préserver la seule dimension commerciale et économique de cet intérêt mais également sa dimension collective. Les critères de l'algorithme doivent ainsi ne pas entrer trop frontalement en opposition avec certains grands intérêts collectifs comme l'exposition à la diversité culturelle ou d'opinion[1465].

547. La neutralité de l'algorithme. Plus encore, l'intérêt des utilisateurs impliquerait un devoir de neutralité de l'algorithme. La « *neutralité du web* » est un concept formulé pour la première fois en 2003 par le juriste américain Tim Wu[1466]. Selon ce dernier, tous les opérateurs de communications doivent traiter de manière égale tous les flux de données quel que soit leur contenu. Elle correspond à l'architecture originelle d'internet et repose sur la règle du « *meilleur effort* » selon laquelle : chaque opérateur fait de son mieux pour assurer la transmission de tous les paquets de données qui transitent par son réseau, sans garantie de résultat et sans discrimination[1467]. Ce principe de neutralité appliqué aux sites de réseaux sociaux induirait la proposition d'un tri alternatif des contenus, en l'occurrence un tri qui ne serait pas personnalisé. Le réseau social offrirait alors, en parallèle de son algorithme classique, une vue exhaustive et purement chronologique des publications opérées par les contacts de l'utilisateur. Selon Monsieur Emmanuel Netter, « *Cela permettrait aux utilisateurs, sans les y contraindre, de procéder par comparaison entre les résultats filtrés et les résultats bruts. Ils verraient à l'œuvre les forces qui modèlent l'information dont ils sont consommateurs au quotidien. Libres à eux, ensuite, de retourner vers le confort d'un monde*

[1463] CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.*, p. 48.
[1464] CE, *Le numérique et les droits fondamentaux*, étude annuelle 2014, pp. 273 et 278-281.
[1465] CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, *op. cit.*, p. 49.
[1466] T. WU, « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, Vol. 2, 2003, p. 141.
[1467] CE, *Le numérique et les droits fondamentaux*, étude annuelle 2014, pp. 11-12.

entièrement conçu à partir de leurs désirs, ou de dégonfler un peu la « bulle *» de subjectivité qui les entoure, faute de pouvoir jamais la percer* »[1468]. Plus loin encore, la plateforme pourrait proposer à ses utilisateurs que ces derniers sélectionnent eux-mêmes les critères sur lesquels ils souhaitent baser le tri de l'information de manière à personnaliser le traitement de leurs contenus.

548. La mise en place d'outils de transparence en matière d'algorithmes. Pour connaître et surveiller le fonctionnement intime de leurs algorithmes, le Conseil national du numérique préconise par ailleurs la création d'agences de notation pour mesurer les niveaux de neutralité des plateformes. Selon ce dernier, ces agences pourraient prendre plusieurs formes : publiques, privées, associatives ou basées sur la société civile[1469]. Leurs missions seraient de révéler les pratiques des plateformes et d'éclairer les usagers dans l'utilisation de leurs services. Dans cette même dynamique, un rapport du Conseil général de l'économie propose de « *créer une plateforme collaborative scientifique, destinée à favoriser le développement d'outils logiciels et de méthodes de test d'algorithmes* », mais aussi de « *créer une cellule de contrôle spécialisée "bureau des technologies de contrôle de l'économie numérique", pour l'ensemble des pouvoirs publics, implantée au sein de la DGCCRF* »[1470].

549. Conclusion de la Section 1. Responsabiliser davantage les sites de réseaux sociaux implique, au vu de leurs spécificités, l'adoption d'un nouveau statut juridique s'insérant entre le statut des éditeurs de contenus et des hébergeurs. Ce nouveau statut justifie l'adoption d'obligations à la mesure de l'impact et du rôle joué par ces grandes plateformes, « *nouveaux empires industriels de notre époque* »[1471]. En conséquence, le législateur propose la mise en place d'un nouveau régime de responsabilité propre à la catégorie particulière des « *accélérateurs de contenus* » prévoyant un renforcement des obligations de ces nouveaux acteurs sur la base des obligations prévues initialement pour les hébergeurs. Ainsi, dans l'optique de lutte contre les contenus haineux en ligne, les opérateurs des réseaux sociaux visés par ce régime sont contraints à une obligation de surveillance ciblée et non temporaire de ce type particulier de contenus s'accompagnant d'un devoir de transparence et de coopération accru à l'égard de l'autorité publique. Mais surtout, il est introduit une obligation

[1468] E. NETTER, *Numérique et grandes notions du droit privé*, mémoire HDR soutenu le 20 novembre 2017, p. 213, n° 173.
[1469] CNNum, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, ministère de l'économie du redressement productif et du numérique, mai 2014, p. 11.
[1470] Ministère de l'économie de l'industrie et du numérique, Modalités de régulation des algorithmes de traitement des contenus, rapport à Mme la Secrétaire d'État chargée du numérique, 13 mai 2016.
[1471] C. FÉRAL-SCHUHL, *Cyberdroit. Le droit à l'épreuve de l'internet*, 7ème éd., Dalloz, 2018-2019, p. 1423, n° 626.11.

de réactivité renforcée des opérateurs suite à un signalement ou à une notification de contenus, prévoyant notamment un court délai de réaction de 24 heures pour les contenus manifestement illicites. Toutefois, au regard de ce régime renforcé d'obligations, il est regrettable qu'aucune disposition particulière ne soit émise concernant l'encadrement de l'usage des algorithmes de traitements au vu de leur rôle dans la mise en avant des contenus haineux. Il serait alors opportun de développer une obligation de loyauté à la charge de ces plateformes qui induirait une transparence sur leur fonctionnement mais également un pouvoir d'action de l'utilisateur sur la mise en visibilité des contenus et *a fortiori* sur les algorithmes.

550. Plus généralement, si l'adoption d'un tel régime de responsabilité au sein de la LCEN apparaît comme une évolution souhaitable au regard de la lutte contre les discours haineux, ce dernier ne doit cependant pas mettre en œuvre un système qui aboutirait *in fine* à un recul des droits et libertés, particulièrement la liberté d'expression et plus encore, la liberté d'opinion. En l'occurrence le champ d'application trop étendu du régime de responsabilité et le délai de réaction raccourci peuvent faire craindre une telle dérive. Il serait dans ce cas souhaitable de restreindre les infractions visées par le nouvel article 6-2 de la LCEN aux seuls contenus haineux ou faisant l'apologie du terrorisme. De même, une plus grande souplesse dans le délai de réaction de l'opérateur s'accorderait davantage avec la difficulté d'apprécier si un contenu relève à juste titre d'une qualification pénale strictement encadrée ou alors s'il ne constitue qu'un discours choquant s'inscrivant dans la liberté d'opinion de son auteur.

Section 2 : L'identification des acteurs de l'encadrement des réseaux sociaux

551. Une réussite de ce nouveau statut juridique dépendante de son effectivité. L'introduction au sein de la LCEN d'un nouveau régime juridique correspondant à une nouvelle catégorie d'acteurs resterait vaine s'il n'était pas prévu l'intervention d'un acteur tiers veillant au bon respect de ces obligations renforcées. Cet acteur prendrait en l'occurrence la forme d'une autorité administrative indépendante (**§1**). Cependant, la garantie de l'effectivité d'un tel régime de responsabilité doit également provenir de l'intérieur du réseau social lui-même, autant de ses opérateurs que de ses utilisateurs. Ces acteurs privés ayant un rôle fondamental à jouer dans le développement d'une régulation collaborative (**§2**).

§1. La nécessaire intervention d'un acteur tiers : une autorité de contrôle

552. La nécessaire intervention d'une autorité publique. L'introduction d'un nouveau régime de responsabilité plus engageant que celui actuellement applicable aux hébergeurs n'est pas gage d'une meilleure effectivité des obligations à la charge des opérateurs des réseaux sociaux. Il est par ailleurs indispensable d'assurer une véritable mise en œuvre d'un tel régime notamment par l'instauration d'une autorité de contrôle chargée de veiller au respect de ces nouvelles obligations. En l'occurrence, de nombreuses autorités indépendantes jouent déjà un rôle dans la régulation des sites de réseaux sociaux[1472], cependant aucune d'entre elles n'est compétente pour contrôler le respect des obligations prévues par la LCEN. Les opérateurs des réseaux sociaux régulent en conséquence seuls les contenus gravitant sur leurs plateformes[1473]. Il est ainsi devenu nécessaire d'introduire une autorité tierce chargée de veiller spécialement au respect des dispositions de la LCEN pour assurer une meilleure régulation dans ce domaine qui relève d'une particulière délicatesse. Cette nécessité juridique s'est transformée en volonté politique en Allemagne avec la loi *NetzDG* entrée en vigueur le 1er janvier 2018[1474] suivie en France par la proposition de loi visant à lutter contre la haine sur

[1472] Il existe un nombre important d'autorité ayant vocation à réguler l'espace numérique y compris les réseaux sociaux, on peut citer entre autres : la CNIL, le CSA, la DGCCCRF, l'ARJEL, l'ARCEP, l'HADOPI, la DILCRAH, la CNCDH. V. : K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018, p. 26.
[1473] V. *supra*, Partie 2, Titre 2, Chapitre 1, Section 2.
[1474] Loi *Netzwerkdurchsetzungsgesetz*, ou *NetzDG*, entrée en vigueur le 1er janvier 2018. Consultable sur <https://www.gesetze-im-internet.de/netzdg/index.html>.

internet[1475] se basant sur le rapport « *renforcer la lutte contre le racisme et l'antisémitisme* »[1476] remis au Premier ministre le 20 septembre 2018.

553. Justification d'un tel encadrement : les réseaux sociaux, des entreprises cruciales. L'immixtion d'une autorité dans le fonctionnement des sites de réseaux sociaux est d'autant plus justifiée que ces derniers peuvent être assimilés à des « *entreprises cruciales* »[1477]. Dans sa conception positive[1478], l'entreprise cruciale correspond à l'entreprise dont la présence est requise pour que l'espace « *fonctionne comme il convient qu'il fonctionne* ». Autrement dit, à l'inverse des banques ou des établissements financiers, ce n'est pas la défaillance de cette entreprise qui est redoutée mais au contraire son succès qui constitue une perspective dont l'État doit se mêler. Cette conception positive de l'entreprise cruciale est en conséquence plus subjective et donc de nature plus politique que la définition négative. La conception positive invite l'État à se positionner de lui-même sur les secteurs où il juge son intervention nécessaire à la défense de l'intérêt commun. L'enjeu consiste alors à identifier les entreprises cruciales qui assurent le fonctionnement de nos sociétés et dont leur régulation garantirait le respect des principes fondamentaux défendus par l'État[1479]. À ce titre, les principaux réseaux sociaux constituent ces entreprises cruciales tant ils possèdent un impact sociétal majeur et tant ils sont devenus un acteur démocratique essentiel par leur monopole de l'exercice de la liberté d'expression dans l'espace numérique. Ce statut justifie la mise en place d'un encadrement visant à garantir l'exercice des droits et des libertés. Après avoir identifié l'acteur en charge de l'encadrement des réseaux sociaux (A), il sera question d'analyser l'étendue des nouveaux pouvoirs pouvant lui être conférés (B).

[1475] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019.

[1476] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, *op. cit*.

[1477] Cette catégorie particulière d'acteurs a été identifiée par le Professeur Marie-Anne Frison-Roche. V. M.-A. FRINSON-ROCHE, « Réguler les "entreprises cruciales" », *D.* 2014, p. 1556.

[1478] Par opposition à la conception positive, le Professeur Marie-Anne Frison-Roche, considère que dans une définition négative, la faillite d'une entreprise cruciale entraîne la défaillance des autres établissements, puis la déconfiture du système financier dans son entier, lequel fait s'écrouler l'économie. C'est le cas particulièrement des banques et des établissements financiers. M.-A. FRINSON-ROCHE, « Réguler les "entreprises cruciales" », *D.* 2014, p. 1556.

[1479] « *La dimension politique de la définition positive de l'entreprise cruciale ressort lorsque l'État manifeste son souci du groupe social dont il a la charge, par exemple le souci de la santé publique, de la préservation des données sensibles, des libertés, du respect des personnes. L'État est en droit d'affirmer ce souci politique en l'exprimant à l'intérieur même des entreprises opérant sur les secteurs cruciaux, quand bien même il n'est pas actionnaire de ces entreprises* ». M.-A. FRINSON-ROCHE, « Réguler les "entreprises cruciales" », *D.* 2014, p. 1556.

A. Identification de l'acteur en charge de l'encadrement : le CSA

554. Une autorité administrative indépendante. Il est question de proposer la mise en place d'une autorité investie d'un pouvoir de régulation de l'expression dans l'espace numérique. La notion d'autorité de régulation est toutefois largement doctrinale et se retrouve peu en droit positif[1480], un auteur soutient même que cette notion serait inexistante[1481]. Les autorités de régulation appartiennent en réalité à des catégories d'institutions préexistantes. En France elles correspondent aux autorités administratives indépendantes (AAI) et forment une catégorie à part entière au sein de l'ordre juridique français. Leur origine se trouve dans la création en 1978 de la Commission Nationale de l'Informatique et des Libertés (CNIL)[1482]. Si la définition de ces acteurs n'est pas aisée[1483], il est toutefois communément admis par une définition large qu'il s'agit « *d'autorités publiques chargées d'assurer la régulation de secteurs sensibles de la vie sociale* »[1484]. Plus précisément, Madame Aurélie Cappello propose de définir les autorités administratives indépendantes comme « *des autorités agissant au nom de l'État de manière autonome, c'est-à-dire sans être subordonnées au Gouvernement ou au Parlement, mais soumises au contrôle du juge, et susceptibles d'intervenir dans trois domaines distincts : la régulation d'un secteur économique, la protection des libertés, le fonctionnement des relations entre l'administration et les administrés* »[1485].

555. Une autorité existante : le CSA. Il s'agit dès lors de déterminer quelle autorité administrative indépendante aurait la charge de la régulation de l'expression sur les grandes plateformes numériques. Suivant le constat de la prolifération des autorités administratives indépendantes[1486] il est préférable de proposer l'extension des compétences d'une autorité existante plutôt que la création d'une nouvelle autorité *ad hoc*. En l'occurrence, le Conseil

[1480] T. PERROUD, *La fonction contentieuse des autorités de régulation en France*, Nouvelle Bibliothèque de Thèses, Dalloz, avril 2013, n° 1, p. 63, n° 56 et suiv.
[1481] G. MARCOU, *La notion juridique de régulation*, *AJDA* 2006, p. 347.
[1482] L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 11 : « *La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante* » (ancien art. 8).
[1483] Le rapport Gérald parle ainsi « *d'objets juridiques non identifiés* ». P. GERALD, *Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié*, Rapport de l'Office parlementaire d'évaluation de la législation n° 404, déposé le 15 juin 2006. Olivier Gohin considère pour sa part que les AAI présentent « *une difficulté conceptuelle certaine* ». O. GOHIN, *Institutions administratives*, LGDJ, 7ème éd., 2016, p. 233. Enfin, le Conseil d'État souligne que la notion n'est pas « *dépourvue d'ambiguïté* ». CE, *Réflexion sur les autoritiés administratives indépendantes*, Rapport public 2001, p. 287.
[1484] J.-P. FELDMAN, « Les autorités administratives indépendantes sont-elles légitimes ? Sur les AAI et générale et le Conseil supérieur de l'audiovisuel en particulier », *D.* 2010, p. 2852.
[1485] A. CAPPELLO, Rép. pén. Dalloz, octobre 2016, *V°* Autorités administratives indépendantes, n° 1.
[1486] V. en ce sens : J. CHEVALLIER, « Le statut des autorités administratives indépendantes : harmonisation ou diversification ? », *RFDA* 2010, p. 896 ; Rapport P. GELARD, *Les AAI : évaluation d'un objet juridique non identifié*, Office parlementaire d'évaluation de la législation, AN n° 3166, Sénat n° 404, 15 juin 2006, p. 9.

Supérieur de l'Audiovisuel (CSA)[1487] apparaît comme l'autorité la plus à même d'endosser cette charge au moyen d'une révision de son statut et particulièrement de l'extension de son champ de compétences. Ceci se justifie dans la mesure où cette autorité semble assurer, dans le domaine de l'audiovisuel, une régulation similaire à celle attendue dans l'espace numérique tant au regard de la teneur de ses missions (1) que du pouvoir de sanction qui lui est conféré (2).

1) Les missions du CSA

556. Le CSA, garant de la liberté de la communication. Créé par la loi du 17 janvier 1989, le CSA a succédé à la Haute Autorité de la communication audiovisuelle (HACA) puis à la Commission nationale de la communication et des libertés (CNCL). Aux termes de la loi du 30 septembre 1986[1488], le CSA a pour mission générale de garantir « *l'exercice de la liberté de communication audiovisuelle* ». Plus précisément, l'article 3-1 alinéa 2 de la loi du 30 septembre 1986 énumère ses différentes missions lui permettant d'atteindre cet objectif : **«** *Il assure l'égalité de traitement ; il garantit l'indépendance et l'impartialité du secteur public de la communication audiovisuelle ; il veille à favoriser la libre concurrence et l'établissement de relations non discriminatoires entre éditeurs et distributeurs de services, quel que soit le réseau de communications électroniques utilisé par ces derniers, conformément au principe de neutralité technologique ; il veille à la qualité et à la diversité des programmes, au développement de la production et de la création audiovisuelles nationales ainsi qu'à la défense et à l'illustration de la langue et de la culture françaises* ».

557. Le CSA, garant de la qualité de la communication. La mission d'assurer la liberté de communication implique nécessairement de garantir la qualité de cette dernière. Le CSA est chargé de veiller au respect de la dignité de la personne humaine et à la sauvegarde de l'ordre public dans les programmes audiovisuels. La loi du 30 septembre 1986 lui donne également compétence pour s'assurer du respect de la déontologie dans les médias audiovisuels. Le respect de cette déontologie se faisant au regard d'autres textes notamment la loi sur la liberté de la presse de 1881 fixant les limites de la liberté d'expression applicables au secteur audiovisuel. À ce titre, la loi du 30 septembre 1986 précise que le CSA doit lutter

[1487] Le CSA est une autorité publique indépendante dont l'indépendance est garantie par l'inamovibilité de ses membres mais également par son absence de rapport hiérarchique avec l'administration et le gouvernement. M. LE ROY, « Le CSA en fait-il trop… ou pas assez ? », *Légipresse* n° 357, février 2018, p. 77.
[1488] L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (ci-après : Loi Léotard), *JORF* 1er octobre 1986, p. 11749.

contre les discriminations tant raciales[1489] que sexistes[1490]. Le CSA garantit en outre la protection de l'enfance et de l'adolescence[1491] à l'égard du caractère violent, sexuel, voire pornographique de certains programmes. Enfin, les missions du CSA précisent que la qualité de la communication passe par le respect d'une expression pluraliste des courants de pensée et d'opinion[1492]. Ce principe vaut particulièrement à l'égard de l'expression dans le domaine politique. Les chaînes doivent ainsi garantir un temps de parole équilibrer pour les membres du gouvernement, les parlementaires liés à la majorité et à l'opposition ainsi qu'aux formations politiques non représentées au Parlement. Cette mission vaut d'autant plus en période électorale.

2) Le pouvoir de sanction du CSA

558. Les dispositions législatives. Le CSA dispose du pouvoir de contrôler le respect par les chaînes de télévision et les stations de radio de différentes obligations légales, réglementaires ou contractuelles. Ce pouvoir de contrôle induit un pouvoir de sanction en cas de non-respect par les entreprises publiques ou privées de radio ou de télévision de certaines de leurs obligations. Concernant les entreprises audiovisuelles du secteur privé le pouvoir de sanction du CSA est prévu aux articles 42 à 42-15 de la loi du 30 septembre 1986, alors que pour les entreprises audiovisuelles du secteur public, le pouvoir de sanction du CSA est régi aux articles 48-1 à 48-10 de la même loi. Dans les deux hypothèses une mise en demeure constitue le préalable nécessaire aux autres mesures de sanctions prononcées par l'autorité, un premier manquement à une obligation ne pouvant à lui seul fonder une sanction. En conséquence, cette dernière ne peut mettre en application son pouvoir coercitif qu'en cas d'un second manquement de même nature que celui qui a fait l'objet d'une première mise en demeure[1493]. Dès lors qu'un tel manquement est constaté, le CSA dispose d'une série de sanctions qu'il peut mettre en œuvre à l'égard de la chaine de télévision ou de la station de radio n'ayant pas satisfait à ses obligations. L'autorité publique indépendante peut ainsi prononcer à l'encontre des entreprises audiovisuelles privées la suspension de la diffusion ou de la distribution du service ou du programme ; la réduction de la durée de l'autorisation ou de la convention dans la limite d'une année, voire le retrait de l'autorisation ou la résiliation

[1489] Loi Léotard, art. 3-1 al. 4.
[1490] Loi Léotard, art. 3-1 al. 5.
[1491] Loi Léotard, art. 15.
[1492] Loi Léotard, art. 13.
[1493] E. DERIEUX, « Le pouvoir de sanction du Conseil supérieur de l'audiovisuel », *LPA* n° 52, 15 mars 2005, p. 3.

unilatérale de la convention ; mais surtout une sanction pécuniaire[1494]. Concernant les entreprises publiques, les sanctions sont peu ou prou identiques à l'exception de celles touchant les autorisations, les entreprises publiques n'y étant pas soumises. Le CSA peut toutefois décider d'une suspension d'une partie du programme ; de l'insertion, dans les programmes d'un communiqué, ou encore d'une sanction pécuniaire[1495]. Les règles fixant le montant de la sanction pécuniaire sont identiques pour les entreprises du secteur privé et public : le montant de la sanction pécuniaire doit être fonction de la gravité des manquements commis et en relation avec les avantages tirés du manquement, sans pouvoir excéder 3 % du chiffre d'affaires réalisé au cours du dernier exercice. Ce maximum est porté à 5 % en cas de nouvelle violation de la même obligation[1496].

559. Exemples de sanctions prononcées par le CSA. Les motifs des sanctions prononcées par le CSA sont multiples : non fourniture des rapports d'activité et des comptes annuels, publicité clandestine, dépassement du temps de publicité, non-respect des quotas d'œuvres européennes ou françaises dans les programmes, entre autres. En réalité, très peu de sanctions concernent le contenu des programmes ou la nature des propos ou images diffusées, ceci s'expliquant par le souci du CSA de ne pas porter atteinte au principe de liberté d'expression dont il est garant[1497]. L'institution n'a toutefois pas hésité à prononcer de lourdes sanctions pécuniaires relatives aux contenus d'émission radio ou télédiffusées. Par exemple, le CSA prononcé une sanction pécuniaire d'un million d'euros contre la station de radio NRJ après la diffusion dans une émission d'un canular téléphonique à l'encontre d'une femme. Les propos qui portaient sur sa vie intime ont été jugés « *avilissant* » ainsi que « *dégradants* »[1498]. L'autorité publique a fait en l'occurrence usage de son pouvoir de sanction afin de satisfaire à son obligation d'assurer « *le respect des droits des femmes dans le domaine de la communication audiovisuelle* »[1499]. Le CSA a également sanctionné de trois millions d'euros la chaîne de télévision C8 pour la diffusion d'une émission où l'animateur avait tenu des

[1494] Loi Léotard, art. 42-1.
[1495] Loi Léotard, art. 48-2 et 48-3.
[1496] Loi Léotard, art. 42-2.
[1497] E. DERIEUX, « Le pouvoir de sanction du Conseil supérieur de l'audiovisuel », *LPA* n° 52, 15 mars 2005, p. 3.
[1498] CSA, ass. plén., décembre du 20 décembre 2017, cité *in* M. LE ROY, « Le CSA en fait-il trop… ou pas assez ? », *Légipresse* n° 357, février 2018, p. 74.
[1499] Le CSA « *veille (…) à l'image des femmes qui apparaît dans ces programmes, notamment en luttant contre les stéréotypes, les préjuges sexistes, les images dégradantes, les violences faites aux femmes et les violences commises au sein des couples. Dans ce but, il porte une attention particulière aux programmes des services de communication audiovisuelle destines à l'enfance et à la jeunesse* ». Art 3, L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard).

propos homophobes, ce dernier ayant eu recours à de nombreux clichés, et attitudes stéréotypées sur les personnes homosexuelles[1500].

560. Un pouvoir de sanction à valeur constitutionnelle. Dans une décision du 17 janvier 1989[1501] le Conseil constitutionnel a admis qu'une autorité dite « *administrative indépendante* » ou « *publique indépendante* » chargée de « *veiller au respect des principes constitutionnels en matière de communication audiovisuelle* » , en l'occurrence le CSA, puisse être investie d'un pouvoir de sanction s'exerçant « *dans la limite nécessaire à l'accomplissement de sa mission* ». Les sages ont cependant tempéré leur analyse dans une décision du 10 juin 2009[1502] venant censurer la loi dite « Hadopi ». Cette dernière souhaitait conférer à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi) un pouvoir de sanction gradué pouvant aller jusqu'à la suspension de l'accès au service internet à l'encontre de l'internaute ayant mis à disposition du public des œuvres protégées par le droit d'auteur. Tout en rappelant que « *le principe de séparation des pouvoirs, non plus qu'aucun principe ou règle de valeur constitutionnelle, ne fait obstacle à ce qu'une autorité administrative […] puisse exercer un pouvoir de sanction dans la mesure nécessaire à l'accomplissement de sa mission* » les juges de la rue Montpensier ont censuré cette disposition en considérant que cette sanction était de nature à limiter l'exercice de la liberté d'expression et ne pouvait dès lors être prononcée par une autorité administrative. En définitive, il ressort de la jurisprudence du Conseil constitutionnel que le pouvoir de sanction d'une autorité administrative doit satisfaire aux conditions suivantes : il doit s'agir d'une autorité administrative agissant dans le cadre de prérogatives de puissance publique, son pouvoir de sanction doit être nécessaire à l'accomplissement de sa mission et enfin, la sanction ne doit pas être de nature à entraîner une privation de liberté[1503]. Le CSA remplit en l'occurrence ces critères lui permettant de détenir légitimement un véritable pouvoir de sanction administrative.

[1500] CSA, décembre n° 2017-532, 26 juillet 2017, portant sanction à l'encontre de la société C8 : *RLDI*, 2017, n° 140, comm. E. DERIEUX.

[1501] Cons. const., 17 janvier 1989, DC n° 88-248, *JO* 18 janvier 1989, p. 754.

[1502] Cons. const., 10 juin 2009, DC n° 2009-580, *JO* 13 juin 2009, p. 9675, Constitutions 2010, p. 97, obs. H. PERINET-MARQUET ; Constitutions 2010, p. 293, obs. D. BELLESCIZE ; *D.* 2009, p. 1770, point de vue J.-M. BRUGUIERE ; *D.* 2009, p. 2045, point de vue L. MARINO ; *D.* 2010, p. 1508, obs. V. BERNAUD et L. GAY ; *RSC* 2009, p. 609, obs. J. FRANCILLON ; *D.* 2010, p. 209, obs. B. LAMY ; *RTD Civ.* 2009. 754, obs. T. REVET ; *RTD Civ.* 2009, p. 756, obs. T. REVET ; *RTD Com.* 2009, p. 730, étude F. POLLAUD-DULIAN.

[1503] A. CAPPELLO, « Retour sur la jurisprudence du Conseil constitutionnel relative aux sanctions administratives », *RSC* 2010, p. 415.

B. L'étendue des nouveaux pouvoirs conférés à l'autorité

561. Au vu de ces pouvoirs actuels en matière d'audiovisuel, il convient d'abord d'étendre les compétences du CSA (1) avant d'étendre ses pouvoirs (2).

1) Des compétences étendues au domaine du numérique

562. Le champ de compétence classique du CSA : la télévision et la radio. L'article 2 de la loi du 30 septembre 1986 circonscrit le champ de compétence du CSA à la communication audiovisuelle. Ce type de communication comprend les communications au public par les services de radio[1504] ou de télévision[1505] mais aussi toutes les communications au public par voie électronique dès lors qu'elles ne relèvent pas de la communication au public en ligne prévue à l'article 1er de la LCEN[1506]. Classiquement, le CSA n'avait vocation à réguler que les éditeurs de services de télévision et de radio et semblait ainsi exclure tout service interactif.

563. Première extension de la compétence du CSA : « *les médias audiovisuels à la demande* ». Cependant, le développement des services à la demande est venu concurrencer les services audiovisuels « *linéaires* »[1507] et a justifié une extension de la compétence du CSA. S'appuyant sur l'arrêt Mediakabel de la CJCE[1508], le parlement a adopté le 11 décembre 2007 la directive « *services de médias audiovisuels* »[1509] incluant désormais les services de « *médias audiovisuels à la demande* ». La loi du 5 mars 2009[1510] est venue modifier l'article 2 de la loi du 30 septembre 1986 pour inclure dans le champ de compétence du CSA « *les*

[1504] « *Est considéré comme service de radio tout service de communication au public par voie électronique destiné à être reçu simultanément par l'ensemble du public ou par une catégorie de public et dont le programme principal est composé d'une suite ordonnée d'émissions comportant des sons* ». Art. 2, al. 5, L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard).

[1505] « *Est considéré comme service de télévision tout service de communication au public par voie électronique destiné à être reçu simultanément par l'ensemble du public ou par une catégorie de public et dont le programme principal est composé d'une suite ordonnée d'émissions comportant des images et des sons* ». Art. 2, al. 4, L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard).

[1506] Aux termes de cet article, « *On entend par communication au public en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur* ».

[1507] P. MOURON, « Et donc une chaîne YouTube est soumise aux pouvoirs de régulation du CSA », *RLDI*, 2017, n° 134, p. 8.

[1508] CJCE, *Mediakabel BV c/ Commissariaat voor de Media*, 3ème ch., 2 juin 2005, aff. C-89/04 : *RLDI*, 2015, n° 9, note M. MORITZ.

[1509] Directive nº 2007/65/CE du Parlement européen et du Conseil du 11 décembre 2007 « *modifiant la directive nº 89/552/CE du Conseil visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à l'exercice d'activités de radiodiffusion télévisuelle, consolidée par la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels, compte tenu de l'évolution des réalités du marché* ».

[1510] L. n° 2009-258 du 5 mars 2009 relative à la communication audiovisuelle et au nouveau service public de la télévision, *JORF* n° 0056 du 7 mars 2009, p. 4321, texte n° 2.

médias audiovisuels à la demande »[1511] définis comme « *tout service de communication au public par voie électronique permettant le visionnage de programmes dont la sélection et l'organisation sont contrôlés par l'éditeur de service* »[1512]. Autrement dit, les services audiovisuels à la demande sont des services non-linéaires où le contenu comme le moment de son visionnage est choisi par l'utilisateur[1513]. La distinction entre « *médias audiovisuels à la demande* » et certains services de « *communication au public en ligne* » n'est cependant pas toujours évidente, au point même de brouiller, si ce n'est effacer les démarcations entre les différents moyens de communication. La porosité de ces frontières s'est vérifiée par une décision du CSA du 13 décembre 2016[1514] dans laquelle l'autorité a adressé une mise en garde à la société *Studio Bagel* pour apologie de l'alcool *via* une de ses chaînes YouTube « *Les recettes pompettes* », disponible en version française depuis avril 2016. L'autorité de régulation de l'audiovisuel a en l'espèce considéré la chaîne comme un service de médias audiovisuels à la demande relevant ainsi son champ de compétence. Le CSA a justifié son interprétation en précisant que, sans égard aux modalités de sa diffusion au public, la chaîne comprend un catalogue de contenus organisés par un éditeur professionnel, dans le cadre d'une activité économique et constitue une offre entièrement autonome de tout autre service. Cette décision ne vise donc pas YouTube directement mais les opérateurs qui fournissent la plateforme de vidéos. Cette dernière marque toutefois une volonté affirmée du CSA d'étendre son champ de compétence y compris dans le secteur numérique.

564. Le nouveau champ de compétence : le numérique. La volonté du CSA d'étendre son champ de compétence au numérique se retrouve déjà dans son rapport de janvier 2013 « *Contribution du Conseil supérieur de l'audiovisuel sur l'adaptation de la régulation audiovisuelle* »[1515] où ce dernier préconise d'étendre ses compétences aux services vidéos en ligne. Le CSA a ainsi marqué le souhait de fixer une corégulation du secteur qui se fonderait sur l'autorégulation de ses acteurs : « *le CSA fixerait le cadre général, mettrait en place un système de labellisation des sites et n'interviendrait qu'en cas d'échec de l'autorégulation* »[1516]. Le président du CSA a réaffirmé cette volonté lors de son discours aux vœux 2018 de l'institution, relevant la nécessité de promouvoir une régulation adaptée au numérique : « *Une régulation étendue aux services audiovisuels numériques tant par son*

[1511] E. DERIEUX, *Droit des médias. Droit français, européen et international*, LGDJ, 7ème éd., p. 157, n° 506.
[1512] L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), art. 2, al. 6.
[1513] Par exemple : MyTF1, 6Play, Netflix, Amazon Prime Vidéos, CanalPlay etc.
[1514] CSA, ass. plén., 16 novembre 2016 : *RLDI*, 2017, n° 134, comm. P. MOURON.
[1515] *Contribution du Conseil supérieur de l'audiovisuel sur l'adaptation de la régulation audiovisuelle*, 24 janvier 2013, disponible sur le site du CSA, v. p. 26.
[1516] *Ibid*, p. 41.

périmètre que par ses méthodes, telle est précisément la perspective de l'année qui s'ouvre, laquelle pourrait constituer un tournant décisif »[1517]. Cette dynamique se retrouve dans la proposition de loi « *visant à lutter contre la haine sur Internet* » donnant au CSA les compétences de contrôler le respect des obligations et de sanctionner tout manquement prévu au nouveau régime de responsabilité applicable aux réseaux sociaux. Ceci implique nécessairement une reconnaissance par la loi de l'extension du champ de compétence du CSA afin que ce dernier puisse veiller au respect des obligations prévues par le nouveau régime de responsabilité applicable aux réseaux sociaux.

2) Des pouvoirs étendus en concurrence avec l'autorité judiciaire

565. Outre l'extension de ses compétences, le CSA doit également disposer de pouvoirs étendus lui permettant d'encadrer les plateformes numériques afin d'assurer l'effectivité de ce nouveau régime de responsabilité. Ses nouveaux pouvoirs doivent s'exercer dans le but d'assurer un meilleur respect des droits et libertés. Il lui est ainsi reconnu un pouvoir de supervision des plateformes numériques dans la régulation des contenus (a). Cependant, les nouvelles attributions du CSA ne doivent pas pour autant constituer une menace pour les droits et libertés, c'est pourquoi son pouvoir de sanction est partagé avec l'autorité judiciaire (b).

a- La supervision des plateformes numériques dans la régulation des contenus

566. Une supervision du CSA dans la régulation des contenus manifestement illicites. La difficulté majeure de la régulation des contenus sur les réseaux sociaux consiste à trouver un juste équilibre entre le respect des exigences européennes en matière de liberté d'expression et l'impératif de lutte contre les discours haineux. Le régime classique de responsabilité des hébergeurs prévu à l'article 6 de la LCEN délègue le pouvoir d'appréciation du caractère manifestement illicite d'un contenu aux opérateurs eux-mêmes. Ainsi, la régulation de la liberté d'expression et en conséquence, la définition de l'ordre public numérique relèvent selon ce régime exclusivement d'acteurs privés[1518]. En réaction, le nouveau régime de responsabilité applicable aux opérateurs des grandes plateformes en ligne confère au CSA les compétences nécessaires pour exercer une supervision de la lutte contre les contenus manifestement illicites. Autrement dit, l'autorité doit accompagner les opérateurs

[1517] Discours d'Olivier Schrameck aux vœux du CSA, 23 janvier 2018, disponible sur le site du CSA.
[1518] V. *supra*, Partie 2, Titre 2, Chapitre 1, Section 2.

dans leur mission de régulation des contenus haineux. Cette extension des missions du CSA aurait la vertu d'introduire un acteur public indépendant en charge de veiller à la bonne interprétation du critère du manifestement illicite et donc de consolider d'une certaine manière l'ordre public numérique. Pour ce faire, le législateur propose d'introduire un nouvel article 17-3 inséré dans la loi n° 86-1067 du 30 septembre 1986[1519] disposant que : « *Le Conseil supérieur de l'audiovisuel veille au respect des dispositions de l'article 6-3 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique par les opérateurs de plateforme en ligne mentionnés au premier alinéa du I de l'article 6-2 de la même loi.* […] *Il s'assure du suivi des obligations reposant sur ces opérateurs* »[1520].

567. Les outils juridiques à disposition du CSA dans son pouvoir de supervision. Reste alors à déterminer l'intensité et la forme de ce pouvoir de supervision et sa nature juridique. Le rapport « *Renforcer la lutte contre le racisme et l'antisémitisme* » propose en l'occurrence que le CSA remette son interprétation à l'opérateur sous la forme d'un avis[1521]. Ce choix se justifie du fait que l'autorité émet déjà ce type d'actes dans le cadre de sa fonction consultative notamment à l'encontre de l'autorité de régulation des communications électroniques et des postes (ARCEP)[1522]. Selon le Professeur Jacques Raynard, dans son sens le plus neutre l'avis doit se comprendre comme le conseil que l'on demande ou que l'on donne. Ce besoin de conseil provenant du fait que celui qui est en charge de prendre la décision, ici l'opérateur d'un réseau social, n'est pas assez éclairé sur la question qui lui ait posé. « *L'avis est alors demandé à un sachant ou donné par un sachant ; il porte sur une information, une opinion technique pour laquelle l'expérience, la compétence de l'émetteur d'avis légitime la procédure* »[1523]. Le nouvel article 17-3 de la loi n° 86-1067 du 30 septembre 1986[1524] dispose par ailleurs qu' « *en cas de nécessité,* [le CSA] *adresse, à ce titre, aux opérateurs mentionnés au même premier alinéa des recommandations, des bonnes*

[1519] L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), *JORF*, 1er octobre 1986, p. 11749.
[1520] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 4, futur article 17-3 I de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.
[1521] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018, p. 26.
[1522] Par exemple : CSA, avis n° 2018-09 du12 décembre 2018 sur un projet de décision de prolongation de la décision n° 2015-1583 en date du 15 décembre 2015 portant sur la définition du marché pertinent de gros des services de diffusion hertzienne terrestre de programmes télévisuels en mode numérique, sur la désignation d'un opérateur exerçant une influence significative sur ce marché et sur les obligations imposées à cet opérateur sur ce marché.
[1523] J. RAYNARD, *Domaine et thème des avis*, *in L'inflation des avis en droit* (dir. T. REVET), Économica, 1998, p. 12.
[1524] L. n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), *JORF*, 1er octobre 1986, p. 11749.

pratiques et des lignes directrices pour la bonne application des obligations mentionnées aux articles 6-2 et 6-3 de la même loi, ainsi qu'en matière d'accompagnement des victimes ». Ainsi, la supervision du CSA peut également s'effectuer sous formes de recommandations aux opérateurs des plateformes numériques. De même que pour les avis, les recommandations invitent à agir dans un sens déterminé mais son dépourvues généralement de caractère contraignant. Or, il va de l'intérêt du nouveau système de responsabilité mis en place que l'interprétation rendue par l'autorité publique soit suivie par l'opérateur sinon quoi le rôle du CSA dans la régulation des contenus illicites ne serait que symbolique. Sur ce point, il convient alors de préciser que les opérateurs des grandes plateformes numériques ont toutefois intérêt à suivre l'interprétation donnée par l'autorité du fait qu'elle dispose *in fine* du pouvoir de les contrôler et de les sanctionner dans l'hypothèse où ils ne se conformeraient pas à son interprétation.

b- Un pouvoir de sanction partagé avec l'autorité judiciaire.

568. Un pouvoir de sanction du CSA sur la base des rapports de transparence. Outre sa mission de supervision concernant la régulation des contenus, la crédibilité de la régulation administrative confiée au CSA repose sur l'existence pour ce dernier d'un pouvoir de sanction. Sur la base des rapports de transparence émis par les opérateurs de réseaux sociaux, le CSA doit être en mesure d'exercer un contrôle de la politique de régulation de ces derniers pouvant justifier le prononcé d'une sanction en cas de non-respect de leurs obligations. Selon le Conseil d'État[1525], une attitude systémiquement non coopérative de l'opérateur mais également des comportements répétés de refus de retrait ou de retraits timorés, pusillanimes, ou au contraire excessifs pourront justifier la mise en œuvre de son pouvoir de sanction. Il apparaît en effet indispensable de que le pouvoir de contrôle et de sanction s'étende à l'hypothèse d'une trop grande activité dans la modération des contenus dans la mesure où elle pourrait porter atteinte au principe de liberté d'expression. Sur ce point la volonté du législateur est claire : l'autorité publique met en œuvre son pouvoir de sanction en appréciant « *le caractère insuffisant ou excessif du comportement de l'opérateur en matière de retrait sur les contenus portés à sa connaissance ou qu'il constate de sa propre initiative* »[1526]. Ainsi, le CSA peut, après mise en demeure et dans les conditions prévues à l'article 42-7 de la loi du 30 septembre 1986, « *prononcer une sanction pécuniaire dont le montant peut prendre*

[1525] CE, avis n° 397368, 16 mai 2019, n° 35.
[1526] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 4, futur article 17-3 II de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

en considération la gravité des manquements commis et leur caractère réitéré, sans pouvoir excéder 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent »[1527]. Il paraît important que la sanction pécuniaire pouvant être prononcée par le CSA soit dissuasive de manière à inciter les opérateurs de réseaux sociaux à fournir les efforts nécessaires pour se conformer aux obligations prévues par le nouveau régime de responsabilité applicable à cette nouvelle catégorie d'acteurs. En parallèle, il est important que les sanctions prévues soient graduées et respectueuses du principe de proportionnalité. Le Conseil national du numérique a ainsi invité le législateur à préciser quant à la façon d'apprécier la « *gravité* » et le « *caractère réitéré* » des infractions concernées aux fins de la détermination du montant de la sanction pécuniaire[1528].

569. La nécessaire présence de voies de recours juridictionnelles. L'importance des mesures de polices administratives conférées au CSA dans le but de veiller à l'ordre public numérique suppose cependant l'existence d'un pouvoir de contrôle juridictionnel concurrent. Autrement dit, s'il est nécessaire de donner à une autorité publique indépendante un pouvoir de supervision et de sanction quant à l'interprétation par les grandes plateformes numériques de la notion de contenus manifestement illicite, il est par ailleurs indispensable de pouvoir recourir en la matière à un juge indépendant et impartial, gardien des libertés. En effet, à travers l'interprétation du caractère manifestement illicite des contenus signalés, les opérateurs des réseaux sociaux, supervisés par le CSA, se positionnent sur des qualifications pénales. Dans cette hypothèse, un juge doit également pouvoir être saisi pour se prononcer sur le caractère manifestement illicite d'un contenu dès lors qu'il implique l'interprétation d'un texte de nature pénale[1529]. Cette position est défendue par le Conseil d'État dans son avis sur la proposition de loi visant à lutter contre les discours haineux sur internet : « *la suppression d'un contenu odieux sur Internet est un acte particulièrement radical au regard de la protection dont jouit la liberté d'expression consacrée à l'article 11 de la Déclaration des droits de l'homme et du citoyen. Le retrait de contenu ne peut donc généralement être opéré que par le juge judiciaire ou à tout le moins sous son contrôle* »[1530].

[1527] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 4, I, futur article 17-3 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

[1528] Communiqué de presse du Conseil national du numérique, *Le CNNum exprime ses interrogations sur la proposition de loi visant à lutter contre la haine sur Internet*, le 21 mars 2019, enjeu n° 5.

[1529] V. en ce sens : K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, *op. cit.*, p. 27.

[1530] CE, avis n° 397368, 16 mai 2019, n° 25.

570. Deux infractions gardiennes de l'intervention du juge. Dans le but de garantir un contrôle juridictionnel de la régulation des contenus exercée par les plateformes numériques, le législateur propose deux infractions permettant de contester devant un juge les décisions de retrait mais également les décisions de non-retrait. La première infraction concerne en réalité l'auteur d'un signalement en créant un délit de notification abusive selon lequel : « *le fait, pour toute personne, de présenter aux opérateurs* […] *un contenu ou une activité comme étant illicite* […] *dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'un an d'emprisonnement et de 15 000 euros d'amende* »[1531]. Cette infraction, calquée sur celle déjà existante à l'article 6, I, 4° de la LCEN, créée ainsi « *un contre-feu qui offre une garantie minimale en faveur de la liberté d'expression* »[1532] en protégeant les idées ou informations qui heurtent, choquent ou inquiètent. Mais surtout, ce nouveau régime de responsabilité consacre à l'encontre des opérateurs des grandes plateformes en ligne un délit de refus de retrait d'un message manifestement illicite. Il est à ce titre précisé que « *le fait de ne pas respecter l'obligation définie au premier alinéa du I du présent article est puni des peines prévues au 1 du VI de l'article 6 de la présente loi* »[1533]. Par ailleurs, dans le but de rendre la sanction dissuasive, le montant de la peine d'amende encourue à l'article 6, VI, 1 de la LCEN a été porté à 250 000 euros. En application de l'article 131-38 du Code pénal le maximum de la peine d'amende prononçable à l'encontre d'une personne morale est porté à 1 250 000 euros. Monsieur Baptiste Nicaud observe alors que cette infraction « *réhabilite* […] *le juge de son rôle de gardien des libertés, offrant ainsi une soupape contre la censure excessive* »[1534].

571. La collaboration entre l'autorité administrative et l'autorité judiciaire. De façon similaire à la CNIL[1535], l'existence de sanctions tant à l'échelle administrative que judiciaire implique de s'interroger sur le cumul possible de ces voies de recours. Sur ce point, la Cour européenne des droits de l'homme est venue récemment rappeler qu'un cumul de poursuites et de sanctions était envisageable dès lors qu'elles s'intégrent « *dans le cadre de phase*

[1531] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 1er *ter* (nouveau), futur article 6-2, III.
[1532] B. NICAUD, « Proposition de loi contre la "cyberhaine" adoptée à l'Assemblée ou l'enfer pavé de bonne (?) intentions », Lexbase Pénal Edition n° 18, 18 juillet 2019.
[1533] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 1er, futur article 6-2, I.
[1534] B. NICAUD, « Proposition de loi contre la "cyberhaine" adoptée à l'Assemblée ou l'enfer pavé de bonne (?) intentions », *op. cit*.
[1535] V. *supra* n° 357.

parallèle, menées par des autorités différentes et à des fins différentes »[1536]. Au vu de cet arrêt, les procédures engagées concurrement devant le CSA et le juge pénal devront alors respecter différents critères pour ne pas se voir sanctionner pour non respect du principe *ne bis in idem*. Le cumul peut ainsi être admis si les procédures visent des buts complémentaires et concernent des aspects différents de l'acte préjudiciable. Ce critère semble cependant ne pas pouvoir être rempli du fait que le CSA et le juge judiciaire auraient vocation à se fonder sur l'irrespect des mêmes obligations à la charge des plateformes numériques pour prononcer leurs sanctions. À moins que soient différenciés d'un côté le contrôle et la sanction du CSA sur le fondement des rapports transmis à l'autorité et donc au vu de la politique générale de régulation des contenus de la plateforme numérique et de l'autre, la sanction pénale prononcée par le juge renvoyant à une omission fautive de l'opérateur dans la régulation d'un contenu bien déterminé. Dans cette hypothèse les rôles joués par les deux autorités pourraient être envisagés comme complémentaires du fait qu'ils concernent des aspects différents de l'acte préjudiciable. De manière générale, à l'instar de la relation unissant la CNIL et le juge pénal[1537], le CSA devra fonctionner en étroite collaboration avec le juge pénal de manière à ce que leur champ de compétence partagé aboutisse à une interraction adéquate, les amènant alors à se renforcer mutuellement et non de manière concurrente dans le respect du principe *ne bis in idem*.

§2. La régulation au sein des réseaux sociaux, l'intérêt d'une régulation collaborative

572. Une régulation horizontale de l'expression sur les réseaux sociaux. Si un rapport d'autorité vertical est nécessaire dans la régulation des sites de réseaux sociaux avec la présence d'une autorité tiers et de l'autorité judiciaire chargées de veiller au respect de leurs obligations, une bonne effectivité du nouveau régime de responsabilité mis en place au sein de la LCEN est également dépendante de l'implication des acteurs des sites de réseaux sociaux, autant leurs utilisateurs (A) que leurs opérateurs (B).

A. La collaboration active des utilisateurs à la régulation des sites de réseaux sociaux

573. Les utilisateurs, premier maillon de la chaîne. Par leur pouvoir de signalement, les utilisateurs des réseaux sociaux en ligne détiennent un rôle fondamental dans la régulation de

[1536] CEDH, *Nodet c. France*, 6 juin 2019, req. n° 47342/14 : *D. actu.,* 27 juin 2019, obs. P. DUFOURQ ; *JCP G* n° 25, 24 Juin 2019, note L. MILANO.
[1537] V. *supra* n[os] 355 à 357.

ces derniers et dans la mise en jeu de la responsabilité de leurs opérateurs. En tant que premier maillon de la chaîne, il est nécessaire d'éduquer la société civile aux bonnes pratiques du numérique de manière à améliorer au possible la qualité des signalements (1). Par ailleurs, la qualité du signalement est également dépendante des outils de signalement mis à disposition des utilisateurs, dans cette optique il est proposé d'uniformiser sur toutes les plateformes la procédure de signalement des contenus (2).

1) La nécessaire éducation de la société civile au numérique

574. Le rôle de l'éducation nationale. L'expression citoyenne sur internet est à la fois un droit fondamental mais également une responsabilité qui nécessite un apprentissage[1538]. Afin de donner aux citoyens une juste place au sein de la société numérique, il est nécessaire d'adopter une politique inclusive permettant à chacun d'acquérir les compétences pour comprendre et interagir avec les outils numériques. Pour ce faire, de nombreux rapports et avis[1539] préconisent l'adoption d'un plan d'action national portant sur l'éducation et la citoyenneté numérique. Ce plan tendrait vers une valorisation d'une parole libre et responsable par la définition de codes de bonnes conduites à destination des internautes. En l'occurrence, dans la recherche d'une efficacité et d'un auditoire maximum il est recommandé d'intégrer dans les programmes de l'éducation nationale une formation spécifique à l'internet et à son usage civique. Cette mobilisation de l'éducation nationale se faisant dans le but de proposer un usage éclairé de l'internet et notamment de former les jeunes citoyens au tri des informations leur permettant de se forger leur propre opinion mais également de détecter les contenus outrepassant les limites de la liberté d'expression. Il ne s'agit donc pas de proposer la mise en place d'une discipline d'enseignement permettant une compréhension du phénomène et du discours raciste, mais plutôt que le système scolaire se saisisse du sujet de la civilité sur internet comme faisant partie des savoirs indispensables devant être transmis aux élèves. Il est notamment proposé d'introduire « *un kit pédagogique réalisé sur la base d'un cahier des charges établi de manière mutualisée avec le soutien d'experts et des acteurs compétents en matière d'internet* »[1540]. Ces cours d'éducation civique numérique devraient être assurés par des intervenants qualifiés soit en raison de leurs savoirs et expériences dans le domaine soit en raison de formations spécifiques qu'ils auraient suivis.

[1538] CNCDH, *avis sur la lutte contre les discours de haine sur Internet*, Paris, 12 février 2015, p. 33.
[1539] V. par exemple : K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, *op. cit.*, recommandation n° 8, p. 42 ; CNCDH, *avis sur la lutte contre les discours de haine sur Internet*, Paris, 12 février 2015, p. 33 ; I. FALQUE-PIERROTIN, *Lutter contre le racisme sur Internet*, Rapport au Premier ministre, 2010, p. 54.
[1540] I. FALQUE-PIERROTIN, *Lutter contre le racisme sur Internet*, Rapport au Premier ministre, 2010, p. 54.

575. Le rôle de la famille. Assurer une éducation au numérique au sein de l'enceinte scolaire n'est cependant pas suffisant, l'éducation au numérique doit également pénétrer la sphère familiale qui constitue un cercle privilégié dans la structuration de la personnalité de l'enfant. L'éducation au numérique doit alors comprendre également l'éducation des parents afin que ces derniers saisissent les bonnes pratiques à suivre mais également leur responsabilité face aux usages de leurs enfants sur internet. Le rapport « *Lutter contre le racisme sur Internet* » [1541] préconise en l'espèce un travail d'information à destination des parents en leur rappelant le cadre légal et leur responsabilité pénale, en vertu de l'article 227-17 du Code pénal[1542] ainsi que leur responsabilité civile en application de l'article 1242 du Code civil[1543].

576. Le rôle des associations. Enfin, il est impératif de mesurer l'importance de l'action associative dans l'éducation au numérique et dans la prévention des atteintes aux personnes. L'engagement des associations est tout aussi déterminant que celui des pouvoirs publics, il est alors primordial de développer les possibilités d'actions de ces acteurs[1544] par le biais de subventions spécifiques[1545]. Ces derniers peuvent assurer une présence en continue sur les réseaux de discussions afin d'apporter un contre-discours mais aussi pour informer et accompagner les internautes. Par exemple, certaines associations proposent par l'intermédiaire de sites internet comme « *Point de contact* »[1546], « *True* visions »[1547] ou « *Stop Hate* »[1548] d'accompagner les internautes dans leur démarche visant à signaler un contenu. Par ailleurs, une autre action préventive suggérée est d'instaurer des « *zones de respect sur les réseaux sociaux* », c'est le cas de l'association *Respect Zone* qui labélise un certain nombre d'individus, entreprises ou organisations présentes sur les réseaux sociaux en ligne, assurant aux visiteurs par un logo visible sur leur photo ou image de profil que ces

---

[1541] *Ibid.*, p. 55.
[1542] « *Le fait, par le père ou la mère, de se soustraire, sans motif légitime, à ses obligations légales au point de compromettre la santé, la sécurité, la moralité ou l'éducation de son enfant mineur est puni de deux ans d'emprisonnement et de 30 000 euros d'amende* », C. pén., art. 227-17 al. 1er.
[1543] « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde* », C. civ., art. 1242, al 1er.
[1544] De nombreuses associations luttent contre le racisme et les discours de haine. On recense notamment : la Ligue contre le racisme et l'antisémitisme (LICRA), le Mouvement de lutte contre le racisme et pour l'amitié entre les peuples (MRAP), le Conseil représentatif des institutions juives de France (CRIF), l'association J'Accuse, l'association des étudiants juifs de France (AEJF), Sos Racisme, la Ligue des droits de l'Homme et du citoyen (LDH) ou encore le Conseil français du culte Musulman (CFCM).
[1545] V. en ce sens I. FALQUE-PIERROTIN, *Lutter contre le racisme sur Internet*, Rapport au Premier ministre, 2010, p. 57 ; CNCDH, *avis sur la lutte contre les discours de haine sur Internet,* Paris, 12 février 2015, p. 34.
[1546] <https://www.pointdecontact.net>
[1547] <http://www.report-it.org.uk>
[1548] <http://www.stophateuk.org>

dernières se sont engagées à appliquer la charte de respect d'autrui et de modération[1549]. Outre ces actions positives, les associations peuvent également assurer une mission de veille dans le but de signaler, voire poursuivre des contenus qu'elles jugeraient illicites dans les conditions prévues par la loi du 29 juillet 1881[1550]. Dès lors, tout signalement émis par une association ou organisme public veillant au respect des droits et libertés devrait recevoir une attention particulière de l'opérateur l'ayant reçu. Une telle coopération entre les opérateurs de réseaux sociaux et certaines associations agréées permettrait d'un côté aux plateformes de bénéficier d'une bonne image et de l'autre, aux associations d'inciter les grands acteurs du web à la bonne mise en œuvre de leurs engagements[1551].

2) L'opportunité de l'uniformisation de la procédure de signalement

577. Création d'une procédure de signalement uniformisée auprès des opérateurs. La bonne implication de la société civile dans la régulation des contenus dépend par ailleurs de la présence d'outils de signalement fonctionnels et efficaces. Dans ce but précis, le rapport visant à « *Renforcer la lutte contre le racisme et l'antisémitisme* » propose la création d'un logo unique de signalement de contenus illicites, visible et identifiable sur toutes les plateformes[1552]. Il est également proposé que cette uniformisation de la procédure de signalement s'accompagne d'une absence d'obligation de créer un compte pour les internautes effectuant le signalement, impliquant notamment la possibilité pour ces derniers de rester anonymes le minimum requis étant la fourniture d'une adresse mail. En outre, le

[1549] <https://www.respectzone.org>

[1550] La loi sur la liberté de la presse du 29 juillet 1881 reconnaît la possibilité aux associations d'agir en justice pour la défense des intérêts collectifs dont elles ont la charge. Ce droit est octroyé aux associations régulièrement déclarées depuis au moins 5 ans à la date des faits. Les associations ne peuvent cependant agir que dans les cas énumérés par les articles 48-1 à 48-6 de la loi sur la presse. Ainsi, l'article 48-4 reconnaît le droit d'exercer les prérogatives reconnues à la partie civile à toute association se proposant, par ses statuts, de combattre les violences ou les discriminations fondées sur l'orientation sexuelle ou d'assister les victimes de ces discriminations, concernant les délits de provocation à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap, ou encore de provocation, à l'égard des mêmes personnes, aux discriminations prévues par les articles 225-2 et 432-7 du Code pénal (L. 1881, art. 24, al. 8), le délit de diffamation envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap (L. 1881, art. 32, al. 3.), le délit d'injure commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap (L. 1881, art. 33, al. 4), ainsi que les délits de provocation aux atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne et les agressions sexuelles, définies par le livre II du code pénal (L. 1881, art. 24, al. 1). Concernant les mêmes hypothèses, les articles 48-5 et 48-6 reconnaissent le droit d'exercer les prérogatives appartenant à la partie civile respectivement aux associations qui se proposent, par leur statuts, de combattre la violence ou la discrimination fondée sur le sexe et sur le handicap ou d'assister les victimes de ces discriminations. V. B. BEIGNIER, B. de LAMY, E. DREYER (dir.), *Traité de droit de la presse et des médias*, Litec, 2009, p. 594 et 595, n^{os} 1007 à 1010.

[1551] L. VITRAL, *Les Organisations Non Gouvernementales dans la régulation de l'économie mondiale*, L'Harmattan, 2008, p. 194 et suiv.

[1552] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme, op. cit.*, recommandation n° 8, p. 31.

rapport suggère que le logo de signalement renvoie à l'ensemble des voies de recours offertes à l'internaute confronté à un contenu qu'il juge illicite ce qui comprend : le simple signalement à l'opérateur, le signalement auprès d'une association spécialisée, le signalement sur la plateforme PHAROS ou encore, la possibilité du dépôt d'une plainte en ligne. Conformément à ces recommandations, le nouveau régime de responsabilité applicable aux opérateurs des grandes plateformes en ligne prévoit à leur charge une obligation de coopération impliquant notamment de mettre en place pour les utilisateurs situés sur le territoire français : « *un dispositif de notification directement accessible et uniforme permettant à toute personne de notifier un contenu illicite dans la langue d'utilisation du service et informant les notifiants des risques qu'ils encourent en cas de notification abusive* »[1553].

578. L'assouplissement de la procédure de notification de contenu. En parallèle de cette logique d'uniformisation et de simplification, le léglisateur propose en outre d'assouplir les critères de recevabilité de la procédure de notification de contenu. Selon la nouvelle rédaction de l'article 6, I, 5° de la LCEN la connaissance des faits litigieux est présumée acquise lorsqu'il est transmis aux opérateurs les éléments suivants :

« *Si le notifiant est une personne physique : ses nom, prénoms, adresse électronique ; si le notifiant est une personne morale : sa forme sociale, sa dénomination sociale, son adresse électronique ; si le notifiant est une autorité administrative : sa dénomination et son adresse électronique ; ces conditions sont réputées satisfaites dès lors que le notifiant est un utilisateur inscrit du service de communication au public en ligne mentionné au même 2, qu'il est connecté au moment de procéder à la notification et que l'opérateur a recueilli les éléments nécessaires à son identification ; La catégorie à laquelle peut être rattaché le contenu litigieux, la description de ce contenu, les motifs pour lesquels il doit être retiré, rendu inaccessible ou déréférencé et, le cas échéant, la ou les adresses électroniques auxquelles ce contenu est rendu accessible* »[1554].

579. Désormais, trois principales exigences se dégagent de cette procédure : premièrement, l'identification claire de la personne, physique ou morale, à l'origine de la notification ; deuxièmement, la sélection par cette dernière de la catégorie à laquelle peut être rattaché le

[1553] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 2, futur article 6-3, 3° de la LCEN.

[1554] Proposition de loi, *visant à lutter contre la haine sur internet*, enregistrée à la Présidence de l'Assemblée nationale le 20 mars 2019, texte n° 310 adoptée en première lecture le 9 juillet 2019, art. 1er *ter* A (*nouveau*), futur article 6, I, 5° de la LCEN.

contenu litigieux d'après une liste d'infractions préétablie ainsi que la description des faits litigieux et des motifs pour lesquels il doit être retiré ; enfin, la personne à l'origine de la notification doit renseigner l'adresse URL à laquelle le contenu est rendu accessible. En conséquence, la qualification juridique du contenu litigieux est simplifiée par rapport au système précédent qui imposait à l'auteur de la notification une localisation des faits litigieux, ainsi qu'une qualification pénale précise du contenu litigieux. Mais surtout, il n'est plus exigé pour que la notification soit valable que le notifiant prouve qu'il ait contacté, ou du moins tenté de contacter, en liminaire l'auteur du contenu lui demandant le retrait de ce dernier. Ces nouvelles règles en matière de notification de contenu illicite ne suivent toutefois pas entièrement les recommandations émises par le rapport « *Renforcer la lutte contre le racisme et l'antisémitisme* », particulièrement concernant l'anonymisation de l'auteur de la notification[1555]. Cette position se justifie au regard du nécessaire engagement de responsabilité de l'auteur d'une notification abusive. Il est à ce titre indispensable au bon fonctionnement du système de notification que leurs auteurs ne soient pas couverts par un anonymat au risque d'engendrer un flux trop important de signalements parmi lesquels, beaucoup pourraient être excessifs. Le délit de notification abusive de contenu illicite doit alors s'appliquer de manière à inciter les utilisateurs à adopter un comportement responsable. En l'espèce, la sanction d'un utilisateur en application du délit de notification abusive pourrait être précédée d'avertissements à l'image des sanctions applicables en matière de téléchargement illicites. De ce fait, seuls les utilisateurs se livrant à un réel comportement abusif marqué par une multitude de signalements inopportuns pourraient se voir sanctionnés, protégeant par là même les utilisateurs diligents qui hésiteraient en raison du caractère incertain de l'illicéité du contenu.

580. La confusion du signalement et de la notification de contenus. L'assouplissement de la procédure de notification de contenu couplée avec l'obligation pour toute plateforme de mettre en place un système uniformisé permettant de satisfaire à ces exigences revient à faire de tout signalement émis depuis une plateforme en ligne, une notification de contenu illicite telle que prévue à l'article 6, I, 5° de la LCEN. La conséquence est majeure : tout signalement opéré depuis les plateformes vaut instantanément présomption de connaissance des faits litigieux pour ces dernières. Cet ajustement tend ainsi à une plus grande effectivité du droit dans la mesure où les opérateurs de réseaux sociaux sont davantage liés par les signalements qu'ils reçoivent.

[1555] K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme, op. cit.*, recommandation n° 8, p. 31.

B. La mise en conformité des réseaux sociaux par leurs opérateurs

581. Une démarche positive des opérateurs des réseaux sociaux. Outre l'encadrement par une autorité publique indépendante et une veille citoyenne, le développement et la préservation d'un ordre public numérique sur les réseaux sociaux dépend avant tout de l'action de leurs opérateurs. Ces derniers doivent ainsi d'une part collaborer activement avec d'un côté les pouvoirs publics édictant les contours de l'ordre public numérique et de l'autre la société civile veillant au respect de cet ordre par leur pouvoir de signalement. D'autre part, les opérateurs de réseaux sociaux se montrent désormais soucieux des droits et principes défendus par l'autorité publique alors même que ces règles n'entrent pas directement dans leur intérêt social ou même y sont en opposition. Cette démarche volontariste consistant à intégrer dans leur fonctionnent des règles d'intérêt public, correspond au processus de mise en conformité ou *compliance* (1) qui est progressivement intégré par les sites de réseaux sociaux (2).

1) La notion de conformité ou *compliance*

582. Définition du devoir de conformité. La conformité est la traduction française de la notion américaine de *compliance*[1556]. La compliance peut se définir comme « *un ensemble de principes et de procédures mis en œuvre – de manière proactive – par les opérateurs économiques, dans le but d'assurer le respect, au-delà des règles de droit applicables, d'un système de valeurs souhaitable pour leur organisation, intégrant une certaine éthique des affaires* »[1557]. Elle peut également se définir comme « *l'ensemble des processus qui permettent d'assurer la conformité des comportements de l'entreprise, de ses dirigeants et de ses salariés aux normes juridiques et éthiques qui sont applicables* »[1558]. Dans cette hypothèse, l'entreprise utilise sa puissance structurelle pour atteindre les buts édictés par l'État qui lui sont *a priori* extérieurs tels que la prise en considération de l'intérêt d'autrui. La compliance consiste alors pour certaines entreprises à se conformer à l'ensemble des règlementations en créant notamment leur propre système de régulation. Selon le Professeur Marie-Anne Frison Roche, la compliance est donc « *l'internalisation mondiale d'une régulation publique locale dans les entreprises supranationales, désignés comme agents*

[1556] Le terme « *conformité* » n'est toutefois pas entièrement adéquat, la notion de *compliance* se révélant difficile à traduire. V. M.-A. FRISON-ROCHE « Compliance ». <http://mafr.fr/fr/article/compliance> (dernière consultation le 9 octobre 2019).
[1557] B. DE JUVIGNY, « La compliance, bras armé de la régulation », *in* M.-A. FRISON-ROCHE (dir.), *Régulation, Supervision, Compliance*, Dalloz, Coll. Thèmes et commentaires, 2017, p. 17 et suiv.
[1558] A. GAUDEMET (dir.), *La compliance : un monde nouveau ?*, Paris, Éd. Panthéon-Assas, 2016, p. 9.

d'effectivité de buts mondiaux monumentaux »[1559]. Aujourd'hui, la compliance n'est plus seulement subie et imposée par des systèmes de régulation émanant de l'autorité publique, elle est également assumée et intégrée volontairement dans le modèle économique des opérateurs.

583. La concrétisation de la théorie de la responsabilité sociétale des entreprises. Selon la théorie de la responsabilité sociétale des entreprises, ces dernières possèderaient une responsabilité vis-à-vis des effets qu'elles exercent sur la société[1560] leur imposant d'adopter un comportement transparent et éthique. Cette théorie entreprend ainsi d'asseoir la transformation de l'intérêt social en intérêt sociétal. L'idée défendue est celle d'une entreprise citoyenne dont l'activité intègre une dimension éthique dans les domaines sociaux et environnementaux[1561]. L'adoption d'une démarche de compliance par une entreprise peut alors s'analyser comme une réception et une mise en œuvre effective du principe de responsabilité sociétale des entreprises.

2) L'intégration progressive du devoir de conformité aux réseaux sociaux

584. Une intégration volontaire ou par la contrainte. Les principaux réseaux sociaux, en collaboration avec l'autorité publique, adoptent une démarche volontaire de mise en conformité de leurs services aux exigences européennes en matière de lutte contre les discours haineux (a). Dans l'hypothèse où l'opérateur du réseau social serait réticent à entreprendre une telle démarche, le juge pourrait contraindre ce dernier à s'y soumettre par le biais d'une sanction pénale de mise en conformité (b).

a- L'intégration volontaire du devoir de mise en conformité

585. L'intégration par une démarche collaborative des opérateurs des réseaux sociaux. Conscients des improbations des institutions européenne face à leur passivité dans la réprobation des discours haineux, les principales entreprises des technologies de la communication, en l'occurrence Facebook, Twitter, YouTube et Microsoft, ont adopté de concert avec la Commission européenne le 31 mai 2016 un code de conduite relatif aux

[1559] M.-A. FRISON-ROCHE, « Droit de la compliance ». <http://mafr.fr/fr/article/le-droit-de-la-compliance> (dernière consultation le 9 octobre 2019).
[1560] Commission Européenne, 3ème Communication Sur la RSE, 25 octobre 2011.
[1561] V. notamment sur la question : M.-C. CAILLET, *Le droit à l'épreuve de la responsabilité sociétale des entreprises : étude à partir des entreprises transnationales*, Thèse, Bordeaux, 2014 ; C. MALECKI, *Responsabilité sociale des entreprises, Perspectives de la gouvernance d'entreprise durable*, coll. Droit des affaires, Paris, LGDJ-Lextenso, 2014.

discours haineux illégaux en ligne[1562]. Au sein de ce code, les entreprises signataires s'engagent à continuer la lutte contre les discours de haine en ligne. Ceci implique notamment la mise au point de procédures internes et la formation d'un personnel qualifié pour que la majorité des signalements valides puissent être examinés en moins de 24 heures et s'il y a lieu, retirés ou bloqués. Ces géants des technologies de la communication promettent également aux côté de la Commission européenne d'élaborer et de promouvoir l'esprit critique de leurs utilisateurs à travers la mise en avant de contre-discours indépendants, et l'adoption de programmes éducatifs. L'adoption de ce code de bonne conduite est le premier signe d'une prise en compte par les principaux sites de réseaux sociaux des standards européens. Si ce dernier ne possède pas une véritable force contraignante, sa force se mesure alors à sa dimension symbolique.

586. Collaboration de la société Facebook avec le Gouvernement. Par ailleurs, dans le cadre de la mission sur la régulation des réseaux sociaux lancée par le Gouvernement en janvier 2019, la société Facebook s'est portée volontaire pour servir de cobaye dans cette expérimentation sur la modération des contenus. Cette dernière a accepté de travailler sur la régulation des contenus haineux de concert avec une délégation de fonctionnaires français dans le but d'améliorer son rôle de modérateur. Cette collaboration vise notamment à améliorer les procédures que doivent mettre en place les réseaux sociaux afin d'identifier et filtrer les contenus revêtant un caractère manifestement illicite. Ceci témoigne d'une volonté du réseau social d'adopter des outils efficaces de manière à se mettre en conformité au principe européen de liberté d'expression. Le rapport de la mission publié en mai 2019[1563] fait état de la démarche actuelle d'autorégulation des sites de réseaux sociaux qui démontre qu'ils peuvent faire partie de la solution aux problèmes constatés. Le rapport rappelle ainsi que ces derniers ont inventé « *des réponses variées et agiles : retrait, moindre exposition, rappel à la règle commune, pédagogie, accompagnement des victimes* »[1564].

[1562] Commission européenne, Communiqué de presse du 31 mai 2016 : « *La Commission européenne et les entreprises des technologies de l'information annoncent un code de conduite relatif aux discours haineux illégaux en ligne* ».
<http://europa.eu/rapid/press-release_IP-16-1937_fr.htm> (dernière consultation le 9 octobre 2019).
[1563] Rapport de la mission « Régulation des réseaux sociaux – Expérimentation Facebook » remis au Secrétaire d'État en charge du numérique, mai 2019.
[1564] *Ibid.*, p. 2.

b- L'intégration du devoir de mise en conformité par la contrainte

587. Existence d'une sanction pénale de mise en conformité en matière financière. L'action de mise en conformité peut en outre s'envisager comme un devoir susceptible d'être imposé sous la forme d'une sanction pénale. Selon le Procureur général près la Cour de cassation Jean-Claude Marin, « *Évoquer la place du droit pénal dans la compliance revient à s'interroger sur la place d'un traitement des difficultés ex post dans une logique de détection ex ante. Toutefois, loin d'apparaître en confrontation, le droit pénal et la compliance se complètent. D'une part du fait de l'intervention du procureur de la République, mais aussi du magistrat du siège dans ces procédures, et d'autre part en raison de la complémentarité de la compliance et de la sanction pénale* »[1565]. Le législateur est venu prévoir une sanction de mis en conformité en matière financière par la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique[1566]. En l'occurrence, quatre éléments ont été ajoutés aux moyens dont dispose le parquet national financier : une agence française anti-corruption (AFA) ; la création d'un mécanisme de transaction pénale nommé la « *convention judiciaire d'intérêt public* » ; l'introduction d'une obligation légale de prévention contre les risques de corruption ; mais surtout, la création d'une peine complémentaire de mise en conformité. La compliance devient ainsi une sanction pénale prononcée dans le but de mettre fin à un comportement délictueux. Selon le nouvel article 131-39-2 du Code pénal créé par la loi Sapin II : « *Lorsque la loi le prévoit à l'encontre d'une personne morale, un délit peut être sanctionné par l'obligation de se soumettre, sous le contrôle de l'Agence française anticorruption, pour une durée maximale de cinq ans, à un programme de mise en conformité destiné à s'assurer de l'existence et de la mise en œuvre en son sein des mesures et procédures définies au II* »[1567].

588. Proposition. Sur la base de l'article 131-39-2 du Code pénal il pourrait dès lors être proposé l'introduction d'une sanction similaire dans la LCEN applicable aux « *accélérateurs de contenus* » lorsque ces derniers auraient commis une des infractions prévues aux articles 226-16 à 226-24 du Code pénal ou en cas de non-respect de leurs obligations. Le contrôle de

[1565] J.-C. MARIN, « Droit pénal et compliance », *in* M.-A. FRISON-ROCHE (dir.), *Régulation, Supervision, Compliance*, Dalloz, Coll. Thèmes et commentaires, 2017, p. 66.
[1566] L. n° 2016-1691, 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, *JORF* n° 0287, 10 décembre 2016, texte n° 2.
[1567] L. n° 2016-1691, 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, *JORF* n° 0287, 10 décembre 2016, art. 18.

l'obligation de mise en conformité serait confié au CSA dans le cadre de ses nouvelles missions visant à encadrer la catégorie des « *accélérateurs de contenus* ».

589. Conclusion de la Section 2. La garantie d'une bonne application du nouveau régime de responsabilité des « *accélérateurs de contenus* » est dépendante d'une pluralité d'acteurs. La mise en place d'une autorité de contrôle apparaît essentielle pour assurer un contrôle et une sanction efficace des sites de réseaux sociaux. Il est en l'occurrence proposé d'étendre les pouvoirs du CSA lui permettant d'acquérir un pouvoir de contrôle et de sanction à l'égard de la catégorie des « *accélérateurs de contenus* ». L'autorité administrative serait alors investie d'un véritable pouvoir de sanction ayant force dissuasive, la sanction pécuniaire pouvant atteindre 4% du chiffre d'affaire annuel mondial de l'entreprise. Ce pouvoir de sanction serait également couplé d'un pouvoir de supervision visant à accompagner les opérateurs des réseaux sociaux dans leur devoir de modération des contenus qui leur sont signalés. L'autorité publique veillerait ainsi avec davantage de neutralité à l'identification et à la modération des contenus manifestement contraires à l'ordre public numérique. Ces pouvoirs reconnus au CSA doivent cependant s'exercer concurremment avec l'autorité judiciaire gardienne des libertés et seul véritable acteur légitime à qualifier pénalement les contenus signalés. Le nouveau régime de responsabilité applicable aux opérateurs des réseaux sociaux prévoit pour ce faire une infraction de notification abusive d'un contenu illicite ainsi qu'une infraction de non-retrait d'un contenu manifestement illicite pouvant entraîner une condamnation de l'opérateur à une peine d'amende d'un maximum de 1 250 000 euros d'amende.

590. Outre l'action d'une autorité de régulation, la réussite du nouveau régime de responsabilité et la garantie d'une meilleure préservation de l'ordre public numérique dépend inexorablement d'une collaboration active des acteurs des réseaux sociaux, à savoir leurs utilisateurs et leurs opérateurs. Les utilisateurs des réseaux sociaux jouent par leur pouvoir de signalement le premier rôle dans la mécanique de responsabilité des réseaux sociaux. La mise en place d'une politique forte d'éducation au numérique et d'outils de signalement clairs et uniformisés sont alors essentiels au bon fonctionnement de cette mécanique. Mais surtout, la collaboration doit être ressentie à l'échelle des opérateurs des réseaux sociaux. Ces derniers s'engagent à ce titre progressivement dans un processus de mise en conformité démontrant leur volonté d'intégrer dans leurs règles de fonctionnement la conception européenne du droit à la liberté d'expression.

Conclusion du Chapitre 2

591. Afin de répondre au constat d'ineffectivité de la sanction pénale et plus généralement de l'affaiblissement de certains standards du droit européen causé par les réseaux sociaux en ligne, un nouveau régime de responsabilité applicable aux grandes plateformes numériques de partage voit le jour au sein des nouveaux articles 6-2 et 6-3 de la LCEN. Calé sur le régime actuellement applicable aux hébergeurs, ce régime de responsabilité est toutefois empreint d'une plus grande sévérité justifiée au regard du rôle actif que jouent les opérateurs des réseaux sociaux sur les contenus et de l'avantage économique qu'ils retirent de l'activité de leurs utilisateurs. Principalement, le nouvel article 6-2 de la LCEN obligerait les opérateurs des grandes plateformes numériques à retirer un contenu qui leur serait signalé sous un délai de 24 heures lorsqu'il appartiendrait à une liste précise d'infractions. Ce délai de réaction extrêmement court couplé avec une liste d'infractions s'avérant trop hétéroclites est cependant de nature à empêcher les opérateurs de se livrer à une régulation satisfaisante des contenus. Le risque étant que ces derniers, de peur d'être sanctionnés, suppriment de façon conservatoire des contenus s'avérant pourtant licites. Un nécessaire équilibre doit alors être trouvé entre la sauvegarde de l'ordre public à l'échelle numérique et la sauvegarde de la liberté d'expression en ligne. Par ailleurs, l'effectivité de ce nouveau régime de responsabilité dépend également de la capacité d'acteurs tiers à veiller à sa bonne application. Le législateur a ainsi choisi de conférer à une autorité indépendante, le CSA, un pouvoir de contrôle et de sanction. Ce dernier se voit doter à ce titre d'un pouvoir de supervision dans la régulation des contenus mais surtout, d'un pouvoir de sanction administrative dissuasif en cas de non-respect par les opérateurs des réseaux sociaux de leurs obligations. Il est toutefois nécessaire que ce pouvoir de sanction s'exerce en concurrence avec l'autorité judiciaire concernant un domaine aussi sensible que celui de la régulation de la liberté d'expression en ligne. Enfin, la mécanique de responsabilité dépend non seulement d'un rapport d'autorité mais également d'une dimension davantage collaborative. À ce titre, les utilisateurs des réseaux sociaux jouent un rôle fondamental par l'intermédiaire de leur pouvoir de signalement. Il est en conséquence nécessaire de mettre en place des formations citoyennes aux bons usages du numérique afin d'améliorer autant que possible la qualité du signalement, premier maillon de la chaîne de responsabilité. La collaboration doit en définitive provenir également des opérateurs des réseaux sociaux à travers la logique de mise en conformité intégrée progressivement par ces

derniers et démontrant leur bon vouloir dans le respect des obligations qui leurs sont imparties.

Conclusion du Titre 2

592. La voie répressive classique n'est plus capable d'assurer seule la réponse aux infractions commises sur les sites de réseaux sociaux et d'assurer ainsi la préservation d'un ordre public stable dans la sphère numérique. Le Professeur Ronan Raffray observe dans ce sens que : « *Associée au recul des États, l'augmentation de la puissance des multinationales crée une horizontalité qui se substitue à la verticalité qui caractérise en principe le rapport entre État et entreprise* »[1568]. Des solutions alternatives se sont alors développées afin d'assurer la pérennité de l'État de droit dans le numérique. Dans un premier temps, la régulation par la modération de certains contenus vient pallier l'incapacité du système judiciaire à répondre à l'ensemble du contentieux généré par les sites de réseaux sociaux. Cette régulation intervient donc en soutient des difficultés répressives mais sans s'y substituer, la mise en mouvement de l'action publique demeurant possible dès lors que l'infraction est constituée, autrement dit, publiée. Cependant, ce type de régulation admis implicitement par la LCEN ne saurait fonctionner efficacement lorsqu'elle est abandonnée à la seule interprétation de l'opérateur du réseau social, un tel système aboutissant nécessairement à la mise en place d'une régulation privée des contenus dangereuse d'un point de vue démocratique. Ceci a poussé le législateur à réagir en proposant l'adoption d'un régime de responsabilité renforcé propre aux acteurs dominants de l'économie numérique avec en tête de proue les opérateurs des grands réseaux sociaux. De plus, afin de garantir l'effectivité d'un tel régime, le CSA se voit étendre ses missions à la supervision des grandes plateformes numériques de partage dans leur devoir de modération des contenus. Cette solution introduit une autorité publique tiers et indépendante dans la gestion de la modération des contenus et vise à garantir une meilleure préservation de l'ordre public dans la sphère numérique. Cette meilleure effectivité de ce nouveau régime de responsabilité est garantie par un pouvoir de sanction dissuasif de l'autorité pouvant atteindre 4% du chiffre d'affaire annuel mondial de l'entreprise. Toutefois, le nécessaire renforcement de l'effectivité de la sauvegarde de l'ordre public à l'échelle numérique ne doit pas pour autant justifier la mise en œuvre d'outils aboutissant à un recul des libertés, particulièrement la liberté d'expression. En conséquence, le nouveau régime mis en œuvre ne doit pas sur-responsabiliser les opérateurs des plateformes numériques, entraînant dans ce cas un risque de suppression conservatoire de contenus en partie licites. Par ailleurs, le juge judiciaire doit demeurer présent dans la mise en

[1568] R. RAFFRAY, « Les multinationales et la création du droit », *in Les nouveaux pouvoirs, approche pluraliste des foyers de création du droit*, Bruylant, 2017, p. 74, n° 4.

œuvre de ce nouveau régime de responsabilité particulièrement dans le contrôle de la modération des contenus réalisée par les grandes plateformes numériques.

Conclusion de la Partie 2

593. Le système répressif se montre de prime abord adapté aux sites de réseaux sociaux. Plus encore, le droit pénal démontre une sévérité particulière à l'encontre des auteurs d'infractions commises sur, ou au moyen des réseaux sociaux. En effet, l'usage d'un site de réseau social pour commettre ou faciliter la commission d'une infraction constitue dans nombre d'infractions une circonstance aggravante justifiant l'augmentation des pénalités encourues. De même, les nouvelles pratiques permises par ces espaces d'échanges ont justifié l'adoption de nouvelles hypothèses d'engagement de la responsabilité pénale à l'image du cas complicité en ligne créée par l'article 222-33-3 du Code pénal envisageant la répression de la pratique du *happy slapping*. Toutefois, le système répressif démontre certaines limites, particulièrement concernant les régimes de responsabilité applicables aux acteurs des réseaux sociaux en ligne. Plus précisément, les systèmes de responsabilité pénale spécifiques applicables tant aux opérateurs qu'aux utilisateurs des sites de réseaux sociaux manifestent des carences quant à la prise en compte des nouveaux enjeux juridiques propres à ces différents acteurs. Ainsi, la jurisprudence assimile classiquement les opérateurs des réseaux sociaux à des prestataires techniques leur octroyant l'application du régime de responsabilité modéré prévu à l'article 6 de la LCEN. L'application d'un tel statut à ces acteurs dominants de l'économie numérique ne prend cependant pas en compte l'action positive de ces derniers sur les contenus gravitant sur leurs plateformes. Plus largement, le système de responsabilité prévu à l'article 6 de la LCEN démontre l'absence de prise en compte des enjeux relatifs à l'apparition, notamment à travers les sites de réseaux sociaux, d'un web intelligeant et intuitif susceptible de proposer des contenus et d'orienter des choix des utilisateurs, autrement appelé le web 3.0. Le manque d'adaptation des statuts se vérifie également à l'échelle des utilisateurs, ces derniers étant soumis au régime de responsabilité en cascade issu de l'article 93-2 de la loi du 29 juillet 1982. Selon ce régime tout utilisateur d'un site de réseau social possédant un compte ouvert au public devient directeur de publication de ce dernier et endosse alors la responsabilité pénale à titre principal pour tous les contenus publiés sur sa page. Ce régime de responsabilité conçu à l'origine pour faire peser la responsabilité pénale sur des personnes ayant la qualité de professionnels dans les médias est inadapté à l'utilisation massive et profane actuelle des sites de réseaux sociaux. Mais surtout, l'inadaptation du système répressif se juge sur l'effectivité de la sanction pénale en la matière. Or, il est constaté un manque d'effectivité de la sanction pénale tant à l'égard des opérateurs des

réseaux sociaux en raison de la souplesse du régime de responsabilité qui leur est accordé que de leurs utilisateurs en raison de l'incapacité de l'autorité judiciaire à se saisir de l'ensemble du contentieux généré par ces sites. Ce constat amène à conclure à une inadéquation des règles de responsabilité actuelles applicables aux acteurs des réseaux sociaux et justifie dès lors un mouvement d'adaptation du droit visant à reconférer à la loi pénale une certaine effectivité.

594. L'évolution des modes de réponse aux infractions dans le domaine numérique aurait pour conséquence de pallier les carences des voies répressives traditionnelles. Le choix d'une régulation numérique des contenus illicites paraît en l'occurrence pouvoir répondre aux enjeux suscités par les sites de réseaux sociaux. Une régulation de l'expression à l'échelle numérique permettrait d'une part de parer l'incapacité du juge pénal à se saisir de l'ensemble du contentieux rencontré sur les sites de réseaux sociaux et d'autre part de responsabiliser les plateformes numériques dans la gestion des contenus qu'elles génèrent. La régulation des contenus, intervenant en complément et non en substitution de la sanction pénale, tendrait donc vers un meilleur respect de l'ordre public à l'échelle numérique. Ce pouvoir régulateur à visée préventive peut cependant se révéler d'une particulière dangerosité dès lors qu'il légitime l'instauration d'une police privée des contenus relevant de la seule interprétation des opérateurs des réseaux sociaux. À ce titre, la trop grande souplesse du système de responsabilité de *notice and take down* a permis, insidieusement, le développement d'une autorégulation des sites de réseaux sociaux entraînant un affaiblissement de l'ordre public européen au profit d'une interprétation plus libérale, davantage conforme au système de pensée américain. Cette modération des contenus effectuée directement et seulement par les opérateurs des réseaux sociaux a fait perdre au droit une de ses fonctions première, à savoir introduire un tiers dans les rapports sociaux afin que les conflits soient réglés avec recul et neutralité[1569]. Il est alors nécessaire de rétablir cet équilibre en introduisant un nouveau régime juridique applicable aux opérateurs des réseaux sociaux accompagné de nouveaux outils juridiques capables de rétablir un ordre public numérique à l'échelle nationale voire européenne et de garantir son application effective. Ce mouvement est justement entrepris par le législateur français qui souhaite proposer un nouvel encadrement des opérateurs des réseaux sociaux afin de proposer une meilleure régulation de l'expression en ligne. Cette dynamique réformatrice pleinement justifiée ne doit cependant pas avoir pour conséquence d'aboutir à un affaiblissement du droit à la liberté d'expression des utilisateurs des réseaux

[1569] En ce sens : F. OST, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant, 1ère éd., 2016.

sociaux par une modération outrancière des contenus. Pour ce faire, il est nécessaire de conférer au nouveau régime de responsabilité des obligations équilibrées et mesurées n'induisant pas une sur-responsabilisation des plateformes. Un tel système de responsabilité ne doit par ailleurs pas justifier un amenuisement du rôle du juge pénal qui demeure l'autorité la plus légitime à fixer les limites admissibles en matière d'expression, y compris dans le domaine numérique. Ainsi, si une adaptation du droit au mouvement d'expression massif rencontré sur les sites de réseaux sociaux est nécessaire, elle ne doit pas aboutir à un affaiblissement des principes fondamentaux de ce dernier sous couvert d'une réaction justifée. Enfin, il doit être relevé que ces changements engagés dans le régime de responsabilité applicable aux grandes plateformes numériques impulsent une évolution en leur sein s'observant notamment par la mise en place progressive d'une logique de mise en conformité visant à adapter leurs modes de fonctionnement aux exigences de l'espace juridique français et plus largement européen.

Conclusion générale

595. Un droit pénal d'ores et déjà adapté. Les réseaux sociaux en ligne doivent être avant tout perçus comme un nouvel espace juridique ouvert aux règles préexistantes, tout autant qu'internet en général. Ainsi selon Monsieur le Professeur Valère Ndior les réseaux sociaux en ligne constitueraient : « *des plateformes d'hébergement agissant en tant qu'intermédiaires techniques dans le but de mettre à disposition du public, à titre personnel ou professionnel, des moyens et espaces de communication ou d'interaction avec d'autres utilisateurs. Le titulaire d'un compte de réseau social y agit en tant qu'éditeur de contenu sur un profil présumé relever de l'espace public, sauf à ce qu'il démontre que les contacts qu'il a agréés forment une communauté d'intérêts dans laquelle les données publiées demeurent sujettes à son contrôle* »[1570]. Le droit pénal démontre alors en nombreux points son adéquation et sa capacité à transcender les évolutions sociétales. Ce constat vaut particulièrement pour le corpus d'incriminations qu'il met en œuvre. En réalité, les comportements cyberdélinquants observés sur les réseaux sociaux en ligne sont pour leur grande majorité, la transcription à l'échelle numérique de comportements qui étaient déjà auparavant appréhendés par le droit pénal. Ainsi, si les sites de réseaux sociaux manifestent un nouveau stade d'avancement de nos sociétés, les valeurs sociales protégées par le droit pénal demeurent pour l'essentiel d'entre elles inchangées et la neutralité technologique des textes d'incrimination permet de saisir des nouvelles formes de comportements qui ne constituent pas pour autant une nouvelle délinquance ou criminalité. Le droit pénal ne doit donc pas être pensé comme un moyen de réaction automatique à chaque épiphénomène constaté à l'échelle numérique, la surpénalisation de certains comportements s'exerçant alors au détriment des principes fondamentaux de la matière et partant, de sa puissance.

596. Un droit pénal qui s'adapte. Toutefois, conclure que le droit pénal s'avère parfaitement adapté aux sites de réseaux sociaux est erroné. Le fort impact sociétal de ces sites justifie des adaptations qui manifestent en réalité des évolutions profondes au sein de cette matière. L'adoption de nouveaux textes en droit pénal se trouve dans ce cas justifiée dès

[1570] V. NDIOR, « Le réseau social : essai d'identification et de qualification », *in* V. NDIOR (dir.), *Droit et réseaux sociaux*, éd. Lextenso, coll. LEJEP, octobre 2015, p. 35.

lors qu'ils respectent sa philosophie et que le recours à de nouveaux instruments répressifs demeure rationnel.

597. En premier lieu, il a été identifié deux carences d'ordre structurel dans le corpus des incriminations ayant pleinement justifié l'adoption de deux nouvelles incriminations à savoir le délit d'usurpation d'identité numérique[1571] et le délit de diffusion non consentie de l'intimité d'autrui[1572]. Si ces deux nouvelles incriminations ne sont pas exemptes de critiques du point de vue de la légistique, leur légitimité ne fait cependant pas débat. Il s'agit d'une hypothèse rare en droit pénal où, suite à l'évolution de valeurs sociales protégées, il devient nécessaire de pénaliser de nouvelles formes de comportements. Sur ce point, les réseaux sociaux en ligne ont forgé de manière durable un nouvel espace d'expression de l'identité individuelle poussant le législateur à protéger pénalement et indépendamment l'identité dans son versant numérique. De même, à l'heure du web social la protection de l'intimité a nécessité de profonds changements. Il n'est plus uniquement question de protéger les individus contre une immixtion dans leur intimité mais également de pénaliser la divulgation non consentie de l'intimité d'autrui qui est devenue techniquement une pratique facilement réalisable sur les sites de réseaux sociaux. Au vu de ces observations, il peut être conclu que l'usage massif des sites de réseaux sociaux a initié une évolution de la protection pénale de la vie privée allant dans le sens général d'une extension de son champ d'application.

598. En second lieu, l'environnement des sites de réseaux sociaux amène au constat de l'inadaptation de certains régimes de responsabilité pénale applicables aux utilisateurs de ces sites mais également à leurs opérateurs. Les raisons sont différentes mais la conséquence est la même : le manque d'effectivité de la norme pénale. Ainsi, les opérateurs des réseaux sociaux en ligne qui bénéficient du statut juridique favorable des hébergeurs ne voient que très rarement leur responsabilité pénale engagée. Les utilisateurs quant à eux, en tant qu'éditeurs de services, sont soumis à un régime juridique d'une particulière exigence pensé à l'origine pour des professionnels. Cette sévérité d'apparence n'est cependant que d'une faible utilité, voire contre-productive au regard des nombreux rapports et études décriant le manque d'effectivité de la sanction pénale en matière d'abus de la liberté d'expression. Pis encore, le régime de responsabilité pénale des opérateurs basé sur le système de *notice and take down* a entraîné un recul du droit national et européen au profit des règles propres aux sites de réseaux sociaux définies dans leurs conditions générales d'utilisation. Le droit pénal se doit

[1571] C. pén., art. 226-4-1.
[1572] C. pén., art. 226-2-1.

alors d'évoluer afin de retrouver son effectivité mais surtout pour ne pas abandonner la gestion de l'ordre public numérique à des plateformes numériques privées. Cependant, le droit pénal ne doit pas, dans cette hypothèse, être pensé comme l'unique voie pour parvenir à ces résultats. L'extraordinaire masse de contentieux qui doit être gérée impose de suggérer l'intervention de l'autorité administrative qui poursuivrait le même but que le droit pénal, à savoir préserver l'ordre public et donc les libertés à l'échelle numérique. Ce pouvoir concurrent entre le droit pénal et l'autorité administrative est un succès concernant le pouvoir d'intervention de la CNIL, concurremment au juge pénal, dans la protection des données à caractère personnel faisant l'objet d'un traitement. L'autorité administrative indépendante dispose ainsi aujourd'hui, en raison de sa spécialisation dans le domaine, d'une véritable légitimité mais surtout d'un réel pouvoir dissuasif au regard des fortes capacités de sanctions dont elle a été progressivement investie. Dans le même ordre d'idée, le législateur français souhaite désormais étendre les missions du CSA de manière à en faire une autorité de supervision des grandes plateformes numériques. Cette dernière aurait pour mission de veiller, dans le cadre de la régulation des contenus notifiés, au bon respect du principe de liberté d'expression et de ses limites envisagées par la loi sur la liberté de la presse. Cette régulation qui touche le domaine sensible de la liberté d'expression ne doit cependant pas voir le rôle du juge pénal s'amoindrir, le droit pénal se doit alors également d'évoluer de manière à disposer d'instruments juridiques forts. Il est dès lors nécessaire que le nouveau système de responsabilité se dessinant à l'article 6-3 de la LCEN propose une juste balance entre les rôles du juge pénal et de l'autorité administrative. Plus largement, le droit pénal démontre en la matière un pouvoir d'influence sur les sites de réseaux sociaux en encadrant ces derniers dans un nouveau régime de responsabilité et en les poussant à adopter par eux-mêmes, à travers une logique de mise en conformité, les comportements adéquats à l'environnement juridique européen. Partant, on peut constater que si les réseaux sociaux en ligne ont un pouvoir d'influence sur le droit pénal, l'inverse se vérifie également : les évolutions législatives et les réformes engagées sont de nature à influencer la politique de gestion de ces espaces d'échanges.

599. Un droit en mutation. Le nouveau système de responsabilité qui reconnaît et encadre le pouvoir régulateur des sites de réseaux sociaux, révèle par-delà l'émergence d'une forme alternative de normativité. Les algorithmes mis en œuvre par ces sites mais également leurs conditions générales d'utilisation constituent de nouveaux objets juridiques encore mal identifiés qui produisent pourtant un effet régulateur sur l'expression à l'échelle mondiale. Si

les États, particulièrement l'État français, réagissent en proposant un encadrement de ce pouvoir de régulation, force est de constater l'émergence de nouveaux acteurs clés disposant d'une hégémonie technologique et remettant en cause le système politique traditionnel pyramidal de l'État souverain, favorisant le glissement progressif vers un système en réseau caractérisé par une multitude d'acteurs[1573]. Les États se doivent, en tant que gardien de l'ordre public et des libertés, de conserver un pouvoir coercitif suffisant à l'égard des grandes plateformes numériques guidées quant à elles par une logique marchande et de ce fait trop éloignée de la notion d'intérêt général. L'Union européenne possède alors la capacité de s'ériger en contrepoids politique à ces grands acteurs dominants de l'économie numérique. Le groupe de l'article 29 constitué des CNIL européennes a ainsi démontré la capacité de l'Union européenne à se rassembler afin de défendre d'une voix commune les droits de ses citoyens. La réforme entreprise en France concernant le CSA constitue une nouvelle opportunité pour l'Union européenne de prouver sa capacité à se rassembler dans le but de protéger les droits et libertés et de forger un peu plus l'identité de l'espace juridique européen.

[1573] V. sur le sujet : F. OST, M. VAN de KERCHOVE, *De la pyramide au réseau ?*, Facultés Universitaires Saint-Louis Bruxelles, 2010.

Bibliographie

I. OUVRAGES GENERAUX, TRAITES, MANUELS, DICTIONNAIRES

ARIÈS Ph., DUBUIS G., *Histoire de la vie privée*, tome 3, De la Renaissance aux lumières, Points d'histoire, n°262.

Association H. CAPITANT, *Vocabulaire juridique*, G. CORNU (dir.), PUF, 12ème éd., 2018.

BECCARIA C., *Des délits et des peines*, ENS éd., 2009.

BÉGUEC D. Le, *Dictionnaire de la culture juridique*, Paris, PUF, 2003.

BEIGNIER B., LAMY B. de, DREYER E. (dir.), *Traité de droit de la presse et des médias*, Litec, 2009.

BEIGNIER B., *Le droit de la personnalité*, coll. « Que sais-je ? », PUF, 1992.

BOULOC B., *Droit pénal général*, Dalloz, coll. Précis, 26ème éd., 2019.

BRUGIÈRE J.-M., GLEIZE B., *Droits de la personnalité*, ellipses, 2015.

CABRILLAC R., *Dictionnaire du vocabulaire juridique*, Litec, 9e éd., 2018.

CARBONNIER J., *Droit civil. Introduction. Les personnes. La famille, l'enfant, le couple,* PUF, coll. « Quadrige », 2004.

CONTE P., *Droit pénal spécial*, LexisNexis, 4ème éd., 2013.

GOUBEAUX G., *Traité de droit civil. Les personnes*, LGDJ, 1989.

CORNU G., *Droit civil, les personnes*, Montchrestien, 13ème éd., 2007.

DEBBASCH C. (dir.), *Droit des médias*, Dalloz, 2002.

DEBET A., MASSOT J., METALLINOS N., *Informatique et libertés*, LGDJ, vol. 10, 2015.

DERIEUX E., *Droit de la communication*, LGDJ, 3ème éd. 2011.

DERIEUX E., *Droit des médias*, LGDJ, 7ème éd., 2015.

DESPORTES F., LAZRERGUE-COUSQUER L., *Traité de procédure pénale*, Economica, 3ème éd., 2013.

DREYER E., *Responsabilités civiles et pénales des médias*, Litec, 2008.

DREYER E., *Droit pénal spécial*, Ellipses, 3ème éd., 2016.

DREYER E., *Droit pénal général*, LexisNexis, 5ème éd., 2019.

GINCHARD S., BUISSON J., *Procédure pénale*, LexisNexis, 12ème éd., 2019.

MALAURIE P., AYNÈS L., STOFFEL-MUNCK P., *Droit des obligations*, LGDJ, 9ème éd., 2017.

MERLE R., VITU A., *Traité de droit criminel, Droit pénal spécial*, Cujas, 1982.

MERLE R., VITU A., *Traité de droit criminel. Problèmes généraux de la science criminelle, droit pénal général*, éd. Cujas, 4ème éd. 1981.

PLANIOL M., *Traité élémentaire de droit civil*, LGDJ, tome 1, 8ème éd., 1920.

PRADEL J., *Droit pénal général*, Cujas, 19ème éd., 2012.

PRADEL J., *Procédure pénale*, Cujas, 19ème éd., 2017.

PRADEL J., VARINARD A., *Les grands arrêts du droit pénal général*, Dalloz, 8ème éd., 2013.

REBUT D., *Droit pénal international*, Dalloz, coll. précis, 2ème éd., 2014.

RASSAT M.-L., *Droit pénal spécial*, Dalloz, coll. Précis, 8ème éd., 2018.

RASSAT M.-L., *Droit pénal général*, Ellipses, 4ème éd., 2017.

RIVERO J., MOUTOUH H., *Liberté publiques*, Thémis Droit public, Tome 1, 9ème éd., 2003.

ROCHFELD J., *Les grandes notions du droit privé*, puf, 2013.

ROLAND H., BOYER L., *Adages du droit français*, 1999, Litec, no 452.

SAINT PAU J.-C. (dir.), *Droit de la personnalité*, Lexis-Nexis, Traités, 2013.

STASIAK F., *Droit pénal des affaires*, LGDJ, 2ème éd., 2009.

SUDRE F., *Droit européen et international des droits de l'homme*, PUF, coll. « Droit fondamental », 10ème éd., 2011.

TERRÉ F., SIMLER P., LEQUETTE Y., *Droit civil. Les obligations*. Dalloz, 11ème éd., 2013.

VÉRON M., *Droit pénal spécial*, Sirey, 16ème éd., 2017.

VINEY G., *Traité de droit civil. Introduction à la responsabilité*, LGDJ, 3ème éd, 2008.

VOIRIN P., GOUBEAUX G., *Droit civil*, LGDJ, 38ème éd., Tome 1, 2018.

II. THESES, OUVRAGES SPECIAUX, MONOGRAPHIES

ABRAVANEL-JOLLY S., *La protection du secret en droit des personnes et de la famille*, Defrénois, coll. « Doctorat & Notariat », 2005.

ALIX J., *Terrorisme et droit pénal, étude critique des incriminations terroristes*, Nouvelle bibliothèque des thèses, Dalloz, 2010.

ATIAS C., *Devenir juriste. Le sens du droit*, LexisNexis, Carré Droit, 2011.

BENYEKHLEF K. (dir.), *Vers un droit global ?*, Montréal, Éditions Thémis, 2016.

BESSE T., *La pénalisation de l'expression publique*, Thèse, Université de Limoges, 2018.

BIGOT C., *Pratique du droit de la presse*, éd. Victoires, PUF, 2013.

BIGOT C., *Connaître la loi de 1881 sur la presse*, PUF, 2004.

BITAN H., *Droit et expertise du numérique*, coll. Lamy Axe Droit, 2015.

CACHARD O., *La régulation du marché électronique*, LGDJ, 2002.

CAILLET M.-C., *Le droit à l'épreuve de la responsabilité sociétale des entreprises : étude à partir des entreprises transnationales*, Thèse, Université de Bordeaux IV, 2014.

CARBONNIER J., *Flexible droit, pour une sociologie du droit sans rigueur*, LGDJ, 10ème éd., 2001.

CASSIA P., *Dignité(s) : une notion juridique insaisissable ?*, Dalloz, coll. Les sens du droit, 2016.

CHAUVET D., *Vie privée, étude de droit privé*, Thèse, Université de Paris-Sud, 2014.

CORNU G., *Droit civil approfondi : l'apport des réformes récentes du code civil sur la théorie du droit civil*, Cours de doctorat, Les cours de droit, 1970.

COURTAIGNE C., *L'adéquation du droit pénal à la protection de l'environnement*, Thèse, Université de Paris II (Panthéon-Assas), 2010.

DARBELLAY J., *Théorie générale de l'illicéité*, Fribourg, éd. universitaire, 1955.

DELIEGE F., *La responsabilité des acteurs de l'internet en matière de délits de presse*, thèse, Université de Nancy 2, 2006.

DERIEUX E., *Droit des médias. Droit français, européen et international*, 8ème éd., LGDJ, 2018.

DERIEUX E., GRANCHET A., *Les réseaux sociaux en ligne. Aspects juridiques et déontologiques*, Lamy, coll. Axe Droit, Paris, 2013.

DONNAT F., *Droit européen de l'internet, Réseaux, données services*, LGDJ, Systèmes, 2018.

DREYER E., *Responsabilité civile et pénale des médias*, LexisNexis, 3ème éd., 2012.

DREYER E., *Droit de la communication*, LexisNexis, 2018.

DREYFUS N., *Marques et internet. Protection, valorisation, défense*, Lamy, coll. Axe Droit, 2011.

DROIN N., JEAN-BAPTISTE W. (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, coll. Grands Colloques, 2017.

EYNARD J., *Les données personnelles, Quelle définition pour un régime de protection efficace ?*, Michalon, 2013.

FÉRAL-SCHUHL C., *Cyberdroit. Le droit à l'épreuve de l'internet*, 7ème éd., Dalloz, 2018-2019.

FAUCHOUX V., DEPREZ P., *Droit de l'internet*, Litec, Paris, 2009.

FOREST D., *Droit des données personnelles*, Gualino, coll. « Droit en action », 2011.

FOUGÈRE L., *Du délit de fausses nouvelles*, thèse, Université de Nancy, 1943.

FRISON-ROCHE M.-A. (dir.), *Régulation, Supervision, Compliance*, Dalloz, coll. Thèmes et commentaires, 2017.

FRYDMAN B., *Petit manuel pratique de droit global*, Bruxelles, Académie royale de Bruxelles, 2014.

FRYDMAN B., BRICTEUX C. (dir.), *Les défis du droit global*, Bruylant, 2017.

FRYDMAN B. et CHEROT J.-Y. (dir.), *La science du droit dans la globalisation*, Bruxelles, Bruylant, 2012.

FRYDMAN B., LEWKOWICZ G., *Le droit global selon l'Ecole de Bruxelles*, Bruxelles, Académie royale de Belgique, 2017.

FRYDMAN B., LEWKOWICZ G. (dir.), *Les théories du droit global*, Paris, Presses de Sciences Po, 2017.

GAUDEMET A. (dir.), *La compliance : un monde nouveau ?*, Paris, éd. Panthéon-Assas, 2016.

GOHIN O., *Institutions administratives*, LGDJ, 7ème éd., 2016.

GOMES B., *Le droit du travail à l'épreuve des plateformes numériques*, Thèse, Université de Paris-Nanterre, 2018.

ITEANU O., *L'identité numérique en question*, Eyrolles, 2008.

ITEANU O., *Quand le digital défie l'État de droit*, Eyrolles, 2016, p. 20.

JOSSERAND L., *De la responsabilité du fait des choses inanimées*, éd. A. Rousseau, 1897.

KAPLAN D., *Informatique, libertés, identités*, FYP, 2010.

KNOBEL M., *L'internet de la haine*, Berg International Éditeurs, 2012.

LAURENT M., BOUZEFRANCE S. (dir.), *La gestion des identités numériques*, éd. Iste, 2015.

LEGER P., *La recherche d'un statut de l'œuvre transformatrice. Contribution à l'étude de l'œuvre composite en droit d'auteur*, LGDJ, 2018.

LEONHARD J., *Étude sur la pornographie pénalement prohibée*, Thèse, Université de Nancy 2, 2011.

LEVASSEUR G., *La protection pénale de la vie privée*, Études offertes à Pierre Kayser, Aix-en-Provence, PUF d'Aix-Marseille, 1979.

LOLIES I., *La protection pénale de la vie privée*, PUF Aix-Marseille, 1999.

LUCAS A., DEVEZE J., FRAYSSINET J., *Droit de l'informatique et de l'Internet*, PUF, Thémis droit, 2001.

MALECKI C., *Responsabilité sociale des entreprises, Perspectives de la gouvernance d'entreprise durable*, Paris, coll. Droit des affaires, LGDJ-Lextenso, 2014.

MATTATIA F., *RGPD et droit des données personnelles*, Eyrolles, 2018.

MATTATIA F., *Traitement des données personnelles*, Eyrolles, 2013.

MITNICK K. D., SIMON W. L., *L'art de la supercherie, l'importance du facteur humain dans la sécurité informatique*, CampusPress, 2011.

MUTELET V., VASSEUR-LAMBRY F., *Qui suis-je, dis moi qui tu es ?*, Artois Presses-Université, coll. Droit et Sciences économiques, 2015.

NDIOR V. (dir.), *Droit et réseaux sociaux*, éd. Lextenso, coll. LEJEP, octobre 2015.

NETTER E., *Numérique et grandes notions du droit privé*, CEPRISCA, coll. Essais, 2019.

OCHOA N., *Le droit des données personnelles, une police administrative spéciale*, Thèse, Université de Paris 1 Panthéon-Sorbonne, 2014.

OST F., *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant, 1ère éd., 2016.

OST F., VAN de KERCHOVE M., *De la pyramide au réseau ?*, Facultés Universitaires Saint-Louis Bruxelles, 2010.

PAILLER L., *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Larcier, 2012.

PERROUD T., *La fonction contentieuse des autorités de régulation en France*, Nouvelle Bibliothèque de Thèses, Dalloz, Avril 2013.

PHILIPPOT P., *Les infractions de prévention*, Thèse, Université de Nancy II, 1977.

PONSEILLE A., *L'infraction de prévention en Droit pénal français*, Thèse, Université de Montpellier, 2001.

POULLET Y., *La vie privée à l'heure de la société du numérique*, Larcier, coll. CRIDS, 2019.

QUEMENER M., *Le droit face à la disruption numérique*, Gualino, 2018.

QUÉMÉNER M., CHARPENEL Y., *Cybercriminalité Droit pénal appliqué*, Economica, 2010.

RASCHEL E., *La procédure pénale en droit de la presse. Presse & édition, radio & télévision, internet, expressions orales et écrites, publiques et non-publiques*, Gazette du Palais, Guide pratique, 2019.

RAVANAS J., *La protection des personnes contre la réalisation et la publication de leur image*, LGDJ., coll., « Bibliothèque de droit privé », 1978.

REVET T. (dir.), *L'inflation des avis en droit*, Economica, 1998.

REBILLARD F., *Le web 2.0 en perspective. Une analyse socio-économique de l'internet*, L'Harmattan, 2007.

RISSOAN R., *Les réseaux sociaux: Facebook, Twitter, Linkedln, Viadeo, Google +, comprendre et maîtriser ces nouveaux outils de communication*, Objectif web, Éditions ENI, 2ème éd., 2011.

ROCHELANDET F., *Économique des données personnelles*, coll. Repères, La découverte, 2010.

SALEILLES R., *Les accidents du travail et la responsabilité civile : essai d'une théorie objective de la responsabilité délictuelle*, éd. A. Rousseau, 1897.

SAINT PAU J.-C, *L'anonymat et le droit*, Thèse, Université de Bordeaux IV, 1998.

SKAF F., *La justice pénale face à la cybercriminalité*, Éditions universitaires européennes, 2018.

STEWART D., *Social media and the law*, Routledge, Abingdon, 2013.

III. AUTRES : PHILOSOPHIE, SOCIOLOGIE, SCIENCES POLITIQUES, LITTÉRATURE

APPLEBY J., BALL T., *Thomas Jefferson. Political Writings*, New York, Cambridge University Press, 1999.

BASCH V., *L'individualisme anarchiste*, Paris, 1904, F. Alcan, réédition en 1928 et en 2008.

BLONDEAU O., *Libres enfants du savoir numérique. Une anthologie du « Libre »*, Éditions de l'Éclat, 2000.

BONALD (de) L. G. A., *Théorie du pouvoir politique et religieux*, 1796.

CARDON D., *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, Seuil, 2015.

CARDON D., *Culture numérique*, Presses de Science Po, 2019.

CARDON D., *La Démocratie Internet. Promesses et limites*, Seuil, Paris, 2010.

CAUCHAT H., DURAND-DELVIGNE A., *De l'identité du sujet au lien social*, Paris, PUF, 1999.

COMPIEGNE I., *La société numérique en question(s)*, Sciences Humaines éd., 2010.

DAGNAUD M., *Le modèle californien. Comment l'esprit collaboratif change le monde*, Odile Jacob, 2016.

ERTZSCHEID O., *Qu'est-ce que l'identité numérique ?*, OpenEdition Press, coll. « Encyclopédie Numérique », 2013.

FRIEDMAN D., *Vers une société sans État*, Paris, Les Belles Lettres, 1992, 2ème éd.

GOFFMAN E., *La mise en scène de la vie quotidienne. La présentation de soi*, tome 1, Les éditions de minuit, coll. Le sens commun, 1959.

HAYEK F., *La route de la servitude*, Paris, PUF, coll. « Quadrige », 2010.

HIMANEN P., *L'Éthique hacker et l'Esprit de l'ère de l'information*, Saint-Élie-de-Caxton (Québec), Exils, 2001.

HOBBES T., *Léviathan ou Matière, forme et puissance de l'État chrétien et civil*, Galimard, 2000.

HONNETH A., *La lutte pour la reconnaissance*, Cerf, Paris, 2007.

JACQUARD R., *La Guerre du mensonge. Histoire secrète de la désinformation*, Plon, 1986.

JEFFERSON T., *On Democracy*, éd. Saul K. Padover, New York, Penguin Books, 1946.

KAFKA F., *Le Procès*, éd. Gallimard, 1933.

LEVY S., *Hackers : Heroes of the Computer Revolution*, New York, Delta, 1984.

MARIENSTRAS É., *Les mythes fondateurs de la nation américaine. Essai sur le discours idéologique aux États- Unis à l'époque de l'indépendance (1763-1800)*, Paris, François Maspero, 1976.

McLUHAN M., *The Medium is the Massage*, Bantam Books, 1967.

MERCKLE P., *La sociologie des réseaux sociaux*, La Découverte, 3ème éd., 2016.

NOZICK R., *Anarchie, État et utopie*, Paris, PUF, 1974.

ORWELL G., *1984*, éd. Gallimard, 1950.

PARISER E., *The filter bubble: how the new personalized web is changing what we read and how we think*, Penguin books, 2012.

ROSNAY (De) J., *La Révolte du pronétariat. Des mass médias aux médias des masses*, Fayard, coll. Transversales, Paris, 2006.

SEGUR P., PIERE-FREY S., *L'internet et la démocratie numérique*, Presses Universitaires de Perpignan, 2016.

SUPIOT A., *La gouvernance par les nombres*, Fayard, 2015.

SIMMEL G., *Sociologie, études sur les formes de la socialisation*, Paris, PUF, 1999.

THOMSON D., *Les français jihadistes*, Les Arènes, 2014.

THOREAU H. D., *Walden; or, Life in the Woods*, Ticknor and Fields, 1854.

TISSERON S., *L'intimité surexposée*, Hachette littérature, 2001.

TURNER F., *Aux sources de l'utopie numérique. De la contre-culture à la cyberculture, Stewart Brand, un homme d'influence*, Caen, éd. C. & F., 2012.

VITRAL L., *Les Organisations Non Gouvernementales dans la régulation de l'économie mondiale*, L'Harmattan, 2008.

IV. ARTICLES, ÉTUDES, CHRONIQUES ET FASCICULES

ADER B.,

« Évolution de la notion de publication : de la presse écrite à Internet », *Légipresse*, octobre 1999, n° 165, p. 123.

« les "amis" sur Facebook forment une communauté d'intérêts », *Légipresse* n° 35, mai 2013, p. 312.

« La loi de 1881, réceptacle naturel de toutes les infractions de "publication", depuis la presse et l'imprimerie jusqu'à internet », *Légicom* n° 57, 2016/2 », p. 19.

ACHILLEAS P.,

« Internet et libertés », *J.-Cl.* Libertés, fasc. n° 820, 2007.

AFROUKH M.,

« La liberté d'expression face aux discours haineux en ligne dans la jurisprudence de la Cour européenne des droits de l'homme », *Dalloz IP/IT* 2017, p. 575.

AGRE P. E., ROTENBERG M.,

« Technology and privacy. The New Landsacpe », *MIT Press*, 1998, p. 3.

AIGOUY C.,

« Le revenge porn ou la revanche du principe d'interprétation stricte de la loi pénale », *LPA* , 21 avril 2016, n° 80, p. 13.

ALIX J.,

« Réprimer la participation au terrorisme », *RSC* 2014, p. 849.

ALLARD L., VANDENBERGHE F.,

« Express Yourself ! Les pages perso. Entre legitimation technopolitique de l'individualisme expressif et authenticité réflexive peer to peer », *Réseaux*, vol. 21, n° 117, 2003, p. 191-220.

ALTERMAN H. et BLOCH A.,

« La fraude informatique », *Gaz. Pal.* 1988, 2, doctr. p. 530, spéc. p. 532.

ANDRÉ S.,

« Que peut-on montrer sur sa photo de profil Facebook ? », *in* C. MANARA (dir.), *Réseaux sociaux : 101 questions juridiques*, éd. Diateino, 2013.

APPLEBY J.,

« Liberalism and the American Revolution », *The New England Quarterly*, vol. 49, n° 1, mars, 1976, p. 3.

C. ATTIAS, D. LINOTTE,

« Le mythe de l'adaptation du droit au fait », *D.*, 1977, p. 251.

AUVRET P.,

« Fausses nouvelles », *J.-Cl.* Comm., fasc. n° 3210, 2003.

AUVRET P. et AUVRET C.,

« Délits de presse sur Twitter et responsabilité », *Légipresse* n° 353, 12 octobre 2017, p. 481.

AZZI T.,

« La responsabilité des nouvelles plates-formes : éditeurs, hébergeurs ou autre voie ? », *in Contrefaçon sur Internet. Les enjeux du droit d'auteur sur le web 2.0*, LexisNexis, coll. IRPI, 2009, n° 33, p. 75.

BADINTER R.,

« La protection de la vie privée contre l'écoute électronique clandestine », *JCP*, 1971, I, chron. n° 2435.

« Le droit au respect de la vie privée », *JCP* éd. G 1968, I, n° 2136.

« De la nécessaire répression du négationnisme en France », *in* Mélanges en l'honneur de Jean-Claude Colliard, Dalloz, avril 2014, p. 51.

BAILLY E., DAOUD E.,

« Cybercriminalité et réseaux sociaux: la réponse pénale », *AJ Pénal* 2012, p. 252.

BARLOW J. P.,

« Déclaration d'indépendance du cyberespace », *in* O. BLONDEAU, *Libres enfants du savoir numérique. Une anthologie du "Libre"*, éd. de l'Éclat, 2000, p. 51.

BARNES J. A.,

« Class and Committees in a Norwegian Island Parish », *Human Relations*, 1954.

BARRAUD B.,

« La lutte contre les fausses informations sur internet : un jeu de lois », *RLDI* décembre 2018, n° 154.

BAUER A.,

« *Le terrorisme singulier est devenu pluriel. Alors que les terrorismes d'État ou nationalistes sont en voie de disparition ou de pacification, de nouveaux opérateurs voient le jour et organisent des opérations marquées par une forte décentralisation, voire une « ubérisation » des acteurs et des modalités d'action* » *in* « Les mutations du terrorisme », *Pouvoirs*, vol. 158, n° 3, 2016, p. 97.

BÉCOURT D.,

« Réflexion sur le projet de loi relatif à la vie privée », *Gaz. Pal.* 1970, I, p. 202.

BEIGNIER B.,

« Vie privée et vie publique », *Arch. phil. droit*, 1997, n° 41, p. 163.

« La protection de la vie privée », *in* : *Libertés et droits fondamentaux*, coll. CRFPA Grand oral, Dalloz, 2014.

BELFANTI L. et BELLOIR P.,

« La "conventionnalité" de l'article 38 ter de la loi de 1881 », *RLDI*, 2010, n° 64.

BERGERON D.,

« Thomas Jefferson et la réflexion sur l'Autochtone. Conception d'une nature au fondement d'un projet humain », *Revue française de science politique*, vol. 67, n° 3, 2017, p. 497.

BERNARD F.,

« Les théories de l'influence en communication : perspectives nord-américaines et françaises », *Hermès, La Revue* 2015/1, n° 71, p. 45.

BIGOT C.,
« Application de la loi de 1881 à l'internet », *Légipresse* n° 168, janvier-février 2000, p. 23, n° 3.

BLANC C.,
« Identité numérique et réseaux sociaux », *in* : *Qui suis-je, dis-moi qui tu es. L'identification des différents aspects juridiques de l'identité*, Études réunies par V. MUTELET et F. VASSEUR-LAMBRY, Droit et Sciences économiques, Artois Presses-Université, 2015, p. 126.

BLAYA C.,
« Nature et prévalence de la cyberviolence et du cyberharcèlement », *in* : C. BLAYA (dir.), *Les ados dans le cyberespace. Prises de risque et cyberviolence*, De Boeck Supérieur, 2013, p. 47.

BONNAL N.,
« Les responsabilités de l'amateur internaute au regard du droit de la presse », *Légicom*, n° 41, 2008/1, p. 15.

BOSSAN J.,
« Responsabilité pénale en cascade dans la communication audiovisuelle et l'internet », *J.-Cl.* comm., fasc. n° 142, 2015 (mise à jour 2017).

BOULLIER D.,
« L'impossible définition des données personnelles », *Cahiers IP innovation et perspective* n°1 vie privée à l'horizon 2020 p. 32.

BOURGAULT-COUDEVYLLE D.,
« La protection pénale de l'identité », *in* : *Qui suis-je, dis-moi qui tu es. L'identification des différents aspects juridiques de l'identité*, Études réunies par V. MUTELET et F. VASSEUR-LAMBRY Droit et Sciences économiques, Artois Presses-Université, 2015, p. 258.

BOYD D.,
« Social Network Sites: Public, Private, or What ? », *The Knowledge Tree*, n° 13, mai 2007.

BOYD D., ELLISON N.,
« Social Network Sites: Definition, History, and Scholarship », *Journal of Computer Mediated Communication*, vol. 13, Issue 1, Octobre 2007, p. 210.

BOYER J.,
« La responsabilité "allégée" ds directeurs de publication de services de communication au public en ligne à raison des messages d'internautes sur les espaces de contributions personnelles », *Légicom* n° 45, 2010/2, p. 80.

BOYER P.-X.,
« La judiciarisation de l'Internet », *in* F. ROUVILLOIS (dir.), *La société au risque de la judiciarisation*, Litec, 2008, Colloques & débats, 2008, p. 55.

BRESSON (de) J. J.,
« Inflation des lois pénales et législatives ou réglementations "techniques" », *RSC* 1985, p. 245.

BRUNAUX G.,
« Le vol de compte de jeu vidéo », *CCE* n° 10, octobre 2011, Étude 17.

BUFFELAN J.-P.,
« La répression de la fraude informatique », *Expertises*, février 1988, p. 55.

BURGADE (De La) D.,
« La physionomie actuelle de la notion de diffamation politique », *LPA* 24 janvier 1997, n° 11, p. 13.

CANTAT-LAMPIN V.,
« Les atteintes à la personne par le biais des communications électroniques. Une réponse imparfaite du droit pénal », in *Entre tradition et modernité : le droit pénal en contrepoint*, mélanges en l'honneur d'Yves Mayaud, Dalloz, 2017, p. 307.

CAPPELLO A.,
« L'adaptation du régime de responsabilité pénale au support d'Internet », *in* N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, coll. Grands colloques, 2017, p. 198.
« Autorités administratives indépendantes », Rép. pén. Dalloz, octobre 2016.
« Retour sur la jurisprudence du Conseil constitutionnel relative aux sanctions administratives », *RSC* 2010, p. 415.

CAPRIOLI É.,
« Protection de l'information – atteinte à l'e-réputation de l'entreprise et de ses salariés », *CCE* n° 10, octobre 2015, comm. 85.
« Usurpation d'identité par création d'adresses mails et de faux profils Facebook », *CCE* n° 1, janvier 2015 comm. 9.
« Condamnation d'un député pour des propos racistes publiés sur son mur Facebook », *CCE* n° 2, février 2014, comm. 23.

CARDON D.,
« Le design de la visibilité. Un essai de cartographie du web 2.0 », *Réseaux*, vol. 26, n° 152, 2008, p. 99.

CARDON D., SMOREDA Z., BEAUDOIN V.,
« Sociabilités et entrelacement des medias », *in* P. MOATI (dir.), *Nouvelles technologies et modes de vie. Aliénation ou hypermodernité ?*, Éditions de l'Aube, 2005.

CARE S.,
« Racines théoriques du libertarianisme américain », *Cités*, vol. 46, n° 2, 2011, p. 137.

CARPENTIER F.,
« Le corps humain, instrument d'une identité révélée : les dérives de la biométrie », *in* : *Qui suis-je, dis-moi qui tu es. L'identification des différents aspects juridiques de l'identité*, Études réunies par V. MUTELET et F. VASSEUR-LAMBRY, Droit et Sciences économiques, Artois Presses-Université, 2015, p. 233-250.

CARRIE L.,
« L'influenceur digital », *Légipresse* n° 368, février 2019, p. 83.

CASTETS-RENARD C.,
« Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet », *D.* 2012, p. 817.

CASSUTO T.,
« Usurpation d'identité numérique », *AJ Pénal* 2010, p. 220.

CATELAN N. et PERRIER J-B.,
« L'entreprise individuelle de terroriste et les axiomes du Conseil constitutionnel », *D.* 2017, p. 1180.

CATTAN J.,
« L'obtention des données d'utilisation des réseaux sociaux », *in* V. NDIOR (dir.), *Droit et réseaux sociaux*, éd. Lextenso, coll. LEJEP, octobre 2015, p. 138.

CAZÉ-GAILLARDE N.,
« Atteinte à la vie privé », Rép. pén., Dalloz, Mai 2005.

CHAFIOL-CHAUMONT F.,
« Retour sur l'obligation de conservation des données d'identification après la parution du décret du 25 février 2011 », *RLDI* mai 2011, n° 71.

CHAVANNE A.,
« La protection de la vie privée dans la loi du 17 juillet 1970 », *RSC*, 1970, p. 614.

CHAVENT-LECLERE A.-S.,
« Le renouveau des infractions sexuelles à l'ère d'internet », *in* Mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, p. 341.

CHEVALLIER J.,
« Le statut des autorités administratives indépendantes : harmonisation ou diversification ? », *RFDA* 2010, p. 896.

CHOPIN F.,
« Cybercriminalité », Rép. pén. Dalloz, Juillet 2013.

COMBLES (de) NAYVES (de) P.,
« Sauf en matière terroriste », *AJ Pénal* 2014, p. 528.

CONTE Ph.,
« Diffusion d'une photographie sans le consentement de l'intéressé », *Dr. pén.* n° 5, mai 2016, comm. 73.
« Une nouvelle fleur de légistique : le crime en boutons. À propos de la nouvelle définition du harcèlement sexuel », *JCP* G n° 30, 24 juillet 2002, act. 320.

COSTES L.,
« Réseaux sociaux: nouveaux enjeux et nouveaux défis pour les entreprises », *RLDI* août 2011, n° 74.

CREDEVILLE A.-E.,
« Fausses nouvelles et nouvelles fausses : la réponse du droit », *Légipresse* n° 364, octobre 2018, p. 468-469.

CROZE H.,
« L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique) », *JCP G* 1988, I, 3333, spéc. n° 7.

DAHAN V., TEMPIER H.,
« Les sites participatifs du web 2.0 sont des hébergeurs: est-ce la fin d'une controverse ? », *RLDI* avril 2011, n° 69.

DALLOZ M.,
« Circonstances aggravantes », Rép. pén., Dalloz, Juin 2017, n° 11 et suiv.

« Quel droit pénal pour réguler l'économie collaborative ? », *in* : *Quelles régulations pour l'économie collaborative ?*, Dalloz, 1ère éd., 2018, p. 159.

DAMON J.,

« La pensée de... Georg Simmel (1858 1918) », *Informations sociales*, vol. 123, nº 3, 2005.

DAOUD E. et PÉRONNE G.,

« *Cyberattaques : la lutte s'intensifie* », *AJ Pénal* 2015, p. 396.

DEBET A.,

« Facebook condamné à une sanction pécuniaire de 150 000 euros par la CNIL », *CCE* n° 7-8, juillet 2017, comm. 67.

« Dans la famille Facebook, la CNIL s'intéresse désormais à WhatsApp », *CCE* n° 5, mai 2018, comm. 38.

DECHENAUD D.,

« Interprétation, téléologique ou interprétation par analogie ? », *in Histoire et méthodes d'interprétation en droit criminel*, Dalloz, Thèmes Commentaires, 2015, p. 137.

DEFFAINS N., THIERRY J.-B.,

V° Fausse nouvelle, Rép. pén. Dalloz, juillet 2015.

DELAGE P.-J.,

« Happy slappers and bad lawyers », *D.* 2007, p. 1282.

DENIZEAU C.,

« L'Europe face au(x) discours de haine », *Revue générale du droit on line*, 2015, n° 21669.

DERIEUX E.,

« Réseaux sociaux et responsabilité des atteintes aux droits de la personnalité », *RLDI* février 2014, n° 100.

« Amateurs et médias : nouveaux défis juridiques ? », *Légicom*, n° 41, 2008/1, p. 22.

« Droit à l'information et droit au secret : pour un équilibre des droits », *Légipresse* 2011, nº 279, p. 3.

« Responsabilité des services de communication au public en ligne. Appréciation des contenus hébergés. Prendre la décision de colmater les fuites ? », *RLDI* février 2011, n° 68.

« Le pouvoir de sanction du Conseil supérieur de l'audiovisuel », *LPA* n° 52, 15 mars 2005, p. 3.

DESGENS-PASANAU G.,

« Le "*revenge porn"* n'est pas (toujours) une infraction pénale », *Dalloz IP/IT* 2016, Obs., p. 321.

DETRAZ S.,

« Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple », *RSC*, 2016, p. 741, n° 19.

« L'enregistrement d'images de violence : un cas de présomption légale de complicité », *Dr. pén.* 2007, étude 23.

DEVEZE J.,

« Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », *RLDI* 1987, mise à jour février 1988, p. 3, spéc. n° 53.

DEVILLIER N.,

« Cambridge Analytica et Facebook : "Le respect de votre vie privée nous tient à cœur." #OuPas », *The conversation*, Chron. juri-geek, 21 mars 2018.

DONATI P.,

« La relation comme objet spécifique de la sociologie », *Revue du MAUSS*, vol. nº 24, nº 2, 2004, p. 233.

DOUCET J.-P.,

« Les infractions de prévention », *Gaz. Pal.* 1973, octobre, p. 764.

DREYER E.,

« L'opportunité d'une sortie des infractions de presse de la loi du 29 juillet 14881 au regard d'un exemple précis : le cas du délit d'apologie du terrorisme et de provocation aux actes de terrorisme », *in* N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, coll. Grands Colloques, 2017, p. 38.

« "Liker" un contenu injurieux revient-il à injurier autrui ? », *D.* 2017, p. 1464.

« Accès frauduleux, indirect, mais certain, dans un STAD et détention du matériel le permettant », *RSC* 2018, p. 701.

« L'amateur sur Internet ou le blog rattrapé par le droit… », *Légicom*, n° 41, 2008/1, p. 22.

DREYFUS N.,

« Quel encadrement juridique pour le hashtag ? », *Expertises des systèmes d'information*, mars 2015, n° 400, p. 107.

DROIN N.,

« L'appréhension des discours de haine par les juridictions françaises : entre travail d'orfèvre et numéro d'équilibriste », *RevDH*, n° 14, 21 juillet 2018, p. 10.

DUBUISSON F.,

« Les restrictions à l'accès au contenu d'internet et le droit à la liberté d'expression », *in Internet et le droit international, société française pour le droit international*, colloque de Rouen, éd. A. Pedone, p. 156.

« Les ambivalences du rôle du juge pénal belge et français dans le répression du négationnisme réflexion à partir de l'affaire Assabyle », *in* J. ALLARD et O. CORTEN, *La vérité en procès le juge et la vérité politique*, Actes du colloque de l'ULB/ARC, 8-9 septembre 2011, LGDJ, p. 143.

DUPEYRON C.,

« L'infraction collective », *RSC* 1973, p. 357.

DUVERT C.,

« Harcèlement moral », *J.-Cl.* Pénal Code, art. 222-33-2, fasc. n° 20, 2003.

DUBEY G.,

« L'identité à l'épreuve de la biométrie », *in* S. LACOUR (dir.), *La sécurité aujourd'hui dans la société de l'information*, L'Harmattan, 2007, p. 87.

DUFOURQ P.,

« Répression des abus de marché : non bis in idem et bis repetita », *D. actu.*, 27 juin 2019.

DURAND-SOUFFLAND S.,
« Les comptes rendus d'audience, *Twitter* et le déroulement du procès en temps réel », *Légicom* n° 48, 2012/1, p. 75.

FASSASSI I.,
« Les effets des réseaux sociaux dans les campagnes électorales américaines », *Les nouveaux cahiers du Conseil constitutionnel*, octobre 2017, n° 57, p. 59.

FARIS D. M.,
« La révolte en réseau : le « printemps arabe » et les médias sociaux », *Politique étrangère*, vol. printemps, nº 1, 2012, p. 99.

FAVRO K.,
« La CNIL, une autorité à "l'âge de la maturité" », *Dalloz IP/IT* 2018 p. 464.

FELDMAN J.-P.,
« Les autorités administratives indépendantes sont-elles légitimes ? Sur les AAI et générale et le Conseil supérieur de l'audiovisuel en particulier », *D.* 2010, p. 2852.

FELLE T.,
« Changement d'algorithme sur Facebook : moins de contenus "médias", plus de recettes publicitaires », *The conversation*, 25 janvier 2018.

FERAL-SCHUHL C.,
« Facebook et la vie privée », *D.* 2010, 2824.

FOURREY T.,
« Twitter et le droit de la presse », *RLDI*, 2014, n° 109.

FRANCILLON J.,
« Piratage informatique. Usurpation d'identité numérique. L'affaire du "faux site officiel" de Rachia Dati : une étape dans la lutte contre la cyberdélinquance », *RSC* 2015, p. 101.
« Cyberharcèlement et interprétation stricte des textes en matière pénale », *RSC* 2016, p. 96.
« La compétence pénale territoriale française à l'épreuve de la cybercriminalité », *in* : Mélanges en l'honneur d'Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, p. 208.

FRANÇOIS P.,
« Pseudonyme en ligne. Remarques sur la vérité et le mensonge sur soi », *Sens-Dessous*, 2014/2, n° 14, p. 15-22.

FREDERIC J.-P.,
« La judiciarisation du maintien de l'ordre : des maux…aux actes ! », *AJ Pénal* 2013, p. 208.

FRINSON-ROCHE M.-A.,
« Réguler les "entreprises cruciales" », *D.* 2014, p. 1556.

FRYDMAN B.,
« A Pragmatic Approach to Global Law », *in* H. MUIR WATT and D. ARROYO, *Global Governance Implication of Private International Law*, Oxford University Press, 2015, p. 181.

FRYDMAN B., RORIVE I.,
« Regulating Internet Content through Intermediaries in Europe and the USA », Zeitschrift für Rechtssoziologie (revue de l'Institut Max Planck de Cologne), 2002, vol. 23 (1), p. 41.

GALMARD M.-H.,
« L'incrimination de la pratique du "vidéolynchage" ou la rupture du lien de causalité entre l'acte de complicité et l'infraction principale », *RPDP* 2007, n° 3, p. 583.

GASSIN R.,
« Le droit pénal de l'informatique », *D.* 1986, chron. p. 35.

GAUTIER P.-Y.,
« Le contenu généré par l'utilisateur », *Légicom*, n° 41, 2008/1, p. 8.

GEORGES F.,
« Représentation de soi et identité numérique. Analyse sémiotique et quantitative de l'emprise culturelle du Web 2.0 », *Réseaux*, 2009, vol. 27, n° 154, p. 165-193.
« L'identité numérique sous emprise culturelle. De l'expression de soi à sa standardisation », *Les Cahiers du numérique*, vol. 7, n° 1, 2011, p. 31.

GERVIER P.,
« L'ordre public et le numérique », *Politeia* n° 31, Les métamorphoses des droits fondamentaux à l'ère du numérique, 2017, p. 187.

GIRAULT C.,
« Identification et identité génétiques », *AJ Pénal* 2010, p. 224.

GONZALEZ G.,
« La liberté sexuelle », *in* F. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 157.

GOZLAN A.,
« Facebook : de la communauté virtuelle à la haine », *Topique*, vol. 122, n° 1, 2013, p. 121.

GRANET-LAMBRECHTS F.,
« Le droit à l'identité », *in* F. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 193.

GRANJON F. et DENOUEL J.
« Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux », *Sociologie*, 2010/1, vol. 1, p. 28.

GUIDERE M.,
« Le terrorisme avant et après l'État islamique », *Confluences Méditerranée*, vol. 102, n° 3, 2017, p. 65.

GUINIER D.,
« Cyberattaques. Macronleaks et diffusion de fausses informations », *Expertises des systèmes d'information*, juillet 2017, n° 426, p. 262.

GUNEHEC (Le) R.,
« Twitter et la vie d'avant : les réseaux sociaux changent-ils tout ? », *Légipresse* n° 355, décembre 2017, p. 597.

GUTMANN D.,
« Le sentiment d'identité », LGDJ, coll. « Bibliothèque de droit privé », 2000, p. 317, n° 381.

HARDOUIN R.,
« L'hébergeur et la publicité : la neutralité comme condition d'une coexistence », *RLDI* juillet 2010, n° 62.

HENAFF P.,
« L'œuvre transformative – Sécuriser l'œuvre transformative sans remettre en cause le monopole de l'auteur de l'œuvre préexistante ? », *CCE* n° 4, avril 2016, étude 8.

HUYETTE M.,
« À propos des injures sur Facebook », *Blog Paroles de juges*, 25 avril 2013.

JEANDIDIER W.,
« Principe de légalité criminelle », *J.-Cl.* Pénal Code, art. 111-2 à 111-5, fasc. n° 10, 2011 (mis à jour 2019).

JOMNI A.,
« Du discours de haine en ligne au cyberterrorisme : quelles régulations possibles ? », *Dalloz IP/IT* 2017, p. 563.

JUVIGNY (de) B.,
« La compliance, bras armé de la régulation », *in* M.-A. FRISON-ROCHE (dir.), *Régulation, Supervision, Compliance, Dalloz,* coll. Thèmes et commentaires, 2017, p. 17.

KATZ C.,
« Le délit de harcèlement moral. Une incrimination nécessaire ? Une application problématique », *AJ Pénal* 2005, p. 13.

KOCHER M.,
« Méfiez-vous de vos @mis ! », *Rev. trav.*, 2011, 39.

KOERING-JOULIN R.,
« La dignité de la personne humaine en droit pénal », *in* M.-L. PAVIA et T. REVET (dir.) *La dignité de la personne humaine*, Economica 1999, p. 83.

KOERING-JOULIN R., SEUVIC J.-F.,
« Droits fondamentaux et droit criminel », *AJDA*, 1998, p. 106.

KURI D.,
« L'hypothèse des délits de presse désuets », *in* N. DROIN et W. JEAN-BAPTISTE (dir.), *La réécriture de la loi sur la presse du 29 juillet 1881 : une nécessité ?*, LGDJ, coll. Grands Colloques, 2017, p. 63-76.

LABOURDIQUE-BOUZIDI D.,
« Les hashtags: quelle protection pour quelle action ? », *JCP* E, 13 octobre 2016 41, page(s) 5-6.

LACROIX C.,
« Usurpation d'identité », Rép. pén. Dalloz, juin 2012.

LANI F.-P. et BACQ E.,
« Facebook sanctionné par la CNIL pour de nombreux manquements à la loi informatique et libertés », *Légipresse* n° 352, septembre 2017, p. 444.

LAPÉROU-SCHENEIDER B.,

« Action publique et action civile », *J.-Cl.* proc. pén., art 2 à 3, fasc. 20, 2019.

LAZERGES Ch.,

« La participation criminelle », p.11-30 *in* Ch. LAZERGES (dir.), *Réflexions sur le nouveau Code pénal*, Paris, Pédone, 1995.

LEGER P.,

« Le cyberharcèlement, une infraction adaptée à la protection de la jeunesse en ligne », *Dalloz IP/IT* 2018, p. 346.

LEGRAIN T.,

« L'utilisation des réseaux sociaux par les bandes criminelles », *Sécurité globale*, 2016/1, n° 5, p. 99-100.

LEPAGE A.,

« Faux profil sur Facebook », *CCE* n° 3, mars 2011, comm. 28.

« Images intimes sur Internet », *CCE* n° 11, novembre 2005, comm. 176.

« Internet au regard de la loi du 29 juillet 1881 sur la presse : un mode de communication comme un autre ? », *in* : *L'opinion numérique : Internet un nouvel esprit public*, Dalloz, 2006, p. 141.

« Enregistrement effectué sans autorisation à l'audience d'une juridiction », *CCE* n° 10, octobre 2010, p. 36.

« Droit pénal et internet la part de la tradition, l'œuvre de l'innovation », *AJ Pénal* 2005, p. 217.

« L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée », *CCE* n° 2, février 2017, étude 3 ; *Dr. pén.* n° 1, janvier 2017, étude 1.

« Le délit d'usurpation d'identité : questions d'interprétation », *JCP* G n° 35, 29 août 2011, doctr. 913.

« Les vertus du droit commun, ou le happy slapping sanctionné sans le secours du nouvel article 222-33-3 du Code pénal », *CCE* n° 11, novembre 2007, comm. 137.

« Collecte déloyale de données personnelles sur Internet », *CCE* n° 9, septembre 2006, comm. 131.

« Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Dr. pén.* n° 3, mars 2005, étude 5.

« Même sur Internet, c'est dans les vieux pots qu'on fait les meilleures soupes », *CCE* n° 5, mai 2013, comm. 58.

« Précision bienvenue au sujet de l'article 226-2 du Code pénal », *CCE* n° 5, mai 2016, comm. 42.

« Droit pénal des médias », *RPDP* n° 1, janvier-mars 2017, p. 176.

« Précisions sur la communauté d'intérêts », *CCE* 2009, n° 11, comm. 102.

LESAULNIER F.,

« La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz, IP/IT* 2016, p. 573.

LEVASSEUR G.,

« La responsabilité collective et le droit pénal », *Lumière et vie*, 1953, n° 10, p. 130.

LIENHARD C.,

« Catastrophe, diffusion de fausses nouvelles et diffamation », *D.* 2002 p. 2972.

LINDER V.,
« Restriction à l'utilisation des réseaux sociaux dans les systèmes juridiques étrangers », *in* V. NDIOR (dir.), *Droit et réseaux sociaux*, éd. Lextenso, coll. LEJEP, octobre 2015, p. 63.

LINDON R.,
« La presse et la vie privée », *JCP* G 1965, II, 1887.
« Les dispositions de la loi du 17 juillet 1970 relative à la protection de la vie privée », *JCP* G 1970, I, 2357.

LOVELUCK B.,
« Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux*, vol. 192, n° 4, 2015, p. 249.

LUCAS DE LEYSSAC M.-P.,
« Fraude informatique : protection des systèmes de traitement automatisé de données, répression de la falsification de documents informatisés et mesures de prévention : loi du 5 janvier 1988 », *informatique et télécom*, 1988, n° 2, p. 18.

MAIGAT P. Le,
« Revenge porn et cyber-harcèlement. Schizophrénie ou déconnexion du juge pénal ? », *Gaz. Pal.* 19 avril 2016, n° 15, p. 12.

MALABAT V.,
« À la recherche du sens du droit pénal du harcèlement », *Dr. soc.* 2003. p. 491.
« Vers une collectivisation de la responsabilité pénale ? », *in* : *La cohérence des châtiments*, Dalloz, coll. Essai de philosophie pénale et de criminologie, vol. 10, 2012, p. 27.

MALLET-POUJOL N.,
« Rumeur et liberté d'expression : entre mensonge et vérité », *Légipresse* n° 364, octobre 2018, p. 484.

MANARA C.,
« Hébergement de contenus : une décision critiquable ! », *D.* 2010, p. 260.
« Twitter : communication de données d'identification », *D.* 2013, p. 300.
« Les créations transformatives », *Juris art etc.*, n° 25/2015, p. 29.

MARCOU G.,
« La notion juridique de régulation », *AJDA* 2006, p. 347.

MARIN J.-C.,
« Droit pénal et compliance », *in* M.-A. FRISON-ROCHE (dir.), *Régulation, Supervision, Compliance*, Dalloz, coll. Thèmes et commentaires, 2017, p. 66.

MARINO L.,
« Qualification de l'injure sur Facebook », *JCP* G n° 17, 22 Avril 2013, n° 466.
« Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement », *J.-Cl.* Comm., fasc. n° 670, 2015 (mis à jour 2017).

MARINO (Di) G.,
« Le recours aux objectifs de la loi pénale dans son application », *RSC 1991*, p. 505.

MARTIAL-BRAZ N.,
« Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017 p. 253.

MARTIN (de SAINT) A.,
« Clarification de la qualification de service d'hébergement », *RLDI* avril 2011, n° 70.

MARZOUKI M.,
« Biométrie : corps étrangers sous contrôle », *Plein droit*, 2008/1, n° 76.

MASCALA C.,
« Consentement de la victime », *J.-Cl.* Pénal Code, art. 122-4 à 122-7, fasc. unique, 2011 (mis à jour 2019).

MASSÉ M.,
« La criminalité terroriste », *RSC* 2012, p. 89.

MATTATIA F.,
« L'usurpation d'identité sur internet dans tous ses états », *RSC* 2014, p. 331.
« La création d'un délit d'usurpation d'identité sur l'Internet », *Gaz. Pal.*, 26 juillet 2008, n° 208, p. 6.
« CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés ? », *RSC* 2009, p. 317.

MAYAUD Y.,
« De la mise en cause diffamatoire d'une gestion municipale : l'enjeu de la publicité », *RSC* 1998, p. 104.
« Ne pas confondre : commentaires tendancieux et fausses nouvelles », *RSC* 2000, n° 1, p. 203.
« La politique d'incrimination du terrorisme à la lumière de la législation récente », *AJ Pénal* 2013 p. 442.
« Terrorisme - Infraction », Rép. pén., Dalloz, janvier 2018.
« violences volontaires », Rép. pén., Dalloz, octobre 2008.
« Le crime terroriste de participation à une association de malfaiteurs : une aggravation révélée dans sa juste portée », *AJ Pénal* 2016, p. 526.

MENDRAS M.,
« *From Moscow … With Fake News !* », *Esprit*, juin 2017, n° 6, p. 17-21.

MEULDERS-KLEIN M.-Th.,
« Vie privée, vie familiale et droits de l'homme », *RIDC* 1992, IV, p. 773.

MIHMAN A.,
« Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques », *J.-Cl.* Pénal Code, fasc. n° 20, 2018.

MISTRETTA P.,
« Harcèlement », Rép. pén., Mai 2019.
« La protection de la dignité de la personne et les vicissitudes du droit pénal », *JCP* G n° 1, 12 janvier 2005, doctr. 100.

MOINY J.-P.,
« Facebook au regard des règles européennes concernant la protection des données », *REDC*, 2010, n° 2, p. 249.

MORITZ M.,
« Entre idéal de neutralité technologique et réalité d'une mutation sémantique : analyse des catégories juridiques du droit français de la communication », *Revue internationale de droit des données et du numérique*, mars 2017, v. 1, p. 31.

MOURON P.,
« Et donc une chaîne YouTube est soumise aux pouvoirs de régulation du CSA », *RLDI* février 2017, n° 134.

NDIOR V.,
« Le réseau social : essai d'identification et de qualification », *in* V. NDIOR (dir.), *Droit et réseaux sociaux*, éd. Lextenso, coll. LEJEP, octobre 2015, p. 17.

NETTER E.,
« La responsabilité juridique de l'utilisateur de Twitter », *JCP* G, 2013, n° 3, p. 102.

NICAUD B.,
« Proposition de loi contre la "cyberhaine" adoptée à l'Assemblée ou l'enfer pavé de bonne (?) intentions », *Lexbase Pénal Edition* n° 18, 18 juillet 2019.

NUCCI (Di) D.,
« Fragmented futur », *Print Magazine*, avril 1999, p. 32.

PELLETIER H.,
« Atteinte à la vie privée – enregistrement de la parole ou de l'image – fabrication, détention, location ou vente d'appareils d'enregistrement », *J.-Cl.* Pénal Code, art. 226-1 à 226-3, fasc. n° 20, juin 2017.

PERBOST F.,
« La lutte contre les propos antisémites sur internet », Chronique du droit des nouvelles technologies, *Revue de jurisprudence commerciale*, juillet/août 2014, n° 4.

PERBOST F. et EUVRETE A.,
« Régulation des réseaux sociaux : où en est-on ? », *Revue de jurisprudence commerciale*, juillet/août 2016, n°4, p. 417.

PEREIRA B.,
« Responsabilité pénale », Rép. pén. Dalloz, juin 2017 (mis à jour 2018).

PERRIER J-B.,
« L'adaptation des incriminations », *RSC* 2017 p. 373.

PIERROUX E.,
« Facebook, Twitter et autres réseaux sociaux : petites injures entre "amis" », *Gaz. Pal.* 3 décembre 2015, n° 337, p. 4.

PIGNARD-CHEYNEL N., RICHARD J. et RUMIGNANI M.,
« Au-delà du mur : l'algorithme de Facebook mis à l'épreuve », *The conversation*, 25 septembre 2017 (mis à jour le 15 janvier 2018).

PLANIOL M.,
« Études sur la responsabilité civile », *Rev. Crit.*, 1906, p. 80.

PONSEILLE A.,
« Les infractions de prévention, Argonautes de la lutte contre le terrorisme », *RDLF*, juillet 2017, n° 2017-26.

POULLET Y. et ROUVROY A.,
« Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie. », *in* K. BENYEKHLEF et P. TRUDEL (dir.), *État de droit et virtualité*, Montréal, Thémis, 2009, p. 161.

POUSSON-PETIT J.,
« Le droit à l'anonymat », *in mélanges dédiés à Louis Boyer*, PU Toulouse, 1996, p. 595.

PRADEL J.,
« Les dispositions de la loi du 17 juillet 1970 sur la protection de la vie privée » *D.* 1971, chron. p. 115.
« Les infractions relatives à l'informatique », *RIDC* 2-1990, p. 820.

PRUD'HOMME M.,
« L'usurpation d'identité bientôt un nouveau délit », *Gaz. Pal.*, 24 avril 2010, n° 114, p. 8.

PUECH M.,
« L'illicéité dans la responsabilité civile extracontractuelle », *Revue internationale de droit comparé*, vol 26, n° 2, Avril-juin 1974, p. 428.

QUEMENER M.,
« Cyberharcèlement : quelles évolutions législatives ? », *RLDI* novembre 2018, nº 153.
« Signalez un contenu illicite sur Internet », *D.* 2013, p. 2096.
« Haine sur internet : quelles nouvelles préconisations ? », *RLDI* décembre 2018, n° 154.

QUINTON F.,
« Quelles questions Facebook nous pose-t-il ? », *ina global*, 4 février 2014.

QUONIAM L.,
« Introduction. Du web 2.0 au concept 2.0 », *Les Cahiers du numérique*, vol. 6, nº 1, 2010, p. 9.

RAFFRAY R.,
« Les multinationales et la création du droit », *in Les nouveaux pouvoirs, approche pluraliste des foyers de création du droit*, Bruylant, 2017, p. 74, n°4.

RASCHEL E.,
« Décryptage de la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique », *Lexbase Hebdo éd. priv.*, n° 691, 2017.

RAY J.-E.,
« Little brothers are watching you », *Semaine sociale Lamy*, 6 décembre 2010, n° 1470, p. 10.

RIAS N.,
« Usurpation d'identité ou usage de données permettant d'identifier un tiers », *J-Cl.* Pénal Code, fasc. 20, mai 2012 (mis à jour 2018).

ROBACZEWSKI C.,
« Atteintes aux systèmes de traitement informatisés de données », *J.-Cl.* Pénal Code, art. 323-1 à 323-7, fasc. n° 2, 2010 (mis à jour 2018).

ROUIDI H.,
« La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme : quelles évolutions ? », *AJ Pénal* 2014, p. 555.

ROY (Le) M.,
« Le CSA en fait-il trop… ou pas assez ? », *Légipresse* n° 357, février 2018, p. 77.

SAENKO L.,
« Le nouveau délit d'usurpation d'identité numérique », *RLDI* juin 2011, n° 72.

SAINT-PAU J.-C.,
« Droit au respect de la vie privée et droit pénal », *Dr. pén.* n° 9, septembre 2011, étude 20.
« Jouissance des droits civils. – Droit au respect de la vie privée. – Définition conceptuelle du droit subjectif », *J.-Cl.* Civil Code, art 9, fasc 10, n° 113.
« Vie privée : du lien entre délit principal et délit de conséquence », *JCP* G, n° 23, 6 juin 2016, 658.
« Le principe de responsabilité pénale du fait personnel », *in* Mélanges en l'honneur du professeur Yves Mayaud, *Entre tradition et modernité : le droit pénal en contrepoint*, Dalloz, 2017, p. 255.

SAUVAGE G.,
« Quel(s) outil(s) juridique(s) contre la diffusion de "*fake news*" », *Légipresse*, n° 352, septembre 2017, p. 431.

SÉGUR P.,
« Le terrorisme et les libertés sur l'internet », *AJDA*, le 2 février 2015, n° 3, p. 160-165.

SERINET A.,
« L'instauration d'une répression des atteintes à l'intimité sexuelle par la loi pour une république numérique », *D.* 2016, p. 1711.

SOLTANI S.,
« "Big data" et le principe de finalité », *RLDI* octobre 2013, n° 97.

SOSKIN I.,
« Les nouvelles formes d'atteintes à la "réputation" et à "l'image" de la personne dans l'environnement numérique », *Légipresse*, n° 336, mars 2016, p. 145.

STASIAK F.,
« Sac de "nœuds" bis in idem : cumul de sanctions pénales et administratives en droit de l'Union européenne », *RSC* 2018, p. 524.

STEINKOLER M.,
« Mar a Logos : L'élection de Trump et les *fake news* », *Savoirs et clinique*, 2017/2, n° 23, p. 23-33.

STOFFEL-MUNCK P.,
« Avis de tempête sur le Web 2.0 : la Cour de cassation juge que Tiscali n'est pas un hébergeur », *CCE* mars 2010, n° 3, comm. 25.

TILLEMENT G.,
« La loi de 1881 sur la liberté de la presse et le contrôle de constitutionnalité », *in* Mélanges en l'honneur de professeur Jean-François Seuvic, *Légalité, légitimité, licéité : regards contemporains*, PUN, 2018, p. 266.

THIERRY J-B.,
« Diffusion sur internet de la photographie d'une femme nue », *AJ Pénal* 2016, p. 268.
« Stupeur et tremblements lors d'une perquisition », *AJ Pénal* 2018, p. 205.
« Choquer n'est pas provoquer », *AJ Pénal*, 2017, p. 398.

THOUMYRE L.,

« Les notions d'éditeurs et d'hébergeurs dans l'économie numérique », *D.* 2010, p. 837.

« Les hébergeurs en ombres chinoises. Une tentative d'éclaircissement sur les incertitudes de la LCEN », *RLDI* mai 2005, n° 5.

« Comment les hébergeurs français sont devenus juges du manifestement illicite », *Juriscom*, 28 juillet 2004.

« Valse constitutionnelle à trois temps sur la responsabilité des intermédiaires techniques », *Légipresse* 2004, nº 214, p. 129.

TRUDEL P., ARBAN F.,

« Gérer les enjeux et risques juridiques du web 2.0 », Centre de recherche en droit public, Université de Montréal, CEFRIO, janvier 2012.

VALETTE M.,

« Sémantique interprétative appliquée à la détection automatique de documents racistes et xénophobes sur Internet », *in* P. ENJALBERT et M. GAIO (dir.), *Approches sémantiques du Document Numérique*, Actes du 7ème colloque International sur le Document Electronique, 22-25 juin 2004, éd., 2004, p. 215.

VALETTE M. et GRABBAR N.,

« Caractérisation de textes à contenu idéologique : statistique textuelle ou extraction se syntagme ? L'exemple du projet PRINCIP », Journées Internationales d'Analyse statistique des Données Textuelles (JADT), 2004, Louvain-la-Neuve, Belgique, UCL Presses Universitaires de Louvain, 2004, p. 1106.

VERNY E.,

« Usurpation d'identité », *J.-Cl.* Comm., fasc. 58, juillet 2015 (mis à jour 2018).

VIVANT M.,

« Entre ancien et nouveau - une quête désordonnée de confiance pour l'économie numérique », *Cahiers Lamy droit de l'informatique et des réseaux*, juillet 2004, nº 171, p. 2.

WARREN S. et BRANDEIS L.,

« The right to privacy », *Harvard Law Review*, n° 5, 15 décembre 1890.

WESTER-OUISSE V.,

« Travail - Infractions contre le salarié », *J.-Cl.* Pénal des Affaires, fasc. n° 30, 2008 (mis à jour 2019).

WU T.,

« Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, Vol. n° 2, 2003, p. 141.

V. RAPPORTS, AVIS, RECOMMANDATIONS

A. VITU, *De l'illicéité en droit criminel français*, rapport présenté à l'occasion des deuxièmes journées franco helléniques de droit comparé à Nancy, Bull. de la société de législation comparé 1984.

Conseil de l'Europe, Comité des ministres, Du comité de ministres aux États membres sur le « discours de haine », Recommandation n° R(97)20 adoptée le 30 octobre 1997.

G. BRAIBANT, *Données personnelles et société de l'information*, Rapport au Premier ministre, La documentation Française, 1998.

Conseil d'État, *Réflexion sur les autoritiés administratives indépendantes*, Rapport public 2001, p. 287.

Conseil de l'Europe, comité des ministres, recomm. n° 2003-13 sur la diffusion d'informations par les médias en relation avec les procédures pénales, 10 juillet 2003.

P. GERALD, *Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié*, Rapport de l'Office parlementaire d'évaluation de la législation n° 404, déposé le 15 juin 2006.

Groupe de travail « article 29 » sur la protection des données, 01189/09/FR WP 163, Avis 5/2009 sur les réseaux sociaux en ligne, 12 juin 2009.

I. FALQUE-PIERROTIN, *Lutter contre le racisme sur Internet*, Rapport au Premier ministre, 2010.

Rapport AN n° 2271, sur le projet de loi (n° 1697), d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2), enregistré à la présidence de l'assemblée nationale le 27 janvier 2010.

I. FALQUE-PIERROTIN, *Lutter contre le racisme sur Internet*, Rapport au Premier ministre, 2010.

Sénat, Rapport d'information n° 296 sur l'évaluation de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon, 9 février 2011.

F. LARUE, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Assemblée générale des Nations Unies, Conseil des droits de l'homme, 17ème session, 16 mai 2011.

Contribution du Conseil supérieur de l'audiovisuel sur l'adaptation de la régulation audiovisuelle, 24 janvier 2013, disponible sur le site du CSA.

Rapport de la Commission sur l'égalité et la non-discrimination du Conseil de l'Europe sur le harcèlement, Doc. 13336, 15 octobre 2013.

Rapport Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014.

Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les internautes.* Rapport sur la cybercriminalité, 2014.

Conseil National du Numérique (CCNum), *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable*, ministère de l'économie du redressement productif et du numérique, mai 2014.

D. BOUZAR, C. CAUPENNE, S. VALSAN, « La Métamorphose opérée chez le jeune par les nouveaux discours terroristes », recherche-action sur la mutation du processus d'endoctrinement et d'embrigadement dans l'islam radical, novembre 2014, p. 82-86.

V.-L. BENABOU et F. LANGROGNET, Rapport de la mission du CSPLA sur les « œuvres transformatives », 24 décembre 2014.

Avis sur la lutte contre les discours de haine sur internet, Commission Nationale Consultative Des Droits De l'Homme (CNCDH), assemblée plénière, 12 février 2015, adoption à l'unanimité.

C. PAUL et C. FERAL-SCHUHL, *Numérique et libertés : un nouvel âge démocratique*, Rapport n° 3119, déposé le 9 octobre 2015, mis en ligne le 13 octobre 2015.

Avis 2016/C 257/05 du Contrôleur européen de la protection des données concernant le « Bouclier vie privée UE États-Unis » (Privacy Shield).

Ministère de l'économie de l'industrie et du numérique, Modalités de régulation des algorithmes de traitement des contenus, rapport à Mme la Secrétaire d'État chargée du numérique, 13 mai 2016.

Rapport d'information de MM. François PILLET et Thani MOHAMED SOILIHI, *L'équilibre de la loi du 29 juillet 1881 à l'épreuve d'Internet*, fait au nom de la commission des lois n° 767 (2015-2016), 6 juillet 2016.

Commission Nationale de l'Informatique et des libertés (CNIL), *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017.

K. AMELLAL, L. AVIA, G. TAIEB, *Renforcer la lutte contre le racisme et l'antisémitisme*, rapport remis au Premier ministre le 20 septembre 2018.

Rapport de la mission *Régulation des réseaux sociaux – Expérimentation Facebook* remis au Secrétaire d'État en charge du numérique, Mai 2019.

Conseil d'État, avis n° 397368 sur la proposition de loi visant à lutter contre la haine sur Internet, 16 mai 2019.

VI. JURISPRUDENCES

A. Décisions des juridictions judiciaires

1. Décisions de la Cour de cassation

Avant 1980 :

- Civ., 16 novembre 1827 : *S.* 1828, 1, p. 135.
- Civ., 2 juillet 1835 : *S.* 1835, 1, p. 861.
- Crim. 21 octobre 1841 : *S.* 1842, 1, 904 ; 24 mars 1944, *DA* 1944, 75, note A. LEBRUN.
- Crim. 3 mars 1859 : *Bull. crim.* n° 69.
- Crim. 28 juin 1860 : *DP* 1860, I, 293.
- Crim. 19 février 1892 : *DP* 1892, I, 550.
- Crim., 31 janvier 1914 : *DP* 1918, I, 60.
- Crim., 27 novembre 1920 : *Bull. crim.*, n° 461.
- Crim. 25 février 1921 : *S.* 1923, I, 89, note J.-A. ROUX.
- Crim. 26 juin 1930 : *Bull. crim.* n° 190.
- Crim. 14 novembre 1931 : *Bull. crim.* n° 258.
- Crim. 3 mars 1933 : *Bull. crim.* n° 49.
- Crim. 7 août 1934 : *DH* 1934, n° 477.
- Crim. 3 janvier 1936 : *DH* 1936, n° 150.
- Crim. 22 octobre 1936 : *Bull. crim.* n° 97.
- Civ., 1er juillet 1937 : *S.* 1938, 1, p. 193.
- Crim. 27 mai 1943 : *DA* 1943, n° 52.

- Crim. 9 mars 1944 : *Bull. crim.* nº 69.
- Crim. 16 décembre 1948 : *Bull. crim.* n° 291.
- Crim., 16 mars 1950 : *Bull. crim.*, n° 100.
- Crim., 28 avril 1950: *Bull. crim.*, n° 137.
- Crim., 7 juin 1951: *RSC* 1951, p. 666 note L. HUGUENEY.
- Crim., 19 mars 1953 : *Bull. crim.* n° 100 ; *D.* 1953, n° 390.
- Crim., 21 juillet 1953 : *Bull. crim.*, n° 254 ; *RSC* 1954, p. 368, obs. L. HUGUENEY.
- Crim. 16 décembre 1953 : *D.* 1954, p. 129.
- Civ., 28 janvier 1954 : *D.* 1954, p. 217, note G. LEVASSEUR.
- Crim. 16 mars 1954: *Bull. crim.*, n° 111.
- Crim., 18 mai 1954 : *Bull. crim.*, n° 187 ; *D.* 1956, p. 366, note LEMERCIER ; *JCP* 1954, II, 8292, note A. CHAVANNE.
- Crim., 22 décembre 1955 : *Bull. crim.*, n° 596.
- Crim. 26 février 1956 : *JCP* 1956, II, 9304.
- Crim., 12 décembre 1957 : *Bull. crim.* n° 837.
- Crim., 18 juin 1958 : *Bull. crim.* n° 465.
- Crim., 22 août 1959 : *Bull. crim.* n° 393.
- Crim. 3 mars 1960 : *Bull. crim.* nº 138 ; *RSC* 1961, p. 105, obs. A. LEGAL.
- Crim., 20 juillet 1960 : *Bull. crim.* n° 382.
- Crim., 18 décembre 1962 : *Bull. crim.* n° 380.
- Crim., 7 novembre 1963 : *Bull. crim.* n° 314 : *JCP* G 1963, IV, p. 171.
- Civ. 1ère, 23 février 1965 : *JCP*, 1965, II, 14255, note P. NEVEU.
- Crim., 11 mars 1965 : *Bull. crim.* n° 777.
- Crim., 1er avril 1965 : *Bull. crim.* n° 106.
- Crim., 26 juin 1968 : *Bull. crim.* n° 210.
- Crim. 3 janvier 1969, nº 68-91.288 : *Bull. crim.* nº 1; *D.* 1969, p. 152 ; *JCP* 1969, II, 15791
- Crim. 21 janvier 1969 : *Bull. crim.* n° 38.
- Crim. 28 janvier 1969 : *Bull. crim.* nº 51.
- Crim. 14 octobre 1970, nº 69-93.195 : *Bull. crim.* nº 267, *D.* 1970. 774.
- Crim., 14 janvier 1971 : *D.* 1971, p. 101 ; *JCP* G 1972, II, 17022.
- Crim., 17 janvier 1971 : *Bull. crim.* n° 14.
- Crim. 7 mars 1972, nº 71-91.303 : *Bull. crim.* nº 85 ; *Gaz. Pal.* 1972, 1, 450.
- Crim. 26 mars 1974 : *Bull. crim.* nº 129.
- Crim., 8 octobre 1974 : *Bull. crim*. n° 280.
- Civ. 2ème, 14 novembre 1975 : *D.* 1976, p. 421, note B. EDELMAN.
- Civ. 2ème, 26 novembre 1975 : *JCP* G 1978, II, 18811, J. REVEL.
- Crim. 18 février 1976, nº 75-92.403 : *Bull. crim.* nº 63 ; *Gaz. Pal.* 1976, 1, 330 ; *RSC* 1976, p. 967, obs. G. LEVASSEUR.
- Crim. 8 novembre 1977 : *Bull. crim.* nº 339.
- Crim. 23 mars 1978, n° 77-90.339 : *Bull. crim.* n° 115.
- Crim., 29 mars 1978 : *Bull. crim.* n° 118.
- Crim. 20 novembre 1978 : *Bull. crim.* nº 323.

Décennie 1980 :

- Crim., 2 janvier 1980 : *Bull. crim.* n° 3.
- Crim., 21 avril 1980 : *Bull. crim.* n° 115.
- Crim., 3 juillet 1980 : *Bull. crim.* n°560.
- Crim., 23 octobre 1980 : *Bull. crim.* n° 270.
- Crim., 27 janvier 1981 : *Bull. crim.* n° 39.

- Crim., 17 février 1981 : *Bull. crim.* n° 64.
- Civ. 2ème, 8 juillet 1981 : *Bull. civ.* II n° 152.
- Crim., 15 juillet 1981 : *Bull, crim.* n° 232.
- Civ. 2ème, 5 janvier 1983 : *Bull. civ.* II n° 4 ; *D.* 1981, 457, note R. LINDON.
- Crim. 15 mars 1983 : *Bull. crim.* n° 82.
- Crim., 22 novembre 1983 : *Bull. crim.* n° 308.
- Civ 1ère, 3 avril 1984 : *Bull. civ.* n° 125.
- Crim., 3 octobre 1984 : *Bull. crim.* nº 285.
- Civ. 1ère, 13 février 1985 : *Bull. civ.* I n° 64 ; *D.* 1985, p. 488, 1ère esp. note B. EDELMAN.
- Crim., 17 juillet 1985 : *Bull. crim.* n° 267.
- Crim., 15 octobre 1985 : *Bull. crim.* n° 315.
- Crim., 22 janvier 1986 : *Bull. crim.* n° 29.
- Crim., 21 novembre 1988 : *Bull. crim.* nº 392, *RSC* 1989, p. 320, obs. G. LEVASSEUR.
- Crim., 25 avril 1989 : *Bull. crim.* n° 165, *RSC* 1990, p. 78, obs. G. LEVASSEUR.

Décennie 1990 :

- Crim., 11 janvier 1990, n° 89-80.642 : inédit ; *Gaz. Pal.* 1991,1, p. 298, note J.-P DOUCET.
- Crim., 8 novembre 1990, nº 89-86.904 : inédit ; *Dr. pén.* 1991, comm. 102.
- Civ 1ère, 28 mai 1991, n° 89-20.258 : *Bull. civ.* I n° 167 ; *D.* 1992, p. 213, note P. KAYSER ; *JCP* G 1992, II, 21845, note F. RINGEL.
- Crim., 13 juin 1991, nº 90-84.103 : *Bull. crim.* nº 253 ; *RSC* 1992. 74, obs. G. LEVASSEUR.
- Ass. plén., 11 décembre 1992, n° 91-11.900 : *Bull. ass. plén.* n° 13 ; *JCP* G 1993, II, 21991, concl. M. JEOL et note G. MEMETEAU ; *RTD Civ.* 1993, p. 99, obs. J. HAUSER.
- Civ. 2ème, 8 novembre 1993, n° 91-18.127 : *Bull. civ.* II n° 318.
- Crim., 9 décembre 1993, nº 93-81.669 : *Bull. crim.* nº 379.
- Crim., 15 décembre 1993, nº 93-84.515 : *Bull. crim.* nº 389.
- Crim. 29 mars 1994, n° 92-80.728 : *Bull. crim.* n° 119.
- Crim., 22 juin 1994, n° 92-21.060 : inédit.
- Crim., 16 mai 1995, n° 93-83.690 : *Bull. crim.* n° 175.
- Civ. 1ère, 19 décembre 1995, n° 93-18.939 : *Bull. civ.* I, n° 179 ; *D.* 1997, p. 158, note J. RAVANAS.
- Civ. 1ère, 6 mars 1996, n° 93-21.728 : *Bull. civ.* I n° 118 ; *D.* 1997, p. 7, note J. RAVANAS.
- Crim., 30 mai 1996, n° 94-82.114 : *Bull. crim.* n° 228.
- Civ. 1ère, 5 novembre 1996, n° 94-14.798 : *Bull. civ.* I n° 378.
- Crim., 3 juin 1997, n° 96-81.706 : *Bull. crim.* n° 218.
- Crim., 7 octobre 1997, n° 96-81.485 : *Bull. crim.* n° 324 ; *D.* 1999, p. 152, note J.-C. SAINT-PAU.
- Civ. 1ère, 13 janvier 1998, n° 95-13.694 : *Bull. civ.* I n° 14 ; *JCP* G 1998, II, 10082, note G. LOISEAU ; *D.* 1999, p. 120, note J. RAVANAS.
- Crim., 29 janvier 1998, n° 95-82.09 : inédit.
- Civ. 1ère, 16 juillet 1998, n° 96-15.610 : *Bull. civ.* I, n° 259 ; *D.* 1999, p. 541, note J.-C. SAINT-PAU.

- Civ. 1ère, 6 octobre 1998, n° 96-12.540 : *Bull. civ.* I n° 274 ; *D.* 1999, somm. p. 376, obs. LEMOULAND ; *Gaz. Pal.* 1999, 1, pan. p. 32 ; *RTD Civ.* 1999, p. 62, obs. J. HAUSER.
- Crim., 20 octobre 1998, n° 97-84.621 : *Bull. crim.* n° 264.
- Crim., 8 décembre 1998, n° 97-83.709 : *Bull. crim.* n° 335 ; *RSC* 1999, p. 607, obs. J. FRANCILLON ; *JCP* G 1999, II, 10135, note J.-Y. LASSALLE.
- Crim., 13 avril 1999, n° 98-83.798 : *Bull. crim.* n° 78 ; *Dr. pén.* 1999, comm. 115, obs. M. VERON. ; *Légipresse* 1999, n° 165, III, p. 141 ; *D.* 1999, somm. p. 406, obs. T. MASSIS ; *D.* 1999, somm. p. 126, obs. B. de LAMY ; *RSC* 2000, p. 203, obs. Y. MAYAUD.
- Civ. 2ème, 10 juin 1999, n° 97-20.028 : *Bull. civ.* II, n° 46.
- Crim., 21 septembre 1999, n° 97-85.551 : *Bull. crim.* n° 191 ; *D.* 2000, somm. 383, obs. M.-C. AMAUGER-LATTES ; *RSC* 2000. 200, obs. MAYAUD.
- Civ. 2ème, 23 septembre 1999, n° 97-18.784 : *Bull. civ* II n° 140.

Décennie 2000 :

- Civ 2ème., 3 février 2000, n° 98-11.438 : *Bull. civ.* 2000, II, n° 26.
- Crim, 26 avril 2000, n° 99-85.951 : inédit.
- Crim., 27 juin 2000, n° 99-85.258 : inédit.
- Crim., 30 janvier 2001, n° 00-83.004 : *Bull. crim.* n° 28 ; *JCP* éd. G 2001, II, n° 10515, note A. LEPAGE.
- Crim., 31 Octobre 2001, n° 01-80.282 : inédit.
- Civ. 2ème, 14 mars 2002, n° 99-19.239 : *Bull. civ.* II n° 41.
- Civ. 1ère, 3 avril 2002, n° 00-12.932 : *Bull. civ.* n° 110.
- Civ. 2ème, 14 novembre 2002, n° 00-15.549 : inédit.
- Crim., 11 février 2003, n° 01-86.041 : inédit.
- Crim., 6 mai 2003, n° 02-80.284 : *Bull. crim.* n° 94 ; *CCE* n° 9, Septembre 2003, comm. 89, A. LEPAGE ; *JCP* G n° 26, 25 juin 2003, 2175 ; *D.* 2003, p. 2192, note E. DREYER.
- Civ. 2ème, 3 juillet 2003, n° 00-15.468 : *Bull. civ.* II n° 228.
- Crim., 30 septembre 2003, n° 03-80.039 : *Bull. crim.* n° 172.
- Civ. 1ère, 9 décembre 2003, n° 01-11.587 : *Bull. civ.* n° 254.
- Civ. 2ème, 19 février 2004, n° 02-11.122 : *Bull. civ.* II n° 72 ; *D.* 2004, p. 2596, note C. BIGOT.
- Civ. 2ème, 10 juin 2004, n° 02-12.926 : *Bull. civ.* II n° 292 ; *JCP* E 2005, 660, J. RAYNARD ; *D.* 2005, p. 469, note J. MOULY et J.-P. MARGUENAUD.
- Civ. 2ème, 30 juin 2004, deux arrêts, n° 02-19.599 et n° 03-13.416 : *Bull. civ.* II n° 341 ; *JCP* G 2004, II, 10160, note D. BAKOUCHE.
- Crim., 10 mai 2005, n° 04-84.118 : inédit ; *Dr. pén.* novembre 2005, n° 177.
- Crim., 10 mai 2005, n° 04-84.705 : *Bull. crim.* n° 144 ; *JCP* G n° 25, 22 juin 2005, IV 243 ; *D.* 2005 p. 2986, pan. G. ROUJOU De BOUBÉE, T. GARE, C. MASCALA.
- Civ. 1ère, 27 septembre 2005, n° 04-12.148 : *Bull. civ.* I n° 346 ; *D.* 2006, 637, note S. VIGAND, Pror. Intel. janvier 2006, n° 18, p. 81, note J. PASSA.
- Civ. 1ère, 7 février 2006, n° 04-10.941 : *Bull. civ.* I n° 59 ; *JCP* G 2006, II, 10041, G. LOISEAU ; *Bull. civ.* n° 59 ; *Gaz. Pal.* 2006, avis J. SAINTE-ROSE ; *RTD Civ.* 2006, p. 279, obs. J. HAUSER.
- Crim., 14 février 2006, n° 05-82.287 : *Bull. crim.* n° 42 ; *D.* 2007, p. 1184, note J.-C. SAINT-PAU ; *CCE* 2006, n° 69, obs. A. LEPAGE.
- Crim., 14 mars 2006, n° 05-83.423 : *Bull. crim.* n° 69 ; *CCE* n° 9, septembre 2006, comm. 131, A. LEPAGE.

- Crim., 16 mai 2006, nº 05-86.860 : inédit ; *Dr. pén.* 2006, comm. 121, obs. J.-H. ROBERT.
- Crim., 28 novembre 2006, n° 06-80.340 : *Bull. crim.* n° 300 ; *CCE 2007*, n° 45, obs. A. LEPAGE.
- Crim., 12 décembre 2006, nº 05-87.658 : inédit.
- Crim., 31 janvier 2007, n° 06-81.258 : *Bull. crim.* n° 25, *Dr. pén.* 2007, comm. 56, obs. M. VÉRON.
- Crim., 3 octobre 2007, nº 07-81.045 : *Bull. crim.* n° 236 ; AJ Pénal 2007, p. 535.
- Crim., 4 décembre 2007, n° 05-87.384 : *Bull. crim.* n° 302 ; *D.* 2008, p. 298.
- Crim., 26 février 2008, n° 07-84.846 : inédit ; *CCE* 2008 comm. 71, obs. A. LEPAGE.
- Civ. 1ère, 7 mai 2008, n° 07-12.126 : *Bull. civ.* I n° 126 ; *CCE* 2008, comm. 94, note A. LEPAGE ; *RTD Civ.* 2008, p. 449, obs. J. HAUSER ; *D.* 2008, p. 1481, obs. C. Le DOUARON.
- Crim., 13 janvier 2009, n° 08-84.088 : *Bull. crim* n° 13 ; *Dr. pén.* 2009, comm. 66, obs. J.-H. ROBERT.
- Crim., 28 avril 2009, n° 08-85.249 : inédit ; *CCE* 2009 comm. 102, obs. A. LEPAGE.
- Crim., 16 juin 2009, n° 08-88.560 : inédit.
- Crim., 30 septembre 2009, n° 09-80.373 : *Bull. crim.* n° 162 ; *JCP* G 2009, 587, note J.-L. CAPDEVILLE.

Après 2010 :

- Civ. 1ère, 14 janvier 2010 n° 06-18.855 : *Bull. civ.* I n° 8 ; *CCE* 2010, nº 3, comm. 25 ; *RLDI* 2010/59, nº 1951 ; R*LDI* 2010/58, nº 1934 ; *RLDI* 2010/58, nº 1935.
- Crim. 16 février 2010, n° 09-81.064 et n° 08-86.301 : *Bull. crim.* n° 30 ; Dr pén. 2010, n° 80, note M. VÉRON ; *D.* 2010, p. 2206, obs. E. DREYER.
- Crim., 16 mars 2010, n° 09-84.160 : inédit.
- Crim., 23 mars 2010, n° 09-80.787 : inédit.
- Crim., 8 juin 2010, n° 09-87.526 : *Bull. crim.* n° 103 ; *CCE* n° 10, Octobre 2010, comm. 100, A. LEPAGE ; *RLDI* octobre 2010, n° 64, p. 29-32, note L. BELFANTI et P. BELLOIR.
- Com., 13 juillet 2010, n° 06-20.230 : *Bull. civ.* IV n° 124 ; *CCE* 2010, comm. 93, obs. C. CARON ; Contrats, conc. consom. 2010, comm. 229, obs. M. MALAURIE-VIGNAL ; *D.* 2010, p. 1966, obs. P. TRÉFIGNY-GOY ; *RLDI* 2010/63, n° 2063, note C. CASTETS-RENARD ; *Légipresse* 2010, p. 367, note P. ALLAEYS.
- Crim., 5 octobre 2010, n° 10-80.050 : inédit.
- Crim., 14 décembre 2010, n° 10-80.088 : inédit ; *D.* 2011 p. 1055, note E. DREYER ; *RSC* 2011 p. 651, note J. FRANCILLON ; *RTD Com.* 2011 p. 356, note F. POLLAUD-DULIAN.
- Civ. 1ère, 3 février 2011, n° 09-10.301 : *Bull. civ.* I n° 21, *CCE* 2011, comm. 46, obs. A. LEPAGE, *D.* 2012. Pan. 765, obs. E. DREYER.
- Civ. 1ère, 17 février 2011, n° 09-67.896 : *Bull. civ.* I n° 30 ; *CCE* 2011, comm. 32, note C. CARON ; *JCP* G 2011, 520, note A. DEBET ; Gaz. Pal 23 juin. 2011, p. 20, note L. MARINO ; Resp. civ. et assur. 2011, étude 8, L. MARINO ; Propr. intell. 2011, n° 39, p. 197, note A. LUCAS ; *D.* 2011, p. 1113, note L. GRYNBAUM ; *RLDI* 2011/69, n° 2258, note C. CASTETS-RENARD ; *Légipresse* 2011, n° 283, p. 297, note V. VARET.
- Civ. 1ère, 17 février 2011, n° 09-13.202 : *Bull. civ.* I n° 31 ; *Légipresse* 2011 n° 281, p. 145.

- Civ. 1ère, 17 février 2011, n° 09-15.857 : *Bull. civ.* I n° 32 ; Amen c/ M. K. ; *D.* 2011, p. 2164, obs. P. SIRINELLI ; *D.* 2012, p. 2836, obs. P. SIRINELLI ; *CCE* 2011, comm. 32, note C. CARON ; *Gaz. Pal.* 23 avril 2011, n° 113, chron. 27.
- Civ. 1ère, 12 mai 2011, n° 08-20.651 : *Bull. civ.* I n° 87.
- Civ. 1ère, 4 novembre 2011, n° 10-24.761 : *Bull. civ.* I n° 196 ; *RLDI* 2011/77, n° 2560.
- Crim., 6 décembre 2011, n° 10-82.266 : *Bull. crim.* n° 249 ; *JCP* 2012, n° 410, note P. MISTRETTA.
- Crim. 31 janvier 2012, n° 11-80.010 : *Bull. crim.* n° 29 ; *CCE* 2012, comm. 43, obs. A. LEPAGE ; *D.* 2012, p. 1249, note C. RAVIGEAUX ; *D.* 2013, p. 457, obs. E. DREYER ; *Dr. pén.* 2012, comm. 53, obs. M. VERON ; *Gaz. Pal.* 13-14 juin 2012, p. 11, obs. F. FOURMENT.
- Civ. 1ère, 12 juillet 2012, n° 11-15.165 et 11-15.188 : *Bull. civ.* I n° 162 ; *Gaz. Pal.* 18 octobre 2012, n° 292, p. 19, note L. MARINO ; *JCP* E 2012, 1627, note J.-M. BRUGUIERE ; *CCE* 2012, comm. 91, note C. CARON ; *D.* 2012, p. 2075, note C. CASTETS-RENARD ; *D.* 2012, p. 2071, concl. C. PETIT ; *Légipresse* 2012, n° 298, p. 566, note P. ALLAEYS ; Propr. intell. 2012, n° 45, p. 416, note A. LUCAS ; *RTD Com.* 2012, p. 771, note F. POLLAUD-DULIAN.
- Crim., 2 octobre 2012, n° 11-82.239 : inédit.
- Civ. 1ère, 16 mai 2012, n° 11-18.449 : inédit ; *CCE* 2012, comm. 114, A. LEPAGE ; *JCP* G 2012, p. 1318, n° 12, E. Dreyer ; *Gaz. Pal.* 3-4 octobre 2012, p. 16, note C. MICHALSKI.
- Crim. 2 octobre 2012, n° 12-80.419 : *Bull. crim* n° 204 ; Dr pén. n° 12, décembre 2012, comm. 157, M. VERON ; *Procédures* n° 12, décembre 2012, comm. 373, J. BUISSON.
- Crim., 30 octobre 2012, n° 11-88.562 : inédit ; *D.* 2013, p. 463, obs. E. DREYER.
- Crim., 30 octobre 2012, n° 10-88.825 : *Bull. crim* n° 233 ; *D.* 2013, p. 160, note E. DREYER ; *Dr. pén.* 2013, comm. 6, obs. M. VERON.
- Civ. 1ère, 10 avril 2013, n° 11-19.530 : *Bull. civ.* I n° 70 ; *JCP* G 2013, 816, spéc. n° 17, obs. L. MARINO ; *JCP* E 2013, spéc. n° 47, note B. BOSSU ; *Légipresse* 2013, p. 312, n° 305, note B. ADER ; *CCE* 2013, comm. n° 81, obs. A. LEPAGE ; *D. actu.*, 24 avril 2013.
- Crim., 28 janvier 2014, n° 12-80.157 : inédit.
- Crim., 21 mai 2014, n° 13-83.758 : *Bull. crim.* n° 136 ; AJ Pénal 2014, p. 528, note P. de COMBLES de NAYVES ; *Dr. pén.* 2014 n° 7-8, comm. n° 106, M. VERON ; *RSC* 2014, p. 849, note J. ALIX.
- Crim., 17 septembre 2014, n° 13-85637 : inédit.
- Crim., 22 octobre 2014, n° 13-82.630 : inédit ; *D.* 2015, p. 415, note A. MENDOZA-CAMINADE ; *CCE* 2015 ; comm. 17, note E. CAPRIOLI.
- Crim., 17 mars 2015, n° 13-87.922 : *Bull. crim.* n° 57.
- Crim., 3 novembre 2015, n° 14-83.420 : inédit.
- Crim. 20 mai 2015, n° 14-81.336 : *Bull. crim.* n° 119 ; *D.* 2015, p. 1466, note L. SAENKO ; *D. actu.*, 5 juin 2015, obs. C. DUHIL de BENAZE ; *AJ Pénal* 2015. 413, note E. DREYER.
- Civ. 1ère, 14 janvier 2016, n° 14 28.327 : inédit.
- Crim., 16 mars 2016, n° 15-82.676 : *Bull. crim.* n° 86 ; *JCP* G 2016, 658, note J.-C. SAINT-PAU ; *Dr. pén.* 2016, comm. 73, obs. P. CONTE ; *CCE* 2016, comm. 42 ; *D.* 2016, p. 935, note A. SERINET ; *RSC* 2016, p. 96, obs. J. FRANCILLON ; AJ Pénal 2016, p. 268, note J-B. THIERRY ; *Dalloz IP/IT* 2016, p. 321, Obs. G. DESGENS-PASANAU.

- Crim. 12 juillet 2016, n° 15-86.645 : Publié au Bulletin ; *Dalloz IP/IT* 2016 p. 618, note B. AUROY ; *CCE* n° 10, Octobre 2016, comm. 83, A. LEPAGE ; *D.* 2016 p. 1848, note E. DREYER.
- Crim, 18 octobre 2016, nº 15-84.068 : inédit ; *RLDI* novembre 2016, nº 131, obs. L. COSTES.
- Civ. 1ère, 3 novembre 2016, n° 15-22.595 : Publié au bulletin ; *Légipresse* 2017, n° 345, p. 27, obs. N. BOTCHORICHVILI ; *JCP* G 2016, 1310, obs. R. PERRAY ; *Dalloz IP/IT* 2017, p. 120, obs. G. PERONNE et E. DAOUD ; *Dr. pén.* 2015, chron. 11, n° 12, obs. A. LEPAGE ; *Gaz. Pal.* 15 novembre 2016, n° 40, p. 24, obs. P. INGALL-MONTAGNIER.
- Crim., 16 novembre 2016, nº 16-80.207 : inédit ; *RLDI* janvier 2017, n° 133, obs. L. COSTES.
- Crim., 29 novembre 2016, n° 16-90.024 : inédit.
- Civ. 2ème , 5 janvier 2017, n° 16-12.394 : Publié au bulletin ; *D.* 2017, n° 62 ; *Dalloz IP/IT*, juin 2017, n° 6, p. 350-351; *RLDI* mars 2017, n° 135, p. 33; *Légipresse*, janvier 2017, n° 345, p. 7 ; *D.* 2017, n° 4, p. 208 ; *CCE* février 2017, n° 2, p. 1.
- Crim., 7 juin 2017, n° 16-80.322 : Publié au bulletin ; *Légipresse*, 2017, p. 1814, note C. BIGOT ; AJ Pénal, 2017, p. 398, obs. J. B. THIERRY.
- Crim. 11 juillet 2017, n° 16-84.859 : Publié au bulletin ; Jurisport 2017, n° 179, p. 9, J. MONDOU ; AJ Pénal 2017, p. 497 ; *D. actu.*, 6 sept. 2017, obs. S. LAVRIC.
- Crim., 13 septembre 2017, n° 15-84.823 : Publié au bulletin ; *D. actu.*, 28 septembre 2017, obs. W. AZOULAY.
- Crim. 16 janvier 2018, n° 16-87.168 : *Bull. crim.* n° 1 ; *D.* 2018, p. 172 ; AJ Pénal 2018, p. 205, obs. J.-B. THIERRY ; *RSC* 2018, p. 480, obs. P. MISTRETTA ; *Dr. pén.* 2018, Comm. 74, obs. P. CONTE ; *CCE* 2018, Comm. 30, obs. E.-A. CAPRIOLI ; *Gaz. Pal.* 30 avril 2018, p. 65, obs. F. FOURMENT ; *RSC* 2018 p.701, obs. E. DREYER.
- Crim. 23 janv. 2018, n° 17-80.323 : inédit ; *Légipresse* 2018, p. 154, note E. DREYER ; *Gaz. Pal.* 30 avril 2018, n° 16, p. 52, obs. S. DETRAZ.
- Crim. 6 mars 2018, n° 16-87.533 : inédit ; *Dr. pén.* 2018. Comm. 105, obs. P. CONTE ; *Gaz. Pal.* 22 mai 2018, n° 18, p. 38, obs. F. FOURMENT.
- Crim. 19 juin 2018, n° 17-86.604 : inédit ; *RSC* 2019 p. 109, note E. DREYER.
- Civ. 1ère, 11 juillet 2018, n° 17-22.381 : Publié au bulletin ; Lexbase Hebdo édition privée, Edition n° 753, 13 septembre 2018, note N. DROIN.
- Crim., 8 janvier 2019, n° 17-81.396 : inédit ; Lexbase Pénal Edition n° 13 du, 21 février 2019, note N. DROIN.

2. <u>Décisions des juges du fond</u>

Avant 1980 :

- TC Seine, 26 décembre 1895 : *D.* 1896, II, 230.
- TC Bourges, 19 juillet 1934 : *D.* 1934, p. 121.
- Dijon, 8 janvier 1936 : *RSC* 1936, 222, note J. MAGNOL.
- Paris, 25 octobre 1961 : *JCP* 1961, II, 12377 ; *RTD Civ.* 1962, p. 302, obs. H. DESBOIS.
- Paris, 4 novembre 1964 : *D.* 1965, somm. p. 35.
- Paris, 6 juillet 1965 : *Gaz. Pal.* 1966, 1, 29.
- TGI Seine, 23 juin 1966 : *JCP* G 1966, II, 14875, R. LINDON.
- TGI Paris, 27 février 1970 : *JCP* 1970, II, 16293, note R. LINDON.

- Paris, 15 mai 1970 : *D.* 1970, p. 466, concl. J. CABANNES ; *RTD Civ.* 1971, p. 114, obs. R. NERSON.
- TC Aix-en Provence, 16 octobre 1973 : *JCP*, 1974, II, n°17623, note R. LINDON ; *RSC* 1976, p. 119, obs. G. LEVASSEUR.
- Toulouse, ch. d'accusation, 26 février 1974 : *JCP* G 1975, II, 17903, note R. LINDON ; *D.* 1974, p. 736 ; *RSC* 1976, p. 119, obs. G. LEVASSEUR.
- TGI Paris 14 mai 1974 : *D.* 1974, p. 766, note R. LINDON.
- TGI Paris, 7 novembre 1975 : *D.* 1976, p. 270, note R. LINDON.
- TGI Saint-Étienne, 19 avril 1977 : *D.* 1978, p. 123, note R. LINDON.

Décennie 1980 :

- Paris, 9 juillet 1980 : *D.* 1981, p. 72, note R. LINDON
- Paris, 27 février 1981 : *D.* 1981, p. 457, note R. LINDON ; *RTD Civ.* 1983, p. 114, obs. R. NERSON et J. RUBELLIN-DEVICHI.
- Paris, 15 juin 1981 : *Gaz. Pal.* 1982, 1, 34.
- Paris, 7 octobre 1981 : *D.* 1982, p. 403, note R. LINDON.
- Paris, 4e ch. B, Dame Birkin c/ SA Ici Paris, 17 novembre 1983 : *D.* 1985, somm. p. 166.
- Basse-Terre, 14 octobre 1985 : JurisData n° 1985-600064 ; *Gaz. Pal.* 1986, 1, somm. p. 12.
- TGI Paris, 20 novembre 1985 : *D.* 1987, p. 140, note D. AMSON.
- Paris, 1ère ch. B, 3 octobre 1986, Antenne 2 c/ Dame André : *D.* 1987, p. 137, obs. R. LINDON et D. AMSON.
- TGI Paris, 17 décembre 1986 : *Gaz. Pal.* 1987, 1, somm. p. 238.
- Paris, 7 janvier 1988 : *Dr. pén.* 1988. comm. 63, obs. M. VERON.
- Paris, 11ème ch., 18 mai 1988 : JurisData n° 1988-025000 ; *Gaz. Pal.* 1989, 1, p. 49, note M. DOMINGO ; *D.* 1990, p. 35, 2e esp., note G. DROUOT.
- TGI Paris, 19 janvier 1989, Grimaldi c/ Cogédipresse : *Gaz. Pal.* 1990, 2, somm. p. 467.
- TGI Paris, 3 mai 1989 : *D.* 1989, p. 228.
- TGI Paris, 27 septembre 1989, Chatel c/ SA République : *Gaz. Pal.* 1991, 1, somm. p. 52.

Décénnie 1990 :

- Paris, 11 janvier 1990 : *D.* 1990, p. 56.
- Douai, 7 octobre 1992 : *JCP* E 1994. I. 359, n° 15, obs. M. VIVANT et C. Le STANC.
- TGI Paris, 16 avril 1996 : *D.* 1997, p. 72, obs. J.-Y. DUPEUX.
- TGI Paris, 1ère ch., 1ère sect., 10 juillet 1997 : *Gaz. Pal.* 18 janvier 1998, p. 42, note A. COUSIN.
- Paris, 11ème ch., sect. A, 7 janvier 1998 : *Dr. pén.* 1998, comm. 63, obs. M. VERON.
- Douai, 4ème ch., 3 mars 1999 : Jurisdata n° 1999-045434 ; *JCP* G 2000, IV, 1615.
- TI Puteaux, 28 septembre 1999, AXA Conseil IARD et AXA Conseil Vie c/ MM. C. M. et C. Sapet, Société Infonie : *Légipresse* n° 168, janvier-février 2000 p. 19.
- TI Paris (11ème arrondissement) 3 août 1999. Société Group Tests c/ Groupe Worldnet : *Légipresse* n° 168, janvier-février 2000 p. 22.

Décennie 2000 :

- TGI Paris, 25 février 2000, n° 9821770011 : *D. Affaires* 2000, p. 219, obs. X. DELPECH.
- TGI Paris, ordonnance de référé, 22 mai 2000, UEJF et Licra c/ Yahoo ! Inc. Et Yahoo ! France.
- Grenoble, 30 octobre 2000, n° 98/03451.
- TGI Paris, ordonnance de référé, 20 novembre 2000, UEJF et Licra c/ Yahoo ! Inc. Et Yahoo ! France.
- TGI Nanterre, 13 décembre 2000 : *CCE*, février 2001, n° 19, obs. A. LEPAGE.
- Paris, 20 septembre 2001, n° 2000/14309 : *D.* 2002, p. 2300, obs. A. LEPAGE.
- Nimes, 3ème ch. corr., 22 mai 2001 : JurisData n° 2001-157851.
- Paris, 1ère ch., sect. B, 20 septembre 2001, n° 2000/14309 : *D.* 2002, p. 2300, obs. A. LEPAGE.
- Paris, 14ème ch., sect. A, 7 novembre 2001, n° 2001/17740 : *D.* 2002, p. 2373, obs. L. MARINO.
- Paris, chambre correctionnelle 11 section B, 14 février 2002 : JurisData n° 2002-181380.
- TC Toulouse, 27 juin 2002 : *D.* 2002, p. 2972, comm. C. LIENHARD.
- TGI Paris, 17ème ch., 22 octobre 2002 : *Légipresse*, 2003, n° 198-I, p. 12.
- Paris, 30 octobre 2002, Kitetoa c/ Sté Tati : *CCE* 2003, comm. 5 ; *D.* 2003, p. 2827, note C. Le STANC ; *LPA* 26 mai 2003, n° 104, p. 12, note E. BOURGEOIS ; *Expertises* 2003, 266, n° 33.
- Paris, ch. corr. 11, 23 Juin 2004, n° 04/00485.
- TGI Paris, 15 novembre 2004, Comité de défense de la cause arménienne c/ M. Aydin A. et Sté France Télécom.
- Paris, Ch. 14, sect. B, 21 janvier 2005, n° 04/14975.
- Paris, ch. corr. 11 section A, 22 Mars 2005 : JurisData n° 2005-277904.
- Paris, 11ème ch. A, 25 janvier 2006, n° 04/21266 : *D.* 2006, p. 2706, obs. C. BIGOT.
- Montpellier, Ch. corr. 3, 2 Février 2006 : JurisData n° 2006-301727.
- Aix-en-Provence, 19è ch. corr., 7 mars 2006 : JurisData n° 2006-312418.
- Grenoble, 1ère ch. corr., 21 juin 2006 : JurisData n° 2006-314267.
- Paris, 24 avril 2007 : *CCE* 2007, n° 156, obs. A. LEPAGE.
- Rennes, 31 mai 2007, n° 07/969 : AJ Pénal 2007, p. 376.
- TGI Paris, 13 juillet 2007, Christian C. c/ Dailymotion : Propr. Intell. 2008. 364, obs. J. PASSA.
- TGI Paris, ord. Réf., 9 janvier 2008, RG n° 07/58913, R. Mezrahi a. c/ YouTube Inc.
- Agen, 20 août 2008 : JurisData n° 2008-002884.
- TC Paris, 17ème ch., 13 octobre 2008, RG n° 08/98771, Bachar K. a. c/20 minutes (SAS) a. : *JCP* G 2008. 646, obs. E. DERIEUX ; *RLDI* 2008/43, n° 1424, obs. L. COSTES ; *RLDI* 2008/44, n° 1454, note J.-L. FANDIARI.
- TGI Paris, 17e ch., 18 décembre 2008 : *RLDI* janvier 2009, n° 45, p. 26, note E. DERIEUX ; *RLDI* octobre 2010, n° 64, p. 29-32, note L. BELFANTI et P. BELLOIR.
- Amiens, Ch. corr., 15 Avril 2009, n° 08/01374.
- TGI Paris, 3ème ch., 3ème sect., 13 mai 2009, Temps noir et autres c/ Youtube, Google Inc, Dailymotion : *Légipresse* 2009, n° 263.
- Paris, pôle 2, ch. 7, 1er octobre 2009, n° 09/00619 : inédit.
- TGI Paris, 17ème ch., 9 octobre 2009, n° 08-02.523039 : *CCE* 2010, comm. 6, obs. A. LEPAGE ; *Dr. pén.* 2010, chron. 5, n° 28, obs. O. MOUYSSET.
- Paris, 3è Pôle, 5è ch., 9 décembre 2009 : JurisData n° 2009-019596.

Après 2010 :

- TGI Paris, réf., 13 avril 2010, n° 10/53340.
- TGI Paris, 20 avril 2010 : *RLDI* 2010/61, n° 2019.
- Clermont-Ferrand, ch. corr., le 24 juin 2010, n°1138/10.
- Reims, ch. civ., 1ère sect., 20 juillet 2010, n° 08/01519, eBay France et International c/ Hermès International et a.
- Paris, pôle 5, ch. 2, 3 septembre 2010, n° 08/12821, eBay Inc, eBay International c/ Christian Dior Couture.
- Paris, pôle 5, ch. 1, 13 octobre 2010, R. Magdane C/ Dailymotion : *Légipresse* 2011, n° 277-19.
- CPH Boulogne-Billancourt, 19 novembre 2010, n° 10/00853.
- TGI Paris, 17e ch. civ., 24 novembre 2010, n° 09/16298 : *CCE* n° 3, mars 2011, comm. 28, A. LEPAGE.
- TGI Paris, ord. req., 6 décembre 2010, Société OVH, *RLDI* 2011/67, n° 2206.
- Paris, pôle 5, ch. 2, 4 février 2011, n° 09/21941, Google et a. c/ Aufeminin.com et a. : *Légipresse* 2011, p. 209, n° 282-16.
- TGI Paris, 2 décembre 2011 : *Légipresse* 2011, n° 279, p. 12.
- TGI Paris, ord. réf., 10 février 2012, n° 12/51224, Claude Guéant c/ Free et a.
- Toulouse, Ch. appl. corr. 3, 27 février 2012 : JurisData n° 2012-012168.
- Bordeaux, 1ère ch., sect. B., 10 mai 2012, Amen c/ M. K.
- TGI Paris, 3ème ch., 1ère sect., 29 mai 2012, TF1 et a. c/ YouTube.
- TGI Paris, 4ème sect., 13 septembre 2012, n° 09/19255, TF1 et a. c/ Dailymotion : *CCE* 2012, comm. 122, note A. DEBET ; *RLDI* 2012/88, n° 2948, note B. VANDEVELDE.
- Montpellier, 14 novembre 2012 : *Légipresse* 2013, n° 301, p. 14.
- TGI Bobigny, 14e ch. corr., 15 novembre 2012, Éric R., MMA Vie c/ M.L.
- TGI Paris, 24 janvier 2013, n° 13/50276, UEJF/ Twitter Inc. Et Sté Twitter France : *Légipresse* n° 304, p. 235 com. N. MALLET-POUJOL.
- TGI Paris, 17e ch. corr., ordonnance de référé, 4 avril 2013 : *CCE* n° 7-8, juillet 2013, comm. 83, A. LEPAGE.
- Paris, pôle 1, ch. 2, 4 avril 2013, RG n° 12/12001, B. Rose c/ JFG Networks.
- Paris, Pôle 1, Chambre 5, ordonnance du 12 juin 2013, UEJF c/ Twitter.
- Nîmes, 3ème ch., 18 octobre 2013, n° 13/00447, Leila T. c/ Stéphane B. et Julien S. : *CCE* n° 2, Février 2014, comm. 23. É. CAPRIOLI,
- TGI Paris, Laurence c. / Telfrance Serie, Facebook France, 28 novembre 2013.
- TC Metz, jugement du 3 avril 2014, n° minute 812/2014, n° parquet : 12261000018.
- TGI Nantes, sect., A, 6ème ch., 3 septembre 2014, T. Meilhon c/ M.-O. Amaury, L. François : *RLDI*, 1er avril 2015, nº 114, p. 29-33 ; *RLDI*, 1er avril 2015, nº 115, p. 28-31.
- Paris, 10 Octobre 2014, n° 13/7387 : É. A. CAPRIOLI, *CCE*, n° 1, décembre 2015, comm. 9.
- TGI Paris, 24e ch. corr. 1, 21 novembre 2014, n° 10183000010 et n° 13311000700 : *CCE*, n° 10, Octobre 2015, comm. 85, É. CAPRIOLI.
- Paris, pôle 5, 1ère ch., 2 décembre 2014, n° 13/08052, TF1 et a. c/ Dailymotion et a. : *Gaz. Pal.* 5 mars 2015, n° 64, p. 20, note L. MARINO ; *JCP* E 2015, 1165, note J.-B. BELIN et L. CONTASSOT-VIVIER.
- TGI Paris, 13e ch. corr., 18 décembre 2014, n° 12010064012 : *RLDI* janvier 2015, n° 111, obs. J. de ROMANET ; *RSC* janvier-mars 2015, p. 101, Chron. J. FRANCILLON.

- TGI Paris, 20 janvier 2015, association Comité IDAHO c/ M. X. et a. : *Légipresse*, n° 326, avril 2015, p. 212.
- TGI Paris, 16e ch. corr., 18 mars 2015 : JurisData n° 2015-005323.
- TGI Paris, 17e ch. corr., 24 mars 2015 : *CCE* n° 10, Octobre 2015, comm. 86, É. CAPRIOLI.
- TGI Paris, 17e ch. corr., 28 mai 2015 : *Légipresse* n° 336, Mars 2016, chron. I. SOSKIN, p. 146.
- TC Metz, jugement du 8 septembre 2015, n° minute 1654/2015, n° parquet 13330000030.
- TGI Paris, 4 décembre 2015, Goyard St-Honoré c/ LBC France.
- Paris, 12 février 2016, n° 15/08624 : *D.* 2016, p. 422 ; *D.* 2016, p. 1045, obs. H. GAUDEMET-TALLON et F. JAULT-SESEKE ; *RTD Civ.*, 2016, 310, obs. L. USUNIER ; *CCE* 2016, comm. 33, note G. LOISEAU.
- TGI Paris, ord. réf., 29 mars 2016, Nathalie X. et Philippe Y.c / Emeric Z. : Legalis.net, avril 2016.
- Paris, pôle 3, 13 avril 2016, n° 10183000010 : *Dr. pén.* 2016, chron. 11, A. LEPAGE ; *RSC* 2016 p. 544, J. FRANCILLON.
- Paris, Pôle 2, Chambre 7, 22 juin 2016, E Zemmour et autres contre Licra et autres : *Légipresse* n° 341, p. 460.
- TGI Paris, réf., 12 août 2016 : *CCE* 2016, comm. 105, Éric CAPRIOLI
- TGI, 17ème ch., 15 décembre 2016, n° 13059000638 : *Légipresse*, 2017, n° 346, p. 71.
- Nancy, 1ère ch. civ., 3 juillet 2018, n° 17/011693.
- Dijon, ch. corr., 7 février 2018, n° 18/00081.
- TGI Paris, 17ème ch., 7 juin 2017, Ministère public c/ Mohamed B. et Jenna K : *Légipresse* n° 354, novembre 2017, p. 529.
- TGI Paris, 17ème ch., 30 juin 2017, Urssaf Ile-de-France c/ José X : *Légipresse* n° 354, novembre 2017, p. 529.

B. Décisions du Conseil constitutionnel

- Cons. const., 17 janvier 1989, n° 88-248 DC : *JO* 18 janvier 1989, p. 754.
- Cons. const., 28 juillet 1989, n° 89-260 DC : *JO* 1er août 1989, p. 9676 ; *RFDA* 1989 p. 671, obs. B. GENEVOIS ; *Pouvoirs* 1990, n° 52, p. 189, obs. P. AVRIL et J. GICQUEL.
- Cons. const., 30 décembre 1997 n° 97-395 DC.
- Cons. const., 16 juin 1999, n° 99-4141 DC.
- Cons. const., 23 juillet 1999, n° 99-416 DC.
- Cons. const., 12 janvier 2002, no 2001-455 DC : *RSC* 2002. 674, obs. V. BÜCK.
- Cons. const., 29 août 2002, n° 2002-461 DC.
- Cons. const., 10 juin 2004, n° 2004-496 DC : *JO* 22 juin 2004, p. 11182 ; *AJDA* 2004, 1534, note J. ARRIGHI de CASANOVA ; *AJDA*, 1385, tribune P. CASSIA ; *AJDA* 2004, 1497, tribune M. VERPEAUX ; *AJDA* 2004, 1537, note M. GAUTIER et F. MELLERAY, note D. CHAMUSSY ; *AJDA* 2004, 2261, chron. J.-M. BELORGEY, S. GERVASONI et C. LAMBERT ; *D.* 2005, p. 1125, obs. V. OGIER-BERNAUD et C. SEVERINO ; *RFDA* 2004 651, note B. GENEVOIS ; *JCP* G 2004. II. 10117, note P. BLANCHETIER ; *CCE* 2004, ét. n° 32, note G. DECOCQ ; *LPA* 18 juin 2004, n° 122, p. 10, note J.-E. SCHOETTL.
- Cons. const., 10 juin 2009, n° 2009-580 DC : *JO* 13 juin 2009, p. 9675 ; *Constitutions* 2010, p. 97, obs. H. PERINET-MARQUET ; Constitutions 2010, p. 293, obs. D. BELLESCIZE ; *D.* 2009, p. 1770, point de vue J. M. BRUGUIERE ; *D.* 2009,

p. 2045, point de vue L. MARINO ; *D.* 2010, p. 1508, obs. V. BERNAUD et L. GAY ; *RSC* 2009, p. 609, obs. J. FRANCILLON ; *D.* 2010, p. 209, obs. B. LAMY ; *RTD Civ.* 2009. 754, obs. T. REVET ; *RTD Civ.* 2009, p. 756, obs. T. REVET ; *RTD Com.* 2009, p. 730, étude F. POLLAUD-DULIAN ; *RLDI* 2009, n° 51, p. 114, obs. C. SIMON.

- Cons const., 25 février 2010, n° 2010-604 DC.
- Cons. const., 16 septembre 2011, QPC n° 2011-164 : *JCP* G 2011, 1247, note E. DREYER ; *CCE* 2011, comm. 106, obs. A. LEPAGE ; *Gaz. Pal.* 12-13 octobre 2011, p. 11, obs. F. FOURMENT ; *D.* 2011. p. 2444, note L. CASTEX ; AJ Pén. 2011, n° 594, obs. S. LAVRIC ; *RSC* 2011, n° 647, obs. J. FRANCILLON, Dr pén. 2012, Chron. n° 5, obs. O. MOYSSET ; *Légipresse* 2011, p. 688, note A. FOURLON.
- Cons. const., 4 mai 2012, n° 2012-339 QPC.
- Cons. const., 4 mai 2012, n° 2012-240 QPC.
- Cons. const., 6 février 2015, n° 2014-448 QPC : *D.* 2015. 324 ; *ibid*. 2465, obs. G. ROUJOU de BOUBEE, T. Garé, C. GINESTET, M.-H. Gozzi et S. MIRABAIL ; *RSC* 2015. 86, obs. Y. MAYAUD ; AJ Pénal 2015. 248, note E. DREYER.
- Cons. const., 18 mars 2015, n^{os} 2014-453/454 et 2015-462 QPC : *JO* 20 mars 2015, p. 5183 ; *D.* 2015 p. 874, obs. O. DECIMA ; *JCP* 2015, n° 13, p. 369, obs. J.-H. ROBERT ; *RSC* 2015 p. 705, obs. B. de LAMY .
- Cons. const., 14 janv. 2016, n° 2015-513/514/526 QPC : *JO* 16 janvier 2016, n° 54 ; *D.* 2016 p. 931, obs. O. DECIMA ; *Dr. pén.* 2016 n° 46, obs. E. BONIS-GARÇON et V. PELTIER ; *Banque et Droit* 2016, n° 165, p. 55, obs. J. CHACORNAC.
- Cons. const., 7 avril 2017, n° 2017-625 DC.
- Cons. const., 10 février 2017, n° 2016-611 QPC : AJ Pénal 2017. 237, obs. J. ALIX ; David P., *D.* 2017 p. 354 ; *Dalloz IP/IT* 2017 p. 289, obs. M. QUEMENER.
- Cons. const., 15 décembre 2017, n° 2017-682 QPC : Droit pén. n° 2, Février 2018, comm. 22, P. CONTE.

C. Décisions des autorités administratives indépendantes

- CNIL, délibération n° 2011-035, 17 mars 2011 : *CCE* 2012, étude 1, note A. DEBET.
- CNIL, délibération n° 2013-420, 3 janvier 2014 : *JCP* G 2014 n° 7, 211, obs. E. DERIEUX.
- CNIL, décision n° 2015-048 du 24 juin 2015 mettant en demeure la société SAMADHI SAS.
- CNIL, décision n° 2015-021 du 24 juin 2015 mettant en demeure la société TOODATE.COM SARL.
- CNIL, délibération n° 2016-054, 10 mars 2016 : *CCE* 2016, comm. 65, note A. DEBET.
- CSA, ass. plén., 16 novembre 2016 : *RLDI* février 2017, n° 134, comm. P. MOURON.
- CNIL, délibération n° 2017-006, 27 avril 2017, prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland.
- CSA, décembre n° 2017-532, 26 juillet 2017, portant sanction à l'encontre de la société C8 : *RLDI* août 2017, n° 140, comm. E. DERIEUX.
- CSA, Ass. plén., décembre du 20 décembre 2017 : *Légipresse* n° 357, février 2018, p. 74.

D. Décisions des juridictions européennes

1. Cour EDH

- CEDH, *Engel et autres c. Pays-Bas*, 8 juin 1976, n° 5100/71.
- CEDH, *Handyside c/ Royaume-Uni*, série A, 7 décembre 1976, n° 5493/72.
- CEDH, *Öztünk c/ Allemagne*, 21 février 1984, n° 8544/79.
- CEDH, *X et Y c. Pays-Bas*, 26 mars 1985, n° 8978/80 : *RSC* 1985, p. 629, obs. L. E. PETTITI ; *JDI* 1986, p. 1082, obs. P. ROLLAND et P. TAVERNIER.
- CEDH, *B. c/ France 25*, mars 1992, n° 13343/87.
- CEDH, *Niemietz c. Allemagne*, 16 décembre 1992, n° 13710/88 : *D.* 1993, p. 386, obs. J.-F. RENUCCI ; *JCP* G 1993, I, 3654, obs. F. SUDRE.
- CEDH, *Burghartz c. Suisse*, 22 février 1994, n° 16213/90 : *RTD Civ.* 1994, p. 563, obs. J. HAUSER ; *JCP* 1995, I, 3823, chron. F. Sudre ; *D.* 1995, p. 5, note J.-P. MARGUÉNAUD ; *RTDH* 1995, p. 53, obs. P. GEORGIN.
- CEDH, *Botta c. Italie*, 24 février 1998, n° 21439/93 : *RTDH* 1999, p. 600, obs. B. MAURER ; *D.* 1998, p. 371, N. FRICERO.
- CEDH, *Oliveira c/ Suisse*, 30 juillet 1998, n° 25711/94.
- CEDH, *Goodwin c/ Royaume-Uni*, 27 mars 1996, n° 17488/90.
- CEDH, *Buckley c. R.-U*, 25 septembre 1996, n° 20348/92 : *JCP G* 1997, I, 4000, n° 33, obs. F. SUDRE.
- CEDH, *Cantoni c/ France*, 15 novembre 1996, n° 17862/91 : *JCP* 1997.II.22836, note FOUASSIER et VION ; *RSC* 1997, chron. p. 462.
- CEDH, *Fischer c/ Autriche*, 29 mai 2001, n° 37950/97.
- CEDH, *Pretty c. R.-U.*, 29 avril 2002, n° 2346/02 : *RSC* 2002, p. 645, obs. F. MASSIAS ; *RTDH* 2003, p. 71, note O. De SCHUTTER.
- CEDH, *Sofianopoulos et autres c. Grèce*, 12 décembre 2002, n° 1988/02.
- CEDH, *Radio Helle Norge Asa c/ Norvège*, 6 mai 2003, n° 76682/01 : *RLDI* octobre 2010, n° 64, p. 29-32, note L.BELFANTI et P. BELLOIR.
- CEDH, *Garaudy c/ France*, 24 juin 2003, n° 65831/01.
- CEDH, *Van Hannover c/ Allemagne*, 24 juin 2004, n° 59320/00,: *JCP* G 2004, I , 161, Obs. SUDRE ; *D.* 2004, p. 3538, obs. J.-F. RENUCCI.
- CEDH, *Norwood c/ Royaume-Uni* 16 novembre 2004, n° 23131/03.
- CEDH, *Prokopovich c.* Russie, 18 novembre 2004, n° 58255/00 : *JCP* G 2005, I, 103, n° 11, obs. F. SUDRE.
- CEDH, *Ivanov c/ Russie*, 20 février 2007, n° 35222/04.
- CEDH, *Garetta c/ France*, 4 mars 2008, n° 2529/04.
- CEDH, *Bigaeva c. Grèce*, 28 mai 2009, n° 26713/05 : *JCP* G 2009, 143, n° 16, obs. F. SUDRE.
- CEDH, *Polanco Torres et Movilla Polanco c. Espagne*, 21 septembre 2010, n° 34147/06 : *Légipresse* 2011, n° 279, p. 63, obs. G. LOISEAU.
- CEDH, *Obst c. Allemagne*, 23 septembre 2010, n° 425/03 : *RDT* 2011, p. 45, note J. COUARD ; *Légipresse* 2011, n° 279, p. 63, obs. G. LOISEAU ; *RTDH* 2011, p. 375, note G. De BECO.
- CEDH, *Ahmet Yildirim c. Turquie*, 18 décembre 2012, n° 3111/10.
- CEDH, *Söderman c. Suède*, 12 novembre 2013, n° 5786/08 : *JCP* G 2014, p. 106, n° 13, obs. F. SUDRE.
- CEDH, *M'Bala M'Bala c/ France*, 20 octobre 2015, n° 25239/13.
- CEDH, *Nodet c. France*, 6 juin 2019, n° 47342/14 : *D. actu.*, 27 juin 2019, obs. P. DUFOURQ ; *JCP G* n° 25, 24 Juin 2019, note L. MILANO.

2. CJCE/CJUE

- CJCE, *Bodil Lindqvist*, 6 novembre 2003, aff. C-101/01.
- CJCE, *Mediakabel BV c/ Commissariaat voor de Media*, 3ème ch., 2 juin 2005, aff. C-89/04 : *RLDI* 2015 n° 9, p. 26-32, note M. MORITZ.
- CJCE, *Tietosuojavaltuutettu*, 16 décembre 2008, aff. C-73/07.
- CJUE, *Infopaq International A/S c./ Danske Dagblades Forening*, 16 juillet 2009, aff. C-5/08.
- CJUE, *Sté Google c/ Sté Louis Vuitton Malletier*, 23 mars 2010, aff. C-236/08 à C-238/08 : *JCP* G 2010, note 642, L. MARINO ; *JCP* G 2011, 1175, doctr. F. TERRÉ ; *CCE* 2010, comm. 88, note P. STOFFEL-MUNCK ; *CCE* 2010, comm. 70, note C. CARON ; *CCE* 2010, étude 12, G. BONET ; *D.* 2010, p. 885, obs. C. MANARA ; *RTDE* 2010, p. 939, obs. E. TREPPOZ ; *CCC* 2010, comm. 132, note M. MALAURIE-VIGNAL ; *RLDI* 2010/60, n° 1980, note L. GRYNBAUM ; *RLDI* 2010/61, n° 1999, note C. CASTETS-RENARD ; *Légipresse* 2010, n° 274, p. 158, note C. MARECHAL ; Propr. industr. 2010, comm. 31, note P. TREFIGNY-GOY.
- CJUE, *L'Oréal et a. c/ eBay International et a.*, 12 juillet 2011, aff. C-324/09 : *CCE* 2011, comm. 99, note C. CARON ; Propr. industr. 2011, comm. 71, note A. FOLLIARD-MONGUIRAL ; *Gaz. Pal.* 26 octobre 2011, n° 299, p. 19, note L. MARINO ; *D.* 2011, p. 1965, obs. C. MANARA ; *D.* 2011, p. 2054, point de vue P.-Y. GAUTIER ; *RTDE* 2011, p. 847, obs. E. TREPPOZ ; *RLDI* 2011/74, n° 67, note C. CASTETS-RENARD ; *RLDI* 2011/74, n° 2459, p. 61, note L. GRYNBAUM.
- CJUE, *Scarlet c/ SABAM*, 3èrech., 24 novembre 2011, aff. C-70/10 : *Gaz. Pal.* 16 février 2012, p. 20, note L. MARINO ; *CCE* 2012, comm. 63, note A. DEBET ; *RSC* 2012, p. 163, obs. J. FRANCILLON.
- CJUE, *SABAM c/ Netlog*, 3ème ch., 16 février 2012, aff. C 360/10 : *Gaz. Pal.*, 1er août 2012, p. 18, note L. MARINO ; *CCE* 2012, comm. 63, note A. DEBET.
- CJUE, *Google Spain c/ Mario Costeja González*, grde ch., 13 mai 2014, aff. C-131/12.
- CJUE, *Maximillian Schrems c/ Data Protection Commissioner*, 6 octobre 2015, aff. C-362/14.
- CJUE, *Breyer, B. Pautrot*, 19 octobre 2016, aff. C-582/14 : *RLDI* 2017, n° 134, p. 23 ; *CCE* 2016, comm. 104, obs. N. METALLINOS ; Rev. int. Compliance 2016, comm. 130, obs. M. GRIGUER et J. SCHWARTZ.
- CJUE, *Menci*, 20 mars 2018, aff. C-524/15 – CJUE, *Garlsson Real Estate*, 20 mars 2018, aff. C-537/16 – CJUE, *Di Puma*, 20 mars 2018, aff. C-596/16 : *D. actu.*, 22 mars 2018, obs. E. MAUPIN ; *RTDE* n° 2 p. 419 ; *AJDA* 2018, 602 ; *ibid.* 1026, chron. P. BONNEVILLE, E. BROUSSY, H. CASSAGNABERE et C. GÄNSER ; *D.* 2018 p. 616 ; Rev. sociétés 2018 p. 731, note H. MATSOPOULOU ; *RSC* 2018, p. 524, obs. F. STASIAK.
- CJUE, *Wirtschaftsakademie Schleswig-Holstein*, 5 juin 2018, aff. C-210/16 : *JCP* G, n° 28, 9 juillet 2018, note D. BERLIN ; *RLDI* juin 2018, n° 149, note L. COSTES.

E. Décisions des juridictions étrangères

- Tribunal constitutionnel de Karlsruhe, 15 décembre 1983 : C. GREWE, « Allemagne. Constitution et secret de la vie privée », AIJC 2000, p. 147.
- Cour constitutionnelle hongroise, 9 avril 1991, Décision n° 15/1991, IV. 13, AB : *Recueil ABH* 1991, 40, *in* P. BON et D. MAUS, *Les grandes décisions des cours constitutionnelles européennes*, Dalloz, 2008, p. 269.
- Cour constitutionnelle fédérale allemande (*Bundesverfassungsgerichsthof*), 4 avril 2006, BverfGE, 1 BvR 518/02, BverfG, 1BvR 2027/02, 23 octobre 2006 : RDP, 2009, n° 6, chron. M. FROMONT, p. 1726.
- Cour constitutionnelle fédérale allemande (*Bundesverfassungsgerichsthof*), 24 avril 2013 : *RDP*, 2014, n° 4, chron. M. FROMONT, p. 1119.

Index Alphabétique

Les chiffres renvoient aux numéros de paragraphes

Table des matières

L'ADAPTATION DU DROIT PÉNAL AUX RÉSEAUX SOCIAUX EN LIGNE
Résumé

Les réseaux sociaux en ligne manifestent la transcription mais également l'intensification des rapports humains à l'échelle numérique. Plus généralement, l'apparition et l'usage massif de ces sites transcrit une évolution profonde des rapports sociaux commencée au milieu des années 2000. Partant, le droit pénal en tant que « *miroir de la civilisation* » s'en trouve nécessairement impacté au point de justifier une adaptation de ce dernier.

Ces sites constituent indéniablement un nouvel espace juridique porteur de comportements cyberdélinquants. Pour la majorité d'entre eux, les réseaux sociaux en ligne ne sont qu'un nouveau support d'atteintes dont les incriminations préexistantes à leur apparition ont parfaitement vocation à s'appliquer. Cependant, de nouvelles formes d'atteintes ont émergé de ces espaces d'échanges mettant en lumière des carences structurelles au sein du droit pénal se traduisant par l'incapacité des incriminations préexistantes à appréhender ces nouvelles formes d'atteintes. Le droit pénal s'est alors adapté par la création de nouvelles incriminations témoignant de l'évolution profonde de la protection pénale de l'intimité et de l'identité et plus généralement, de la vie privée.

Les réseaux sociaux suscitent également des enjeux pour le droit pénal concernant la répression des comportements cyberdélinquants pouvant s'y retrouver. En l'occurrence, les régimes de responsabilité pénale applicables aux différents acteurs des réseaux sociaux, utilisateurs et opérateurs, démontrent une inadaptation certaine se matérialisant par un problème d'effectivité de la loi pénale sur les réseaux sociaux. La solution consiste alors à faire évoluer, ou plutôt diversifier la réponse aux infractions en développement et encadrant une régulation des contenus en collaboration avec l'autorité administrative. Se dessine alors un nouveau régime de responsabilité applicable aux principales plateformes numériques de partage favorisant progressivement en leur sein une logique de mise en conformité. Au final, tant le droit pénal s'adapte aux réseaux sociaux en ligne que les réseaux sociaux en ligne s'adaptent au droit pénal.

THE ADAPTATION OF CRIMINAL LAW FOR ONLINE SOCIAL NETWORKS
Abstract

Online social networks demonstrate the transcription, as well as the intensification, of human relationships on a digital level. More generally, the apparition and widespread use of these sites reveal a profound evolution of social relationships that began in the mid-2000s. Consequently, criminal law, as a "*mirror of civilisation*" has necessarily been impacted to the extent of warranting its adaptation.

These websites undeniably constitute a new legal arena within which delinquent online behaviour is present. For the most part, online social networks are merely a new medium for infringements, to which pre-existing criminal offences are perfectly designed to apply. However, new forms of infringements have emerged from these places of exchange, highlighting the structural shortcomings within criminal law, that manifest as the inability of pre-existing criminal offences to cover these new forms of infringements. Criminal law has therefore adapted through the creation of new criminal offences, demonstrating the profound evolution of the protection of privacy, identity and more generally, private life, under criminal law.

Social networks also raise criminal law issues with regard to the suppression of delinquent online behaviour that can be found on them. In this case, the regimes of criminal responsibility applicable to different social network players, users and operators, demonstrate a certain unsuitability which manifests itself as the ineffectiveness of criminal law on social networks. The solution therefore consists of developing, or rather diversifying the response to emerging offences and providing a framework for the regulation of content in collaboration with the administrative authorities. A new regime of responsibility thus emerges, applicable to the main digital sharing platforms, that progressively promotes a principle of compliance within them. Ultimately, criminal law adapts to online social networks as much as social networks adapt to criminal law.