Université Paris Panthéon-Assas

École doctorale de droit international, droit européen, relations internationales et droit comparé

Thèse de doctorat en droit public
soutenue le 13 octobre 2023

Thèse de Doctorat octobre 2023

L'encadrement juridique européen et international des cyberviolences

Carlotta GRADIN

Sous la co-direction de MM. les Professeurs Fabrice Picod et Olivier de Frouville.

Membres du jury de thèse :

Mme Anne-Thida NORODOM, Professeure à l'Université Paris-Cité

M. Sébastien VAN DROOGHENBROECK, Professeur à l'Université Saint-Louis-Bruxelles (rapporteur)

Mme Claire VIAL, Professeure à l'Université de Montpellier (rapporteure)

À ma famille.

Avertissement

La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

Je souhaite remercier chaleureusement mes directeurs de thèse, Messieurs les professeurs Fabrice Picod et Olivier de Frouville pour leur confiance, pour avoir cru en moi et à mon sujet de thèse. Je les remercie pour m'avoir accompagnée de près pendant ces années à travers leur grande expertise, leurs conseils fins, ainsi que leurs encouragements. Merci pour vos mots rassurants qui m'ont permis d'avancer sereinement pendant mon parcours doctoral. Je tiens également à adresser mes plus vifs remerciements à Mesdames les Professeures Claire Vial et Anne-Thida Norodom ainsi qu'à Monsieur le Professeur Sébastien Van Drooghenbroeck, pour m'avoir fait l'honneur d'accepter de siéger dans mon jury de soutenance.

Je remercie ma famille, mes parents, Lorella et Giampaolo, pour leur soutien indéfectible, pour croire en moi et pour m'avoir donné la possibilité de me former et de grandir professionnellement loin d'eux. Merci à mon frère Giulio qui m'encourage depuis mon plus jeune âge. Un grand merci à mon oncle Sergio et à ma tante Carla que, depuis mon enfance, me soutiennent et m'accompagnent dans mes réalisations en portant de l'art et de la musique dans ma vie.

Un grand merci à toi, Arnaud, pour ton soutien sans faille. Merci de croire en moi, de me soutenir et de m'encourager à donner le meilleur de moi-même.

Merci à toutes et tous mes collègues du CRDH et du CDE, en particulier, Joanne, Wendy, Nadia, Claire et Pauline, pour leur soutient.

Je remercie également mes collègues d'ONU Femmes France et d'EUROsociAL+ pour m'avoir encouragée pendant mes dernières années de thèse.

Un grand merci à mes amies et à leur patience, merci, en particulier à Pauline, Anna, Saskia et Berta et à l'énergie positive de Silvina.

Résumé : L'encadrement juridique européen et international des cyberviolences

Les violences en ligne ne sont pas un phénomène nouveau, elles existent depuis la création d'Internet. En perpétuelle évolution, elles prennent différentes formes et touchent les utilisateurs du monde entier. Les caractéristiques d'Internet confèrent à ces comportements illicites des spécificités qui ont un impact sur leur qualification et sur leur régime.
Si progressivement des réglementations juridiques ont été adoptées au niveau national et européen pour les encadrer, il n'existe pas encore une définition claire de cyberviolence et des règles uniformes reconnues par la communauté internationale pour protéger les droits fondamentaux des utilisateurs. De plus, le cadre préventif et répressif demeure insatisfaisant. Cela conduit à des conséquences négatives, notamment en termes d'évaluation du phénomène et d'adoption de mesures appropriées, ainsi que des manquements en matière de protection des destinataires des services.

Descripteurs : droit international ; droit européen ; droit comparé ; droits fondamentaux ; cyberviolences ; Internet ; cyberespace ; prévention ; sanction ; nouvelles technologies.

Title and Abstract: The European and international legal framework for cyber-violence

Online violence is not a new phenomenon, it has existed since the creation of the Internet. It is constantly evolving, taking different forms and affecting users all over the world. The characteristics of the Internet give to these illicit behaviors special characteristics that have an impact on their qualification and on their regime. Although legal provisions have gradually been adopted both at national and European levels to regulate them, there is still no clear definition of cyber-violence and no uniform rules recognized by the international community to protect the fundamental rights of users. Moreover, the preventive and repressive framework remains unsatisfactory. This leads to negative consequences, particularly in terms of evaluating the phenomenon and adopting appropriate measures, as well as a lack of protection for the recipients of the service.

Keywords: International law; European law; comparative law; fundamental rights; cyber-violence; Internet; cyberspace; prevention; sanction; new technologies.

Principales abréviations

AGNU	Assemblée générale des Nations Unies
CEDH	Convention européenne des droits de l'Homme
CSA	Conseil supérieur de l'audiovisuel
CSNU	Conseil de sécurité des Nations Unies
Cour EDH	Cour européenne des droits de l'Homme
CNIL	Commission nationale de l'informatique et des libertés
DSA	Digital Services Act
EI	État islamique
EIGE	Institut européen pour l'égalité entre les femmes et les hommes
EUROPOL	European Union Agency for Law Enforcement Cooperation
GREVIO	Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique
INTERPOL	Organisation internationale de police criminelle
IA	Intelligence artificielle
LGBTQIA+	Lesbiennes, gays, bisexuels, transgenres, queers, personnes en questionnement, intersexes, asexuels, alliés et plus
NetzDG	Loi Netzwerkdurchsetzungsgesetz
ODD	Objectifs de Développement Durable
ONG	Organisation non gouvernementale
ONU	Organisation des Nations Unies
ONU Femmes	Agence des Nations unies pour l'égalité de genre et l'autonomisation des femmes
ORECE	Organe de régulateurs des communications électroniques
RGPD	Règlement général sur la protection des données
TIC	Technologies de l'information et de la communication
TUE	Traité sur l'Union européenne

TFUE	Traité sur le fonctionnement de l'Union européenne
SGNU	Secrétaire général des Nations Unies
UE	Union européenne
UNESCO	Organisation des Nations unies pour l'éducation, la science et la culture
UNICEF	Fonds des Nations unies pour l'enfance
UNICRI	Institut interrégional de recherche des Nations unies sur la criminalité et la justice
UNODC	Office des Nations unies contre les drogues et le crime
UIT	Union internationale des télécommunications
WFA	Fédération mondiale des annonceurs

Sommaire

« Nommer c'est dévoiler, et dévoiler c'est déjà agir »

S. DE BEAUVOIR, *Le sexisme ordinaire*, Seuil, 1979, p. 7.

« La violence n'est pas innée chez l'homme. Elle s'acquiert par l'éducation et la pratique sociale »

F. HERITIER, *Le Monde de l'éducation*, 2001.

Introduction

1. Le phénomène des cyberviolences date de l'apparition d'Internet vers la fin des années 80. Trente ans plus tard, leur définition juridique ne fait pas l'unanimité au sein de la communauté internationale. Comme le disait Simone De Beauvoir nommer un phénomène c'est déjà agir, agir pour mieux le connaître et mieux y répondre. Le principe qui porte à penser que ce qui est illégal hors ligne devrait l'être en ligne[1] nous paraît peut être une évidence. Toutefois, au fur et à mesure de nos recherches il est apparu que ce principe n'était pas établi. Pour cela, nous chercherons à analyser si cette équivalence existe en droit, en nous intéressant aux rapports entre le droit numérique et les droits fondamentaux et plus particulièrement à la définition et à l'encadrement juridique des violences en ligne. Les cyberviolences évoluent rapidement et s'adaptent à leur théâtre d'opération : les nouvelles technologies de l'information et de la communication. Et cela représente un grand défi pour les droits nationaux, le droit européen et international.

2. Pour commencer, il est nécessaire de définir les termes du sujet.

I. La définition de cyberespace et des violences

3. D'abord, définir le mot « violence » est complexe. Aujourd'hui, la violence semble « indéfinissable »[2] et de nombreux auteurs qui ont travaillé sur le sujet, l'ont fait sans forcément en donner une définition précise[3]. Nous assimilons souvent la « violence » à la violence physique et plus généralement à l'intégrité de la personne. Toutefois, ce mot qualifie également des atteintes psychologiques ou économiques. Dans ce travail, nous adoptons la même approche que celle du Conseil de l'Europe, en particulier celle utilisée dans la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence

[1] *« Les mêmes droits dont les personnes disposent hors ligne doivent être aussi protégés en ligne »,* Conseil des droits de l'Homme, La promotion, la protection et l'exercice des droits de l'homme sur Internet, résolution 32/13, 18 juillet 2016, A/HRC/RES/32/13, § 1.
[2] Y. MICHAUD, « Définir la violence ? », *Les cahiers dynamiques,* 2014/2, n°60, p. 35.
[3] M.MARZANO, *Dictionnaire de la violence,* PUF, 2011, p. VIII.

à l'égard des femmes et la violence domestique[4]. Cette dernière définit la « violence à l'égard des femmes » comme : « une violation des droits de l'homme et une forme de discrimination […] qui entraînent, ou sont susceptibles d'entraîner pour les femmes, des dommages ou souffrances de nature physique, sexuelle, psychologique ou économique, y compris la menace de se livrer à de tels actes, la contrainte ou la privation arbitraire de liberté, que ce soit dans la vie publique ou privée »[5]. Même si cette définition concerne une catégorie de personne déterminée, nous estimons qu'elle est universelle et détient l'avantage de montrer le caractère multiforme des violences qui ont lieu dans la sphère privée ou publique.

Selon la philosophe Hannah Arendt, quand nous nous approchons du domaine de la violence, il y a un élément d'imprévisibilité totale[6]. Pour elle, « dans un monde stable et régulier, [la violence] introduit le dérèglement et le chaos »[7]. Cette imprévisibilité est également l'une des caractéristiques des cyberviolences que nous étudierons dans nos travaux.

Enfin, nous appréhendons la notion de violence également avec celle de « vulnérabilité ». Nous définissons la vulnérabilité comme un état « de la personne dont la situation conduit à constater qu'elle est susceptible de subir une atteinte »[8]. Comme souligné par M.-H. Soulet la vulnérabilité est la « potentialité à être blessé »[9]. Dans plusieurs systèmes juridiques et notamment en droit pénal, la vulnérabilité est reprise comme un élément constitutif de l'infraction ou bien comme une circonstance aggravante[10]. Cet état touche certaines personnes au regard de certaines caractéristiques intrinsèques ou extrinsèques[11]. En premier lieu, à cause de leur condition physique ou

[4] Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, STCE n° 210, Istanbul, 11 mai 2011.
[5] Article 3 a) de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, STCE n° 210, Istanbul, 11 mai 2011.
[6] Y. MICHAUD, « Définir la violence ? », *Les cahiers dynamiques*, 2014/2, n°60.
[7] *Ibid.*
[8] T. REVET, Rapport de synthèse, in *La vulnérabilité*, Journée québécoises 2018, Association Henri Capitant, Bruylant, 2020, p. 10.
[9] M.-H. SOULET, « La vulnérabilité comme catégorie de l'action publique », *Pensée plurielle*, 2005/2, n°10, 2005, pp. 50 et 55.
[10] T. REVET, Rapport de synthèse, in *La vulnérabilité*, Journée québécoises 2018, Association Henri Capitant, Bruylant, 2020, p. 12.
[11] M. BLONDEL, *La personne vulnérable en droit international*, Thèse de doctorat, Université de Bordeaux, 2015, pp. 56-100.

mentale, mais également de leurs caractéristiques biologiques. En second lieu, des évènements extérieurs qui les défavorisent par rapport à d'autres individus (comme la situation économique, politique et migratoire).

La vulnérabilité a été saisie à plusieurs reprises par les textes européens et internationaux et des listes sont souvent élaborées qui mettent en avant les catégories de personnes les plus vulnérables. Parmi les exemples, la directive 2013/33/UE du Parlement européen et du Conseil, du 26 juin 2013, établissant des normes pour l'accueil des personnes demandant la protection internationale qui indique comme personnes vulnérables « les mineurs, les mineurs non accompagnés, les handicapés, les personnes âgées, les femmes enceintes, les parents isolés accompagnés d'enfants mineurs, les victimes de la traite des êtres humains, les personnes ayant des maladies graves, les personnes souffrant de troubles mentaux et les personnes qui ont subi des tortures, des viols ou d'autres formes graves de violence psychologique, physique ou sexuelle, par exemple les victimes de mutilation génitale féminine »[12]. La Cour européenne des droits de l'Homme cite également certaines catégories comme les femmes, les enfants, les personnes transgenre et les demandeurs d'asile[13].

Sur Internet, nous verrons que certaines des personnes considérées vulnérables hors ligne le sont également en ligne et sont surexposées aux comportements illicites.

Cependant, nous tenons à souligner que nous ne considérons pas tous les membres de ces catégories comme vulnérables. En effet, les caractéristiques de chaque personne doivent être analysées dans leur contexte. Nous ne voulons pas défendre une « logique d'essentialisation »[14], mais montrer que certains individus sont plus vulnérables que d'autres dans certaines circonstances, ce qui peut justifier des politiques et des actions ciblées.

---

[12] Article 21 de la directive 2013/33/UE du Parlement européen et du Conseil, du 26 juin 2013, établissant des normes pour l'accueil des personnes demandant la protection internationale.
[13] L. BURGORGUE LARSEN, *La vulnérabilité saisie par les juges en Europe,* Cahiers européens, Pedone, 2014, voir en particulier le chapitre de S. BESSON pour une analyse de la vulnérabilité dans la jurisprudence de la Cour européenne des droits de l'Homme et E. DUBOUT pour une analyse de la vulnérabilité dans la jurisprudence de la Cour de justice de l'Union européenne.
[14] M.-H. SOULET, « La vulnérabilité, une ressource à manier avec prudence » in L. BURGORGUE LARSEN, *La vulnérabilité saisie par les juges en Europe,* Cahiers européens, Pedone, 2014, p. 13.

4. **La distinction entre le cyberespace et Internet** - Le terme « cyber » ajouté au mot « violence » indique que ces dernières sont perpétrées dans le cyberespace. Appliqué aux comportements illicites en ligne, « the term « cyber » is used to capture the different ways that the Internet exacerbates, magnifies or broadcasts the abuse »[15]. Pour le grand public le terme « cyberespace » est souvent synonyme d'Internet. Au contraire, au sein du milieu universitaire et militaire[16] ce dernier est désigné comme un « environnement »[17] ou un « théâtre d'opérations »[18]. Le cyberespace est défini comme un « domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des services en ligne. »[19]. Cette définition, comme souligné par Barbara Louis-Sidney, a le mérite de prendre en compte trois dimensions du cyberespace. Celle physique qui correspond à Internet ; celle logique qui englobe les logiciels et les protocoles du réseau et, enfin, celle cognitive qui concerne l'ensemble des données et des informations qui circulent sur le réseau[20]. Pour certains auteurs, nous parlons de cyberespace pour échapper à la territorialisation du droit. Internet, par nature n'est pas territorialisé, il n'a pas de frontières spatiales ou physiques[21], il est invisible et intangible[22]. Alors que pour d'autres, il présente des

[15] UN Broadband Commission for digital development working group, *Cyberviolence against women and girls, A world-wide wake-up call*, 2015, p. 21. Traduction de l'autrice « Le terme « cyber » est utilisé pour décrire les différentes façons dont l'Internet exacerbe, amplifie ou diffuse les abus ».
[16] A. DESFORGES, « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, 2014/1-2, n° 152-153, 2014, p. 67-81.
[17] R. J. HARKNETT, J. P. CALLAGHAN and R. KAUFFMAN, « Leaving Deterrence Behind: War-Fighting and National Cybersecurity », *Journal of Homeland Security and Emergency Management*, January 2010.
[18] O. KEMPF, *Introduction à la cyberstratégie*, Economica, 2eme édition, 2015.
[19] Glossaire interarmées de terminologie opérationnelle, document cadre DC-004_GIATO(2013), N° 212/DEF/CICDE/ NP, 16 décembre 2013, amendée le 1er juin 2015.
[20] B. LOUIS-SIDNEY, « La dimension juridique du cyberespace », *Revue internationale et stratégique*, 2012/3, n° 87, 2012, p. 73-82.
[21] A.T. NORODOM, « Internet et le droit international : défi ou opportunité ? », in *Internet et le droit international*, SFDI, Pedone, 2014, p. 25-26.
[22] S. Rosenne le cyberespace est « is invisible, unidentifiable, irrefragable, intangible, and cannot be felt or identified in any way: it has no known natural characteristics », voir S. ROSENNE, *The perplexity of Modern International Law*, RCADI, 2003, T III, p.349.

frontières électroniques[23] qui, toutefois, ne permettent pas de délimiter des compétences étatiques[24].

Concernant la définition d'« Internet », selon l'Institut national de la statistique et des études économiques (INSEE) il s'agit d'un ensemble de réseaux mondiaux interconnectés qui permet à des ordinateurs et à des serveurs de communiquer efficacement au moyen d'un protocole de communication commun (IP). Internet permet d'accéder à plusieurs services comme les messageries électroniques, les plateformes de réseaux sociaux ou le « Web », c'est-à-dire le « service permettant d'accéder à des serveurs multimédias interactifs offrant divers services ou contenant des documents de toute nature (textes, images, sons, logiciels) »[25].

5. **La définition retenue de cyberviolences** - Concernant la définition de « violences en ligne » ou « cyberviolences », aujourd'hui il n'existe pas une définition universellement acceptée par le droit international ou par le droit de l'Union européenne. Outre quelques exceptions que nous étudierons dans ces travaux, les droits nationaux ne présentent pas non plus une définition unitaire de ces infractions. Il existe des définitions élaborées par des institutions et des organismes internationaux. Dans ce travail, nous nous sommes basés sur la définition adoptée par le Comité de la Convention du Conseil de l'Europe sur la cybercriminalité. Ce dernier, définit la cyberviolence comme « l'utilisation de systèmes informatiques pour causer, faciliter ou menacer de causer à des personnes de la violence qui entraine ou est susceptible d'entrainer un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques et peut comprendre l'exploitation de leur situation, de leurs caractéristiques ou de leur vulnérabilité »[26].

---

[23] A.T. NORODOM, « Internet et le droit international : défi ou opportunité ? », in *Internet et le droit international*, SFDI, Pedone, 2014, p. 26 qui cite D. VENTRE, Cyberespace et acteurs du cyberconflits, Lavoisier, 2011, p.83.
[24] *Ibid*, p. 26.
[25] P. SIRINELLI, « L'adequation entre le village virtuel et la création normative - Remise en cause du role de l'État ? » in K. BOELE-WOELKI et C. KESSEDJIAN, *Internet: Which Court Decides? Which Law Applies?*, 1998, pp. 29-30.
[26] Conseil de l'Europe, Comité de la Convention sur la cybercriminalité, *Étude cartographique sur la cyberviolence*, 2018, p.5.

En effet, les violences en ligne se présentent sous différentes formes : physiques, sexuelles, psychologiques et économiques et s'exercent dans le cadre privée (foyer), public (entre personnes connues ou inconnues) mais également dans le monde du travail.

Les cyberviolences sont également l'une des catégories de la cybercriminalité. Cette dernière, selon la Commission européenne, englobe trois catégories d'activités criminelles : « La première comprend les formes traditionnelles de criminalité, telles que la fraude ou la falsification (…). La deuxième concerne la publication de contenus illicites par voie électronique (par exemple, ceux ayant trait à la violence sexuelle exercée contre des enfants ou à l'incitation à la haine raciale). La troisième vise les infractions propres aux réseaux électroniques, c'est-à-dire les attaques visant les systèmes d'information, le déni de service et le piratage »[27]. Nous nous intéresserons plus particulièrement à la deuxième catégorie énoncée.

De plus, la Convention du Conseil de l'Europe sur la cybercriminalité, premier texte contraignant au niveau international en la matière, distingue également cinq catégories d'infractions en ligne. L'une d'entre elles concerne les infractions se rapportant au contenu et plus particulièrement les contenus se rapportant à la pédopornographie[28].

6. **Les comportements et les contenus illicites -** Cela nous amène à définir également le terme « contenu » et les différentes typologies de contenus. D'abord, avec le terme « contenu » nous définissons toute information partagée en ligne sous forme d'écrit, image, vidéo ou fichier audio. Ensuite, nous pouvons distinguer plusieurs typologies des contenus : un contenu illégal ou illicite quel que soit le contexte, un contenu illicite en raison de son contexte, ainsi qu'un contenu préjudiciable mais qui n'est pas illicite[29].

   En premier lieu, le « contenu illicite quel que soit le contexte » est défini comme toute information sous forme d'écrit, image, vidéo ou audio qui n'est pas conforme au droit

---

[27] Voir Communication de la Commission au Parlement européen, au Conseil et au Comité des Régions - Vers une politique générale en matière de lutte contre la cybercriminalité, COM/2007/0267 et M. QUEMENER, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », *Sécurité et stratégie*, 2011/1 (5), 2011, p. 56-67.

[28] Article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité adoptée le 23 novembre 2001 à Budapest.

[29] Conseil de l'Europe, Modération de contenu, *Meilleures pratiques en vue de la mise en place de cadres juridiques et procéduraux efficaces pour les mécanismes d'autorégulation et de corégulation de la modération de contenu,* Note d'orientation, Adoptée par le Comité directeur sur les médias et la société de l'information (CDMSI), Juin 2021, pp. 40-42.

international, au droit européen mais également au droit national dans la limite du respect des droits humains. En effet, nous verrons que certains États adoptent des lois qui vont à l'encontre des droits et libertés des individus sur Internet. Certains États adoptent, par exemple, des mesures pour filtrer ou bloquer l'accès à des contenus considérés illicites, mais qui, en réalité, ne le sont pas, pour censurer les défenseurs des droits humains ou les opposants politiques. De plus, un contenu peut être illicite lorsqu'il ne respecte pas les règles internes établies par des sociétés privées, telles les plateformes des réseaux sociaux. Cependant, il arrive qu'un contenu qui porte atteinte aux règles internes des plateformes n'enfreigne pas le droit national.

Ensuite, le « contenu illicite en raison de son contexte » se caractérise par une publication qui n'est pas illicite en soi mais qui le devient à cause de la manière dont elle est mise à disposition du public. Un exemple est le partage des contenus à caractère sexuel sans le consentement de la victime. En effet, le contenu, comme une photo ou une vidéo intime, n'est pas en soi illicite si pris avec le consentement de la personne ; il le devient lorsque ce même contenu est diffusé sans son consentement[30].

Enfin, il peut y avoir des contenus préjudiciables mais qui ne sont pas forcément illégaux. C'est le cas, par exemple, des écrits ou des vidéos de désinformation.

7. Même si la plupart des comportements illicites en ligne constituent une infraction pénale, il y a également des infractions qui relèvent d'autres branches du droit privé. Nous utiliserons indistinctement le terme « cyberviolences » et « violences en ligne » pour caractériser et qualifier tous les comportements illicites de contenu commis à travers les nouvelles technologies de l'information et de la communication. D'autres auteurs utilisent également le terme de « technology-facilitate abuse » ou « technology-facilitate violence » pour souligner que les violences sont facilitées par les nouvelles technologies.

8. Selon certains auteurs, notamment Romain Boos, les cyberviolences sont, très souvent, des infractions qui existent déjà dans le droit commun avant Internet et qui ont trouvé en ce dernier un formidable moyen de se pérenniser et de se développer. Pour certains auteurs, le cyberharcèlement, par exemple, serait une simple transposition du

[30] *Ibid.* p. 42.

harcèlement vers le monde virtuel, il ne s'agirait que d'un changement de contexte[31]. Cette analyse semble identifier le cyberespace en tant qu'endroit comme un autre dans lequel les violences ont lieu.

9. D'autres auteurs ne sont pas du même avis. Certains, comme Leroux, estiment que le cyber espace est un espace complexe qui ne peut pas être défini comme une copie numérique du monde et qui, par conséquent, est le théâtre des violences qui ont des particularités et qui ne sont pas seulement une simple répétition des violences hors ligne[32]. Englander et Muldowney[33] décrivent la cyberviolence comme une infraction opportuniste, puisqu'elle cause un préjudice sans interaction physique, exigeant peu de planification et en réduisant la menace d'être pris.

10. En effet, ce que nous pouvons constater est que les violences en ligne se caractérisent par plusieurs éléments. Premièrement, ces violences se retrouvent dans l'espace numérique. Par conséquent la dissémination de leurs conséquences nuisibles est très large. Cela est rendu possible par l'abolition des distances physiques qui a permis de s'affranchir de la distance et de perpétrer les infractions depuis un ou plusieurs endroits vers un ou plusieurs autres endroits. Ces caractéristiques s'ajoutent au fait que les violences en ligne ont lieu 24h/24 7j/7, leur diffusion est instantanée et sans fin car les contenus sont stockés en ligne et peuvent resurgir à tout moment. Les contenus peuvent être envoyés à « n'importe quel point du cyberespace » et diffusés « en tous points de ce même espace »[34]. Ces contenus peuvent devenir « viraux » et les victimes n'ont pas de répit. En effet, les auteurs eux-mêmes, une fois leur message publié, n'ont plus de maîtrise sur sa diffusion, ce qui permet à tout internaute de s'emparer du contenu et de le diffuser. Les commentaires, les photos ou les vidéos peuvent produire rapidement un effet boule de neige, depuis l'envoi initial, les renvois, les partages et les captures d'écran

---

[31] C. BLAYA, « Le cyberharcèlement chez les jeunes », *Enfance*, 2018/3, n° 3, p. 421-439.
[32] Leroux, 2011.
[33] ENGLANDER and MULDOWNEY, 2007. Englander and Muldowney describe cyberbullying as an opportunistic offense, since it results in harm without physical interaction, requires little planning, and reduces the threat of being caught.
[34] P. LAGRANGE, « Internet et l'évolution normative du droit international : d'un droit international applicable à l'internet à un DI du cyberespace ? », in *Internet et le droit international*, SFDI, Pedone, 2014, p. 65. Le texte reprend les termes de « immédiateté et ubiquité » utilisés pour caractériser le cyber espace dans l'article de J. PATRICK, « La gouvernance de l'Internet du point de vue du droit international public », in *Annuaire français de droit international*, volume 56, 2010, p. 544 qui reprend l'ouvrage de M. DELMAS-MARTY, *Les forces imaginantes du droit. Le relatif et l'universel*, Paris, Seuil, 2004, pp. 331 s.

qui permettent au contenu de ne jamais disparaître. La viralité est l'une des caractéristiques qui explique l'amplification des cyberviolences. Il s'agit de la diffusion rapide et imprévisible des contenus sur Internet, qu'ils soient licites ou illicites. La viralité implique que les actions abusives sont plus rapides de celles hors de l'espace numérique. Et, comme nous le verrons dans ces travaux, la viralité est rendue possible par des outils propres à Internet et aux plateformes en ligne.

Deuxièmement, agir illicitement sur Internet ne demande pas beaucoup d'efforts et de moyens financiers. Le budget pour certaines infractions en ligne est de plus en plus accessible. Certains outils pour commettre des infractions[35] sont achetés à des prix raisonnables voir gratuits ou donnés en échange pour d'autres types de services. Ce phénomène est appelé par Nicolas Arpagian « consumerisation »[36] des outils d'attaque, et cela montre que c'est à cause de la demande que ces outils existent. Toutefois, pour un grand nombre de violences, aucun outil n'est nécessaire, le plus souvent un ordinateur et une connexion Internet suffisent.

Troisièmement, Internet permet aux utilisateurs d'agir anonymement. L'anonymat peut être un facilitateur pour la diffusion des contenus illicites. Ce dernier peut être défini selon deux composantes, une composante active qui consiste « à ne pas être identifié alors qu'on agit »[37] et une passive « qui consiste à rester à l'écart des interactions sociales pour éviter de faire l'objet d'identifications »[38]. Aujourd'hui, très peu d'utilisateurs font la distinction entre anonymat et pseudonymat. En effet, seuls les individus qui utilisent un TOR[39] ou d'autres techniques (par exemple des services de proxies anonymes) peuvent être vraiment anonymes sur Internet. Les autres, notamment ceux qui utilisent un simple pseudonyme, ne le sont pas et peuvent être identifiés par les plateformes et les forces de l'ordre. Cependant, l'anonymat ou le pseudonymat, est un facteur décisif

---

[35] Par exemple pirater le téléphone ou l'ordinateur d'une personne afin de voler des informations personnelles, des photos intimes et/ou échanges intimes.

[36] Conseil National des Femmes Françaises et Fondation Scelles, Colloque « Cyberviolences - Cybercriminalité », Palais du Luxembourg, 2 décembre 2019. Programme disponible sur : http://www.cnff.fr/CNFF-Colloque-Cyber-criminalite-cyber-violences.pdf

[37] E. DAVIO, « Anonymat et autonomie identitaire sur Internet », in *Droit des technologies de l'information*, sous la direction de Etienne Montero, CRID, Bruyant, 1999, p. 298.

[38] *Ibid.*.

[39] Le TOR est un service de réseau mondial qui permet d'anonymiser l'origine des connexions. Il permet d'empêcher la localisation des appareils connectés ainsi que la traçabilité des recherches en ligne, pour plus d'informations voir : https://www.torproject.org/.

concernant les conséquences de violences en ligne. En effet, les victimes qui ne connaissent pas leur agresseur se retrouvent dans une situation de déséquilibre de pouvoir et d'impuissance. L'anonymat réduit les capacités de « coping »[40] des victimes et restreint le niveau d'empathie des agresseurs qui ne perçoivent pas les effets de leurs actes sur les victimes[41].

Quatrièmement, contrairement aux violences hors ligne, les nouvelles technologies permettent une multiplication des cibles et d'agresseurs. Aujourd'hui, un individu isolé peut s'attaquer à une multitude de personnes ; de la même façon un individu peut être victime d'un « raid numérique »[42] c'est-à-dire être attaqué par un ensemble d'individus de manière concerté[43].

Cinquièmement, les cyberviolences ont un caractère transnational. C'est-à-dire qu'un utilisateur peut être exposé à des contenus illicites dans un État A, publiés dans un État B et dont les images sont prises dans un État C.

Enfin, il est aussi important de souligner une autre caractéristique des cyberviolences qui est celle de l'attribution de la responsabilité. En effet, plusieurs acteurs sont concernés : d'un côté les utilisateurs qui peuvent être victimes ou agresseurs, de l'autre les États qui peuvent manquer à leur obligation de protéger leurs citoyens et, enfin, les plateformes qui sont responsables lorsque des contenus signalés n'ont pas été retirés.

---

[40] LAZARUS et FOLKMAN (1984) définissent le *coping* comme « l'ensemble des efforts cognitifs et comportementaux destinés à maîtriser, réduire ou tolérer les exigences internes ou externes qui menacent ou dépassent les ressources d'un individu », voir A. MARIAGE, Stratégies de coping et dimensions de la personnalité : étude dans un atelier de couture, *Le travail humain*, 2001/1, Vol. 64.

[41] C. BLAYA, « Le cyberharcèlement chez les jeunes », *Enfance*, 2018/3, n° 3, p. 424 et O'BRIEN et MOULES, 2010.
La désinhibition des agresseurs et le manque d'empathie sont souvent favorisés par « l'effet cockpit » qui indique la distance entre l'agresseur et la victime. Voir également Haut Conseil à l'Égalité entre les femmes et les hommes, *En finir avec l'impunité des violences faites aux femmes en ligne, : une urgence pour les victimes*, 2017, p. 25 et Observatoire régional des violences faites aux femmes du Centre Hubertine Auclert, *Cybersexisme : une étude sociologique dans des établissements scolaires franciliens*, 2016.

[42] Le « raid numérique » appelé également « harcèlement de meute » est défini par l'article 222-33 du Code pénal français comme des propos ou comportements imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée. Mais également, des propos ou comportements sont imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition.

[43] Un exemple célèbre en France est celui de la « Ligue du LOL », un groupe de journalistes français que, à travers un groupe Facebook, organisaient de raid numérique sur Twitter à l'encontre de collègues journalistes femmes ou hommes homosexuels.

11. Après avoir défini les cyberviolences, il est nécessaire d'identifier et introduire les acteurs du cyberespace.

II. Les acteurs du cyberespace

12. **La définition d'utilisateur** - Premièrement, l'utilisateur, l'usager ou le « destinataire de service » est « toute personne physique ou morale utilisant un service intermédiaire, notamment pour rechercher une information ou la rendre accessible »[44]. Le règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques (Digital Services Act) définit également le « destinataire actif d'une plateforme en ligne » comme « le destinataire du service qui a été en contact avec une plateforme en ligne, soit en demandant à la plateforme en ligne d'héberger des informations, soit en étant exposé aux informations hébergées par la plateforme en ligne et diffusées via son interface en ligne »[45].

La définition des acteurs privés - Avec le terme « plateformes en ligne » nous considérons « un service d'hébergement qui, à la demande d'un destinataire du service, stocke et diffuse au public des informations, à moins que cette activité ne soit une caractéristique mineure et purement accessoire d'un autre service ou une fonctionnalité mineure du service principal qui, pour des raisons objectives et techniques, ne peut être utilisée sans cet autre service, et pour autant que l'intégration de cette caractéristique ou de cette fonctionnalité à l'autre service ne soit pas un moyen de contourner l'applicabilité du présent règlement »[46]. Nous pouvons également utiliser le terme « fournisseur de services » qui est défini comme « toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et toute autre entité traitant ou stockant des données informatiques pour ce

[44] Article 3 (b) du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[45] *Ibid.* article 3 (p)
[46] *Ibid.* article 3 (i).

service de communication ou ses utilisateurs »[47]. Il s'agit donc de l'intermédiaire entre l'éditeur des contenus et l'utilisateur[48].

La distinction entre l'hébergeur et l'éditeur - Le premier est défini par la Cour de justice de l'Union européenne comme un prestataire de service qui exerce son activité ayant un caractère « purement technique, automatique et passif » et qui « n'a pas la connaissance ni le contrôle des informations transmises ou stockées »[49]. Au contraire, l'éditeur est celui qui « édite » le contenu publié en ligne et pour cela il a un véritable rôle actif « dans le contenu du site de nature à [lui] conférer une connaissance et un contrôle des données publiées sur [le] site »[50]. Ces caractéristiques sont essentielles pour comprendre la différence d'attribution de la responsabilité lorsque des contenus illicites sont publiés en ligne. En effet, d'un côté, l'hébergeur est responsable seulement s'il avait la connaissance ou le contrôle des données stockées[51], en particulier s'il avait connaissance du caractère illicite d'un contenu, et il n'a pas pris des mesures pour le retirer ou rendre son accès impossible. De l'autre, l'éditeur est responsable des contenus qu'il publie.

13. **La distinction entre les médias sociaux et les réseaux sociaux -** Les médias sociaux sont des supports de diffusion massive d'information dont font partie la presse écrite, la radio ou la télévision. Pour être considérés comme tels, ils doivent permettre l'interaction sociale, utiliser des technologies récentes et permettre la création de contenu. Les médias sociaux ont comme finalité de diffuser des messages. Ils permettent à tout le monde de participer et de partager des contenus. Plus particulièrement, les usagers peuvent créer des contenus, les organiser, modifier et commenter. C'est le cas de YouTube pour le partage des vidéos et Flickr pour le partage de photos. Certains chercheurs analysent les médias sociaux en utilisant un modèle d'analyse des médias traditionnels en

---

[47] Article 1 (c) de la Convention du Conseil de l'Europe sur la cybercriminalité adoptée le 23 novembre 2001 à Budapest.
[48] Voir également P. VAN CLEYNENBREUGEL, *Plateformes en ligne et droit de l'Union européenne, Un cadre juridique aux multiples visages*, 1re édition, Bruylant, 2020 et A. BEELEN, C. CHARLIER, J. VIGNERON, *Guide pratique des plateformes*, 20 legal designs commentés, 1ère édition, Larcier, 2021.
[49] CJUE, GC, *Google France et Google Inc c. Louis Vuitton Malletier*, 23 mars 2010, affaires jointes C-236/08 à C-238/08, §113.
[50] TGI Paris, ordonnance de référé, *Lafuma Mobilier c. Alibaba a.*, 21 novembre 2017.
[51] CJUE, GC, *Google France et Google Inc c. Louis Vuitton Malletier*, 23 mars 2010, affaires jointes C-236/08 à C-238/08, §120.

décomposant plusieurs étapes : la création, l'agrégation, la distribution et la consommation[52]. La chercheuse Lucile Merra y ajoute d'autres phases, notamment une phase de sélection et de fabrication[53]. Pour connaître le panorama des médias sociaux, le spécialiste d'Internet Frédéric Cavazza propose une division entre les médias de discussion, de messagerie, de partage, de publication, de réseautage et les médias collaboratifs[54].

14. Ensuite, les réseaux sociaux sont une sous-catégorie des médias sociaux et se concentrent sur l'interaction entre leurs usagers. Le groupe de travail G29 sur la protection des données définit les services de réseautage comme des « plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs »[55]. C'est notamment le cas de Meta (Facebook et Instagram)[56], Snapchat, TikTok ou LinkedIn. Le réseau social a comme principale caractéristique celle de créer des interactions et des liens sociaux entre des individus. Ces interactions peuvent apparaître après la création d'un profil qui est personnalisé et personnalisable et à travers des connexions (amis, « followers »). Dans chaque réseau social, les individus créent des contenus adaptés au format du réseau, par exemple sur Instagram il s'agit de photos ou de vidéos et sur Twitter (ou « X »[57]) des textes qui doivent respecter un certain nombre de caractères.

15. Il y a également les blogs et les forums qui peuvent être le théâtre de certains comportements illicites. Richard Donegan donne des exemples de cyberharcèlement sur des forums[58] utilisés par des collégiens pour insulter leurs camarades de façon anonyme. Selon Azy Barak les messages sexuels humiliants, les remarques sexuelles ou les

---

[52] L. MERRA, *Pour une sociologie des médias sociaux. Internet et la révolution médiatique : nouveaux médias et interactions*, Thèse de doctorat, Paris Sorbonne Cité - Paris Descartes, 2013, p. 125.
[53] *Ibid*. p. 126.
[54] F. CAVAZZA, Panorama des médias sociaux, 6 mai 2021. Disponible sur : https://fredcavazza.net/2021/05/06/panorama-des-medias-sociaux-2021/
[55] Groupe de travail « Article 29 » sur la protection des données, avis 5/2009 sur les réseaux sociaux en ligne, 01189/09/FR, WP 163, 12 juin 2009, point 2, p. 4. Disponible sur : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp163_fr.pdf
[56] Le groupe Meta, anciennement Facebook, détient les réseaux sociaux Facebook et Instagram ainsi que le système de messagerie instantanée WhatsApp.
[57] Le réseau « Twitter » a été rebaptisé « X » le 24 juillet 2023 par Elon Musk qui l'a acheté en octobre 2022.
[58] Par exemple College ABC et Juicy Campus

plaisanteries vulgaires sont souvent pratiqués sur les « chats rooms », les forums[59] ou les moteurs de recherche[60].

16. Concernant l'action et la responsabilité de ces acteurs, ces derniers peuvent être qualifiés à la fois comme des hébergeurs ou des éditeurs après un examen du rôle qu'ils ont pu jouer vis-à-vis du contenu illicite publié sur Internet. En effet, un acteur peut exercer plusieurs fonctions à la fois[61]. Pour cela, le régime de responsabilité sera appliqué selon leur qualification et leur réaction face au contenu illicite.

17. Aujourd'hui les cyberviolences se retrouvent dans tous les médias et réseaux sociaux. Toutefois, certaines formes d'infractions se retrouvent plus sur certains réseaux sociaux ou sites Internet que d'autres. Par exemple, les commentaires haineux et les menaces ont lieu surtout sur les réseaux sociaux comme Facebook, Twitter ou YouTube, car ils se manifestent après la publication d'une photo, une vidéo ou une actualité qui ne fait pas consensus. Les infractions sexuelles[62] ont lieu, en particulier, sur les sites de rencontres, sur les messageries instantanées comme Messenger ou Telegram ou des plateformes de jeux vidéo mais aussi sur les logiciels qui permettent aux utilisateurs d'échanger à travers une webcam (Skype par exemple). Le recrutement des femmes ou hommes exercé par les réseaux de prostitution ou de pédocriminalité se retrouvent sur des sites de rencontre, des sites Internet lambda par exemple des sites d'annonces en ligne[63] ou sur des réseaux sociaux type Instagram. De plus, l'utilisation des médias sociaux est variable selon les États : par exemple, en Israël, concernant la prostitution c'est surtout Tinder[64] qui est

---

[59] B. AZY, « Sexuel Harassment on the internet », *Social Science Computer Review*, Vol. 23 No. 1, Spring 2005, p. 77-92.

[60] Le moteur de recherche est défini comme « un service numérique qui permet aux utilisateurs de formuler des requêtes afin d'effectuer des recherches sur, en principe, tous les sites internet ou les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot-clé, d'une demande vocale, d'une expression ou d'une autre entrée, et qui renvoie des résultats dans quelque format que ce soit dans lesquels il est possible de trouver des informations en rapport avec le contenu demandé », voir l'article 2 (h) bis de la proposition de règlement du Parlement européen et du Conseil, du 15 décembre 2020, relatif à un marché intérieur des services numériques et modifiant la directive 2000/31/CE (« Digital Services Act »).

[61] M. DELMAS-MARTY, *Les forces imaginantes du droit. Le relatif et l'universel*, Paris, Seuil, 2004, p. 345.

[62] Par exemple, le voyeurisme digital, c'est-à-dire le fait de regarder les parties intimes d'une personne sans son consentement, de les prendre en photo ou en vidéo et de les partager en ligne ; ou le « sextage » abusif qui est l'échange non consensuel d'écrits, images, vidéos ou d'autres contenus à caractère sexuel sur Internet.

[63] Par exemple Backpage.com aux États-Unis ou VivaStreet en France.

[64] Fondation Scelles, *Système prostitutionnel, Nouveaux défis, nouvelles réponses, 5e rapport mondial*, 2019, p. 350.

utilisé alors qu'en Zambie ce sont les messageries comme WhatsApp ou le réseau social Facebook[65]. Les outils où les cyberviolences sont détectées varient aussi en fonction de l'âge et du sexe de l'utilisateur. Selon une étude du Pew Research Center[66] les utilisateurs qui ont plus de 50 ans et qui ont subi du cyberharcèlement sont susceptibles de dire que ces types de violences ont eu lieu par email. Les plus jeunes, au contraire, subissent ces violences sur les réseaux sociaux, en particulier les filles, et les garçons sur les plateformes de jeux en ligne.

18. Depuis plusieurs années les auteurs s'expriment au sujet de l'opportunité d'un encadrement des activités sur Internet.

III. Le droit européen et international face aux cyberviolences

19. La réponse juridique aux comportements illicites en ligne - Selon le professeur Mayer-Schönberger, il y a trois discours principaux : le discours étatiste traditionaliste qui consiste à dire que le seul régulateur approprié du cyberespace est l'État au vu notamment de sa légitimité démocratique ; le discours des cyberséparatistes[67] qui considèrent le cyberespace comme « un espace social distinct et séparé du monde réel » dans lequel les normes nationales ne sont et ne devraient pas s'appliquer ; le discours des cyberinternationalistes qui voient le cyberespace comme une communauté globale internationale possible à gouverner seulement à travers le droit international[68].

En 2003, les États ont pu s'exprimer lors du Sommet mondial sur la société de l'information dans lequel 180 gouvernements ont réaffirmé la pleine applicabilité de la Déclaration universelle des droits de l'Homme en ligne[69].

Toutefois, aucun texte unifié n'a été adopté en la matière. En 2005, la « voie d'une adaptation du texte de la Convention [européenne des droits de l'Homme] à

---

[65] *Ibid.*

[66] Pew Research Center, *Online Harassment*, Octobre 2014. Disponible sur : http://www.pewinternet.org/2014/10/22/online-harassment/

[67] J. P. BARLOW, Déclaration d'indépendance du cyber espace, 8 février 1996.

[68] V. MAYER-SCHÖNBERGER, « The shape of governance: analysing the World of internet regulation », *Virginia Journal of international law*, vol. 43, 2003, p. 612 et s.

[69] Declaration of principles, *Building the Information Society: a global challenge in the new Millennium* », Document WSIS-03/GENEVA/DOC/4-E, World Summit on the Information Society, 12 December 2003. Voir également G. RONA et L. AARONS, State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace, *Journal of National Security Law and Policy*, Cardozo Legal Studies Research Paper No. 503, 27 October 2016, p. 505.

l'environnement numérique a finalement été écartée »[70]. Aujourd'hui nous voyons que des tendances se dessinent en droit international pour défendre les droits fondamentaux en ligne, notamment avec l'adoption de la Convention du Conseil de l'Europe sur la cybercriminalité[71], premier texte international contraignant sur la cybercriminalité et son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Mais encore, à travers l'adoption de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[72], première convention internationale contraignante en la matière. En droit de l'Union européenne, nous constatons des avancées. Nous avons assisté : premièrement, à l'adoption d'instruments de *soft law* comme le Code de conduite signé avec les plateformes numériques[73] ; deuxièmement, à l'adoption du règlement général sur la protection des données (RGPD)[74] et du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques[75]. Ce dernier a comme objectif de renforcer la protection des droits fondamentaux des utilisateurs en responsabilisant plus les plateformes en ligne. Et, enfin, nous avons assisté à la publication de la proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique[76] dans laquelle il y a l'apparition de définitions et sanctions de cyberviolences à l'encontre des femmes. Ces instruments montrent la nécessité de réguler Internet et, en particulier, font apparaître les limites de l'auto-régulation par les acteurs privés.

---

[70] F. DUBUISSON et I. RORIVE, « La liberté d'expression à l'épreuve d'Internet », in *Entre ombres et lumières : cinquante ans d'application de la Convention européenne des droits de l'homme en Belgique*, Centre de droit public de l'Université libre de Bruxelles, Bruxelles, Bruylant, 2008, p. 362.
[71] Convention du Conseil de l'Europe sur la cybercriminalité adoptée le 23 novembre 2001 à Budapest.
[72] Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n°108, Strasbourg, 28 janvier 1981.
[73] Commission européenne, Code de conduite pour la lutte contre les discours haineux illégaux en ligne, mai 2016.
[74] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[75] Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[76] Proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD).

Pour conclure, il faut souligner qu'aucun instrument n'a été adopté aujourd'hui concernant l'encadrement des cyberviolences de contenu dans leur ensemble.

20. L'utilisation d'instruments juridiques déjà existants - La réponse juridique aux cyberviolences dépend de la nature de l'acte, plusieurs instruments juridiques pouvant être mobilisés afin de prévenir et réprimer les comportements illicites.

21. Il n'est pas toujours nécessaire qu'il y ait une réponse pénale, ces violences pouvant être traitées par une approche progressive et une combinaison de mesures préventives, éducatives et protectrices[77]. Aujourd'hui, plusieurs dispositions sont adoptées par les États en droit civil et pénal et également en droit européen et international. Nous constatons que la plupart des dispositions existantes utilisées pour encadrer et réprimer les infractions ne sont pas spécifiques aux violences en ligne, mais concernent plutôt les violences traditionnelles et sont appliquées en les adaptant aux comportements illicites sur Internet. En effet, comme le souligne Agathe Lepage, au sujet de la protection de la personnalité en ligne, « nombre de règles de droit commun ont vocation à remplir leur office sur internet comme si de rien n'était »[78].

Plusieurs conventions internationales protégeant les droits des individus sur Internet peuvent être mentionnées, par exemple la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels[79] et la Convention du Conseil de l'Europe sur la cybercriminalité[80] qui prévoient des dispositions pour les comportements illicites à l'égard des mineurs. Nous pouvons citer également la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique[81], qui ne prévoit pas des dispositions *ad hoc* sur les atteintes sur Internet mais dont les dispositions peuvent être interprétées pour

---

[77] Conseil de l'Europe, Comité de la Convention sur la cybercriminalité, *Étude cartographique sur la cyberviolence*, 2018, p.6

[78] A. LEPAGE, « Les droits de la personnalité confrontés à l'Internet », in *Libertés et droits fondamentaux à l'épreuve d'Internet*, Dalloz, 12eme édition, 2006, p. 229 et cité par L. MARINO, « Les nouveaux territoires des droits de la personnalité », Gazette du palais, 127eme année, n° 138 et 139, mai 2007, p. 24.

[79] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, STCE n° 201, Lanzarote, 25 octobre 2007.

[80] Convention du Conseil de l'Europe sur la cybercriminalité, STCE n° 185, Budapest, 23 novembre 2001.

[81] Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, STCE n° 210, Istanbul, 11 mai 2011.

protéger les femmes victimes de cyberviolences ou encore la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains[82].

Cela mène à une multiplication de dispositions juridiques nationales et à l'absence d'un cadre unifié. Cette situation conduit à plusieurs conséquences négatives, notamment à une faible protection des utilisateurs dans certains États et à l'absence de données fiables sur l'ampleur du phénomène.

Ces dispositions sont très souvent mises sous pression par la balance à faire entre les droits et libertés fondamentaux concurrents. Cela est surtout dû à la multiplicité des droits qui peuvent s'appliquer et à l'extra-territorialité des affaires. Par exemple, le traitement d'un commentaire haineux sur les réseaux sociaux n'est pas le même en France et aux États-Unis où la liberté d'expression prime sur beaucoup d'autres libertés individuelles.

De plus, la prévention et la sanction sont également défiées par la question des acteurs qui opèrent dans la sphère numérique ce qui rend l'attribution de la responsabilité très difficile, notamment entre les hébergeurs et les éditeurs des sites Internet et les utilisateurs.

IV. Genèse et intérêt des travaux

22. **Intérêt du sujet** – Lorsque nous avons commencé l'étude du phénomène des cyberviolences en droit européen et international, ce sujet ne faisait pas encore l'objet d'études juridiques approfondies en France. En principe, nos réflexions sont nées d'un constat relatif aux violences faites aux femmes. En effet plusieurs institutions européennes et internationales, comme l'Institut européen de l'égalité de genre ou ONU Femmes, alertaient sur l'impact disproportionné des violences en ligne sur les femmes et les filles. À partir de là, nous nous sommes intéressés plus en détail à ce phénomène et nous avons constaté qu'il était très peu étudié du point de vue juridique. Plusieurs études sociologiques existantes prouvaient les effets des violences en ligne sur les

[82] Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains, STCE n° 197, Varsovie, 16 mai 2005.

mineurs[83] et les adultes[84], mais aucune réflexion juridique n'avait été menée sur les définitions et l'encadrement juridique.

La loi allemande NetzDG[85] venait à peine d'être adoptée et, en France, le sujet commençait à faire son apparition dans la presse lors des premiers procès médiatiques sur le cyberharcèlement[86]. Cette prise de conscience a mené à l'adoption des lois pour sanctionner le cyberharcèlement, le raid numérique ainsi que le projet de loi Avia en 2020[87].

Suivent ensuite les travaux du Conseil de l'Europe[88] et des institutions européennes[89] ainsi que les colloques et les premières publications académiques en français[90].

Ces constats nous ont mené à proposer un premier travail de thèse sur les définitions et l'encadrement juridique des cyberviolences pour plusieurs raisons. La première est celle de démontrer que le système actuel n'est pas suffisant pour prévenir et sanctionner les cyberviolences. L'intérêt serait donc de proposer des pistes d'amélioration pour l'encadrement des cyberviolences afin que ce phénomène soit mieux appréhendé et traité par le droit européen et international. La deuxième est celle d'en faire un sujet de recherche de premier plan, en effet les violences en ligne sont en pleine expansion et en constant renouvellement, il faudrait continuer à chercher des solutions innovantes pour l'éradiquer. Enfin, la troisième, est celle d'avoir un premier travail de réflexion en français et d'ouvrir la voie à d'autres travaux plus approfondis en la matière, par exemple avec des focus thématiques sur une cible ou un comportement illicite en particulier.

---

[83] Voir par exemple : BLAYA C., « Le cyberharcèlement chez les jeunes », *Enfance*, 2018/3 n°3.
[84] Voir par exemple : BOCIJ P., « Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet », *First monday*, 2003.
[85] Loi Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG) du 1er septembre 2017.
[86] Le procès de Nadia Daam par exemple en 2018, journaliste menacée, avec sa fille, de mort et de viol sur les réseaux sociaux.
[87] Le projet de loi Avia, largement inspiré par la loi allemande NetzDG, visait à lutter contre les contenus illicites sur Internet. La loi a été adoptée en 2020, cependant certaines de ses dispositions phares comme le retrait des contenus manifestement illicites sous 24h par les plateformes ont été censurés par le Conseil constitutionnel.
[88] Voir par exemple : Conseil de l'Europe, Comité de la Convention sur la cybercriminalité, *Étude cartographique sur la cyberviolence*, 2018.
[89] Voir par exemple : VAN DER WILK A., *Cyber violence and hate speech online against women*, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, September 2018.
[90] Voir par exemple : SFDI, *Le standard de due diligence et la responsabilité internationale*, Journée d'études franco-italienne du Mans, Pedone, 2018 ou VAN ENIS Q. et DE TERWANGNE C., *L'Europe de droits de l'homme à l'heure d'Internet,* Bruyant, 2019.

Délimitations - L'étude se concentre sur les violences qui ont lieu dans le cyberespace. Nous allons nous intéresser aux comportements illicites et, en particulier de contenu, qui ont lieu sur les médias et réseaux sociaux, les sites web et les moteurs de recherche. Il s'agit de s'interroger sur la nature et les caractéristiques de ces comportements illicites et, notamment, de comprendre si les violences en ligne ont un « objet cyber » qui les caractérise ou s'il s'agit simplement de violences « traditionnelles » qui s'amplifient sur Internet.

23. 1/ Premièrement, il importe de comprendre la caractérisation des cyberviolences. Afin d'analyser au mieux les comportements illicites en ligne, il semblerait nécessaire de distinguer deux catégories de comportements illicites.

D'une part, il y a les formes d'infractions « traditionnelles » qui existent même sans l'intermédiaire des nouvelles technologies. De l'autre, il y a les infractions qui sont spécifiques à Internet et qui n'ont pas lieu hors du contexte de l'informatique. Ces dernières ont comme objet principal l'ordinateur et les systèmes informatiques. Dans ce contexte, ces infractions se manifestent notamment par l'accès frauduleux à un ou plusieurs systèmes informatiques, par l'atteinte à l'intégrité des données, les attaques par déni de service, le piratage de logiciels ou les intrusions non autorisées dans les systèmes informatiques des tiers. Dans la première catégorie, l'ordinateur, Internet et les systèmes informatiques sont utilisés comme simple moyen et non plus comme cible. Cela veut dire que les formes d'infractions sont très variées, par exemple, le vol, la fraude, l'usurpation d'identité, la contrefaçon mais aussi la diffusion de contenus illégaux, l'incitation à la haine, la diffamation ou l'apologie du terrorisme. La distinction objet/moyen amène à la distinction entre les « anciens crimes » qui sont perpétrés au moyen de l'ordinateur et les « nouveaux crimes »[91] qui ont comme objet l'ordinateur et qui « ne disposent d'aucun équivalent non informatique »[92]. Il est évident que ces dernières formes d'infractions existent depuis toujours et qu'il n'est pas indispensable d'avoir un ordinateur pour les commettre. Toutefois ces dernières trouvent une

[91] P-E LAVOIE, F. FORTIN et S. TANGUAY, « Problèmes relatifs à la définition et à la mesure de la cybercriminalité » in F. FORTIN (dir.) *Cybercriminalité, entre inconduite et crime organisé,* Presses Internationales Polytechniques Polytechnique et Sûreté du Québec, 2013.
[92] *Ibid*. p. 12.

amplification importante à travers l'utilisation d'appareils de communication et d'information.

24. 2/ Secondement, il est intéressant d'étudier les limites de l'encadrement juridique des cyberviolences, non seulement, au regard de la qualification mais également du régime appliqué. Il est nécessaire d'approfondir la question de la prévention et de la sanction pour comprendre si le pluralisme causé par l'absence d'unité des mesures encadrant les définitions et les sanctions nuisent à la protection des droits fondamentaux des utilisateurs.

25. Dans nos travaux, nous allons analyser les comportements illicites qui portent atteinte aux droits fondamentaux des personnes physiques. En effet, nous n'allons pas analyser les atteintes portées aux personnes morales. Nous nous concentrerons sur les atteintes aux droits des personnes privées portées par d'autres particuliers, par les pouvoirs publics, les États ainsi que les plateformes en ligne. Nous nous intéresserons, entre autres, aux cas de manquement des États à la protection des particuliers quand ces derniers n'ont pas été protégés des violations de leurs droits causés par d'autres particuliers ou par les plateformes. Pour cela, la question de la responsabilité sera traitée du point de vue des individus, des États ainsi que des plateformes en ligne qui ont un véritable rôle à jouer dans la prévention et la sanction. Il s'agira également de traiter la question de la modération qui est au cœur des problèmes liés à la diffusion des contenus illicites et des atteintes aux droits fondamentaux des utilisateurs.

26. Nous étudierons principalement l'encadrement juridique en droit de l'Union européenne et en droit international, ainsi que le droit national des États membres de l'Union européenne et du Conseil de l'Europe. Nous avons fait ce choix pour délimiter *a minima* nos recherches au vu de la difficulté de comparer les législations nationales et la jurisprudence. Cependant, d'autres États non membre du Conseil de l'Europe, comme les États-Unis, seront également étudiés. Ensuite, nous donnerons une importance particulière à l'analyse de la jurisprudence, notamment celle de la Cour européenne des droits de l'Homme et de la Cour de justice de l'Union européenne. Cette analyse nous permettra non seulement de comprendre la mise en œuvre des dispositions législatives, mais également l'évolution de l'interprétation des juges en la matière.

27. **La problématique retenue –** Ces réflexions nous amènent à nous poser la question de savoir si l'encadrement juridique des cyberviolences actuel est satisfaisant et s'il doit s'adapter ou pas à leurs nouvelles caractéristiques et au nouveau contexte numérique.

28. **Annonce de plan -** Dans la première partie de notre étude, nous allons étudier la caractérisation et la qualification des cyberviolences dans le droit matériel de l'Union européenne et en droit international. La recherche porte également sur la jurisprudence européenne et internationale, ainsi que sur la doctrine. Nous aurons recours également au droit comparé, tout d'abord aux législations nationales des États membres de l'Union européenne, ensuite, à celles des États non membres, en particulier les membres du Conseil de l'Europe. Le choix des États étudiés a été fait avec l'objectif d'analyser les législations nationales plus avancées ou plus en retard en termes de qualification, prévention et sanction des cyberviolences, ainsi que par rapport à la jurisprudence identifiée. En effet, cette dernière nous permet d'appréhender l'approche adoptée par les juridictions nationales à ce sujet.

Dans la seconde partie, il s'agira d'analyser le régime juridique adopté pour régir ces comportements illicites en ligne à travers les sources précédemment citées. À cet égard, nous étudions les mesures de prévention et de sanction prévues par les États et par les institutions européennes. Ainsi, nous analyserons également les solutions et les recommandations des acteurs de la société civile et les mesures adoptées par les entreprises privés, en particulier les plateformes.

Il convient dès lors d'aborder cette étude à travers un plan en deux parties. D'abord, il s'agit d'analyser la difficile caractérisation des cyberviolences **(Partie I)** et, ensuite, d'étudier leur régime juridique fragmentaire **(Partie II)**.

PARTIE I : LA DIFFICILE CARACTERISATION JURIDIQUE DES CYBERVIOLENCES

29. Étudier le phénomène des cyberviolences nous mène d'abord à nous intéresser à leurs caractéristiques. Comme expliqué dans les développements précédents, les caractéristiques des cyberviolences sont dues à la dimension cyber qui garantit une large diffusion des contenus, 7 jours sur 7 et 24h sur 24h, avec le danger omniprésent de perdre leur maîtrise et d'une diffusion massive sur plusieurs réseaux à la fois. Internet et les plateformes permettent également d'atteindre une multiplicité de cibles dans le monde entier et de façon anonyme. Tous ces éléments et bien d'autres montrent que ce phénomène est spécifique aux nouvelles technologies et que, même si certains comportements hors ligne sont reproduits en ligne, leurs conséquences nuisibles sont amplifiées.

30. Toutefois, alors que l'émergence des violences en ligne existe depuis l'apparition d'Internet, il n'existe pas encore une définition universellement acceptée ce de phénomène et de ses manifestations. Cette situation nous mène non seulement à analyser les conséquences de ce manquement mais aussi à proposer des solutions pour améliorer leur qualification juridique, ce qui aura des conséquences sur la prévention de ces comportements, la sanction des auteurs des cyberviolences et la prise en charge des victimes.

31. Au vu de ces éléments, il s'agira d'analyser les spécificités des cyberviolences (**Titre I)** pour ensuite étudier la nécessité d'une qualification universelle (**Titre II**).

TITRE I : LES SPECIFICITES DES CYBERVIOLENCES

32. L'utilisation de systèmes informatiques est le fondement du phénomène des violences en ligne. Sans la sphère "cyber", elles n'existeraient tout simplement pas. Les violences en ligne ont des caractéristiques propres qui les distinguent des violences hors ligne. Leur exécution est facilitée par les qualités techniques d'Internet mais aussi par la dimension transnationale d'Internet qui complexifie le traitement des comportements illicites. De plus, les évolutions d'Internet et des réseaux sociaux en ont fait un outil où les atteintes à la vie privée des utilisateurs et leurs droits fondamentaux sont de plus en plus facilitées. Les caractéristiques d'Internet facilitent également la viralité et par conséquent l'amplification des comportements illicites. Cette amplification se manifeste par l'atteinte aux droits fondamentaux des utilisateurs à une plus grande échelle de celle qui pourrait se matérialiser hors ligne.

Au vu de ces éléments, il s'agira d'analyser les caractéristiques d'Internet facilitant l'exécution des cyberviolences (**Chapitre I**) et leurs amplification (**Chapitre II**).

Chapitre I : La reconnaissance des caractéristiques d'Internet, facilitatrices de l'exécution des cyberviolences

35. Nous allons nous intéresser à certaines caractéristiques d'Internet et en particulier à sa dimension globale qui facilite l'exécution des cyberviolences. En effet, ses qualités techniques qui permettent une diffusion très large de l'information, à la différence des médias dits « traditionnels » (la presse, la radio ou la télévision) permettent l'exécution des comportements illicites à une large échelle. Cette capacité d'ubiquité a été reconnue à plusieurs reprises par les Cours européennes, ce qui est fondamental pour appréhender les caractéristiques d'Internet afin de protéger efficacement les droits fondamentaux sur Internet. Ainsi, Internet est caractérisé par une grande capacité de stockage d'informations, ce qui permet de garantir une facilité d'accès à l'information et à la communication mais également la liberté d'expression de la presse et des individus. Cependant, cela peut conduire à des atteintes aux droits fondamentaux, en particulier à la vie privée et aux données personnelles, en effet, des informations personnelles peuvent être publiées et référencées sur les moteurs de recherche. Pour mitiger ces atteintes, un droit à l'oubli a été consacré mais il reste un droit relatif et à géométries variables. En outre, cette dimension globale est également due à la composante transnationale du cyberespace qui se répercute ensuite sur les cyberviolences, car les contenus illicites peuvent se propager dans plusieurs États en même temps. En effet, le contenu peut, par exemple, être partagé dans un État et avoir ses conséquences dans un autre. Cet aspect facilite l'exécution des cyberviolences car des agresseurs peuvent prendre avantage de cette situation et publier un contenu licite dans un État donné dont les conséquences sont illicites dans un autre État. Par conséquent, la dimension transnationale peut rendre difficile l'établissement de la compétence juridictionnelle et le traitement des contenus.

33. De plus, d'autres caractéristiques d'Internet facilitent les atteintes aux droits fondamentaux, notamment la possibilité donnée par Internet et les réseaux sociaux d'exposer la vie privée des individus de façon volontaire ou involontaire. En effet, la conception des plateformes de réseaux sociaux est, en partie, fondée sur le partage des moments de vie et des informations personnelles. Ainsi, une fois connectés les utilisateurs s'exposent à recevoir ou voir des contenus illicites et, par conséquent, ils ne jouissent plus d'une protection effective de leur droit à la vie privée. Cette situation se présente malgré l'évolution du droit

à la vie privée aux nouveaux risques liés aux nouvelles technologies de la communication et de l'information.

34. Enfin, Internet offre également la possibilité d'être anonymes. Que cela soit un anonymat ressenti ou effectif, cette possibilité assure un sentiment d'impunité. Toutefois, la dangerosité du droit à l'anonymat doit être nuancée car, si d'un côté il facilite l'exécution des contenus illicites, de l'autre, il permet la protection de droits fondamentaux comme le droit à la vie privée ou la liberté d'expression.

35. Dans les développements qui vont suivre, il s'agira d'analyser la dangerosité d'Internet au vu de sa dimension globale (**Section I**) et les atteintes potentielles aux droits fondamentaux auxquelles sont exposés les utilisateurs au moyen d'Internet (**Section II**).

Section I : La dangerosité d'Internet au vu de sa dimension globale

36. Avant d'analyser les spécificités des cyberviolences, il est essentiel d'analyser le lieu où ces dernières s'exercent et s'amplifient, c'est-à-dire Internet. Dans cette section, nous analyserons le cyberespace en tant que lieu unique assurant des droits aux individus, comme le droit d'accès à l'information ou le droit à la liberté d'expression et, en même temps, en tant que lieu où les atteintes aux droits fondamentaux sont multiples. Cela se manifeste notamment à cause de ses spécificités, reconnues notamment par la jurisprudence des cours européennes. En effet, à la différence des médias traditionnels, les cyberviolences sont facilitées par les qualités techniques d'Internet (**§I**) et leur traitement est fragilisé par la dimension transnationale de ce dernier (**§II**).

I. L'exécution des cyberviolences facilitée par les qualités techniques d'Internet

37. Les atteintes aux droits fondamentaux sont fortes à cause de certaines caractéristiques d'Internet. Nous analyserons ces dernières à travers l'œil de la jurisprudence des cours européennes qui met en avant, entre autres, l'instantanéité, la facilité et l'étendue de la diffusion des contenus (**A**), ensuite, nous étudierons plus en détail les risques et les dangers liés à la possibilité de stocker un grand nombre d'informations (**B**).

A. Les risques d'Internet selon les cours européennes

38. Internet est un moyen d'émancipation, de liberté d'expression et d'information mais, en même temps, comme l'expose la Cour européenne des droits de l'Homme, « les avantages de ce média s'accompagnent d'un certain nombre de risques [car des] propos clairement illicites, notamment des propos diffamatoires, haineux ou appelant à la violence, peuvent être diffusés comme jamais auparavant dans le monde entier, en quelques secondes, et parfois demeurer en ligne pendant fort longtemps »[93].

39. Pour appréhender les caractéristiques d'Internet, les cours européennes ont souvent fait une comparaison avec les médias dits traditionnels, comme la presse, la radio ou la télévision. Cette analyse a porté à des décisions souvent différentes les unes avec les autres et portant à une appréciation hétérogène entre Internet et les médias traditionnels. D'abord, à travers l'*arrêt Vérités Santé Pratique Sarl c France*[94] la Cour européenne des droits de l'Homme a reconnu l'équivalence entre Internet et un média traditionnel afin de diffuser une information. Le cas d'espèce concernait une saisine en violation de l'article 10 de la Convention européenne des droits de l'Homme, relatif à la liberté d'expression, car la requérante s'était vue refuser le renouvellement aux registres de la

[93] Cour EDH (GC), 16 juin 2015, *Delfi AS c. Estonie*, req. n° 64669/09 § 110, voir S. TURGIS, « Les droits de l'homme à l'heure d'Internet et du numérique : rupture ou continuité ? », in C. DE TERWANGNE et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 108.
[94] Cour EDH, 1er décembre 2005, *Vérités Santé Pratique Sarl c France*, req. n° 74766/01.

commission paritaire des publications et agences de presse (CPPAP) qui lui permettait de bénéficier d'un régime économique spécifique à la presse comprenant des tarifs postaux préférentiels et des allègements fiscaux. Or, la Cour, pour motiver sa décision, avait retenu un point soulevé par le Gouvernement défendeur qui mentionnait que les activités de la revue avaient pu être poursuivie sur Internet[95]. La Cour reconnaît donc la possibilité dont la requérante disposait de poursuivre ses publications par d'autres moyens, notamment Internet, ce qui a atténué l'ingérence à son droit à la liberté d'expression[96]. La Cour a ensuite établi, par son arrêt *Fatullayev c. Azerbaïdjan*[97], que la diffusion des contenus sur Internet n'est pas moins puissante que lorsqu'ils sont diffusés par voie de presse. En effet, elle s'exprimait ainsi concernant la publication sur un forum d'Internet : « a medium which in modern times has no less powerful an effect than the print media »[98].

40. Ensuite, en 2011 la Cour commence à se détacher de cette équivalence et fait une distinction entre Internet et les autres médias, en particulier pour surligner les caractéristiques spécifiques de ce dernier. À cet égard, dans l'arrêt *Pravoye Delo* la Cour estime que « […] Internet est […] un outil d'information et de communication qui se distingue particulièrement de la presse écrite, notamment quant à sa capacité à emmagasiner et diffuser l'information »[99]. Ainsi, cette distinction entre Internet et les médias traditionnels est constatée non seulement dans l'étendue de la diffusion des contenus, mais également dans les effets beaucoup plus immédiats et puissants d'Internet par rapport aux médias traditionnels, en particulier vis-à-vis des atteintes potentielles aux droits des utilisateurs. La Cour s'exprime dans ce sens à plusieurs reprises. Elle estime

---

[95] Cour EDH, 1er décembre 2005, *Vérités Santé Pratique Sarl c France*, req. n° 74766/01, point 3.
[96] Voir S. TURGIS, « La coexistence d'Internet et des médias traditionnels sous l'angle de la Convention européenne des droits de l'homme », *RTDH* 2013, nr. 93, p. 23.
[97] Cour EDH, 22 avril 2010, *Fatullayev c. Azerbaïdjan*, req. n° 40984/07.
[98] Cour EDH, 22 avril 2010, *Fatullayev c. Azerbaïdjan*, req. n° 40984/07, §95. Traduction par l'autrice « un média qui, à l'époque moderne, n'a pas moins d'impact que la presse écrite ». La Cour avait tenu le même raisonnement dans la comparaison entre les médias audiovisuels et la presse en estimant que les médias audiovisuels ont des effets beaucoup plus immédiats et puissants que la presse écrite, voir notamment Cour EDH, 23 septembre 1994, *Jersild c. Danemark*, req. n° 15890/89,§31, Cour EDH, 10 juillet 2003, *Murphy c. Irlande*, req ° 44179/98, §69, ainsi que Cour EDH, 11 décembre 2008, *TV Vest AS & Rogaland Pensjonistparti c. Norvège*, req° n° 21132/05, §60,
[99] Cour EDH, 5 mai 2011, *Pravoye Delo*, req n°33014/05, § 63, dans ce sens voir également Cour EDH, 16 octobre 2013, *Węgrzynowski et Smolczewski c. Pologne*, req. n° 33846/07, § 58.

que « […] les communications en ligne et leur contenu risquent bien plus que la presse de porter atteinte à l'exercice et à la jouissance des droits et libertés fondamentaux, en particulier du droit au respect de la vie privée »[100]. De plus, elle ajoute également que « the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press »[101].

41. Toutefois, en 2013, dans une autre affaire, la Cour s'exprime différemment. En effet, elle estime que « rien ne montre qu'Internet et les réseaux sociaux aient bénéficié […] d'un transfert de l'influence des médias de télédiffusion suffisamment important pour qu'il devienne moins nécessaire d'appliquer à ces derniers des mesures spéciales »[102]. La position du juge Sajó va dans le même sens, en effet, dans son opinion dissidente à l'affaire *Féret*[103] il estime que « les sites web se distinguent d'autres formes de distribution parce qu'on peut les « télécharger » à son gré (les intéressés doivent rechercher eux-mêmes activement l'information). Autrement dit, les opinions ne sont pas « imposées » comme elles le sont lors de la divulgation de documents papier »[104]. Il précise également qu'il n'y a pas « […] besoin de préciser que l'impact de la radio et de la télévision sur une action coordonnée est différent de celui de tracts disparates et de sites web »[105]. Il ressort de son analyse qu'Internet est moins dangereux que les médias traditionnels, au contraire de ce que la Cour a établi dans l'affaire *Féret* où elle tend à faire d'Internet une circonstance aggravante[106]. Cette approche rappelle d'ailleurs celle

---

[100] Cour EDH, 5 mai 2011, *Pravoye Delo*, req n°33014/05, § 63.
[101] Cour EDH, 16 octobre 2013, *Węgrzynowski et Smolczewski c. Pologne*, req. n° 33846/07, § 58. Traduction de l'autrice : « le risque de préjudice que représentent les contenus et les communications sur Internet pour l'exercice et la jouissance des droits et libertés de l'homme, notamment le droit au respect de la vie privée, est certainement plus élevé que celui que représente la presse ». Dans le même sens, voir Cour EDH., 16 juin 2015, *Delfi AS c. Estonie*, req. n° 64669/09, § 147 où la Cour estime que « la facilité, l'ampleur et la vitesse avec lesquelles les informations sont diffusées sur Internet, et leur caractère persistant après leur publication sur ce média, toutes choses qui peuvent considérablement aggraver les effets des propos illicites circulant sur Internet par rapport à ceux diffusés dans les médias classiques ».
[102] Cour EDH, GC, 22 avril 2013, *Animal Defenders International c. Royaume-Uni*, 48876/08, § 119.
[103] Cour EDH, 16 juillet 2009, *Féret c. Belgique*, req. n° 15615/07.
[104] Opinion dissidente dans l'affaire *Féret* du jugé Sajó à laquelle déclarent se rallier les juges Vladimiro Zagrebelsky et Nona Tsotsoria, p. 27.
[105] *Ibid.* p. 29. Opinion dissidente dans l'affaire *Féret* du jugé Sajó à laquelle déclarent se rallier les juges Vladimiro Zagrebelsky et Nona Tsotsoria, p. 29.
[106] F. TRÉGUER, « Internet dans la jurisprudence de la Cour européenne des Droits de l'Homme », *RDLF*, chron. n°13, 2013, pp. 11-12.

de la Cour Suprême des États-Unis dans les années '90, en particulier l'arrêt *Reno c. ACLU,* où la Cour considère qu'Internet n'a pas le même caractère « invasif » que la radio ou la télévision[107].

42. Enfin, un paradoxe se présente à la lecture de l'arrêt de la Cour européenne des droits de l'Homme, *Mouvement raëlien suisse c. Suisse*[108]. Dans cet arrêt, la Cour établit la non violation de l'article 10 de la Convention européenne des droits de l'Homme concernant l'interdiction d'affiches dans l'espace public du mouvement raëlien au vu de l'existence de moyens alternatifs de diffusion, notamment Internet. Toutefois, le contenu du site Internet du mouvement avait été à la base des justifications qui avaient portées à l'interdiction de la campagne d'affichage[109], ce qui rend la décision assez ambigüe.

43. Concernant l'approche adoptée par la Cour de justice de l'Union européenne, cette dernière ne s'est pas exprimée très souvent, elle clarifie toutefois la différence entre Internet et les médias traditionnels dans son arrêt *eDate Advertising Gmbh c. X* où elle considère que « la mise en ligne de contenus sur un site Internet se distingue de la diffusion territorialisée d'un média tel un imprimé en ce qu'elle vise, dans son principe, à l'ubiquité desdits contenus. Ceux-ci peuvent être consultés instantanément par un nombre indéfini d'internautes partout dans le monde, indépendamment de toute intention de leur émetteur visant à leur consultation au-delà de son État membre d'établissement et en dehors de son contrôle » [110]. De ce fait, selon la Cour « […] la portée de la diffusion de contenus mis en ligne est en principe universelle »[111]. La Cour montre donc l'étendue

---

[107] Cour Suprême des États-Unis, *Reno v. American Civil Liberties Union*, 521 U.S. 844, 1997.
[108] Cour EDH, GC, *Mouvement raëlien suisse c. Suisse*, 13 juillet 2012, req. n° 16354/06.
[109] Ce paradoxe était exprimé par l'opinion dissidente commune sous l'arret Cour EDH, GC, *Mouvement raëlien suisse c. Suisse* aux des juges Tulkens, Sajó, Lazarova Trajkovska, Bianku, Power-Forde, Vučinić et Yudkivska qui s'exprimaient ainsi : « Interdire à la requérante une campagne d'affichage en raison principalement du contenu de son site Internet tout en soutenant que la portée d'une telle interdiction reste limitée en raison du fait que l'intéressée demeure libre de communiquer via ce même site Internet est singulier, sinon paradoxal », §9. Voir également S. TURGIS, *Les droits de l'homme à l'heure d'Internet et du numérique : rupture ou continuité ?*, in C. DE TERWANGNE et Q. VAN ENIS (dir.), L'Europe des droits de l'homme à l'heure d'Internet, 1e édition, Bruxelles, Bruylant, 2019, p. 110-111.
[110] CJUE, (GC), *eDate Advertising Gmbh c. X*, 25 octobre 2011, affaires jointes C-509/09 et C-161/10, § 45.
[111] *Ibid § 46.*

de la puissance d'Internet et donne un aperçu de ses spécificités.

44. Malgré certaines contradictions de la Cour européenne des droits de l'Homme, il semblerait que les cours européennes reconnaissent des spécificités à Internet notamment vis-à-vis des médias traditionnels et que l'unicité attribuée à Internet puisse représenter un danger pour la protection de certains droits fondamentaux. Les effets d'Internet sont beaucoup plus importants dans la diffusion de l'information mais également dans le stockage, car les contenus peuvent rester en ligne très longtemps et certains pour toujours avec une grande difficulté pour les utilisateurs à les faire effacer. Il est donc important de parler des archives en ligne et du droit à l'oubli.

B. Internet, lieu d'archivage et d'oubli relatif

45. Une fois publiés sur Internet, les contenus, que cela soit une image, une vidéo ou un écrit, s'engouffrent dans les méandres du cyberespace. Il ne sera pas chose facile de les faire retirer ou déréférencer par les moteurs de recherche.

46. C'est dans cette ubiquité et dans la mémoire sans fond d'Internet qu'il faut trouver un part de sa richesse mais également une part de sa dangerosité. En effet, d'un côté, Internet contribue à améliorer l'accès du public à l'actualité et à faciliter la communication de l'information. Il permet la constitution d'archives qui « [représentent] un aspect essentiel du rôle joué par les sites Internet »[112] et leur création et mise à disposition assurent une facilité d'accès à l'information. La Cour européenne des droits de l'Homme précise également que les archives « constituent une source précieuse pour l'enseignement et les recherches historiques, notamment en ce qu'elles sont immédiatement accessibles au public et généralement gratuites »[113]. De l'autre, Internet peut représenter une atteinte aux droits et libertés, notamment le droit à la vie privée et aux données personnelles. En effet, comme mentionné précédemment la diffusion des contenus sur Internet permet de

[112] Cour EDH, 10 mars 2009, *Times Newspapers Limites (nos 1 et 2) c. Royaume Uni*, req. n°s 3002/03 et 23676/03, §27.
[113] *Ibid. § 45.* Cour EDH, 10 mars 2009, *Times Newspapers Limites (nos 1 et 2) c. Royaume Uni*, req. n°s 3002/03 et 23676/03, §45.

toucher un large nombre de personnes. Et, les contenus partagés peuvent rester en ligne beaucoup de temps, même indéfiniment. Il est donc important de s'intéresser au droit à l'oubli pour comprendre les spécificités d'Internet et le danger qu'il représente pour certains droits fondamentaux. En effet, si un droit à l'oubli numérique existe, il s'agit d'un droit relatif qui ne rime pas avec droit à l'effacement (**1**) et qui fait l'objet d'une application à géométries variables[114] (**2**).

1. Le droit à l'oubli ne rimant pas avec l'effacement des contenus en ligne

47. C'est par l'arrêt *Google Spain et Google Inc c/Agencia Española de Protección de Datos* (ci-après *Google Spain)* [115] de la Cour de justice de l'Union européenne que le « droit à l'oubli » a été consacré pour la première fois[116] en Europe sous le fondement de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette dernière a été abrogée et remplacée par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, plus généralement appelé règlement général sur la protection des données (RGPD)[117]. C'est, en effet, par l'article 17 de ce dernier que les conditions d'exercice de ce droit, les motifs qui mènent au déréférencement ainsi que leurs limites ont été fixés[118].

[114] Voir notamment S. TURGIS, « La conciliation d'un droit à l'oubli avec les droits fondamentaux consacrés par la CEDH », colloque *Le droit à l'oubli numérique, enjeux et perspectives*, organisé par l'Institut de l'Ouest : Droit et Europe (IODE) le 6 mars 2015. Conférence disponible sur YouTube https://www.youtube.com/playlist?list=PLVDuo6AGUn6xv4FK_wyeLaNtPhsmLiqgK
[115] CJUE, GC, 13 mai 2014, *Google Spain et Google Inc c/AEPD*, aff. C 131/12.
[116] *Ibid.* point 88 et suivants. CJUE, GC, 13 mai 2014, *arrêt Google Spain et Google Inc c/AEPD*, aff. C 131/12, point 88 et suivants. À la suite de cet arrêt, Google et d'autres moteurs de recherche ont mis en place rapidement un formulaire de suppression d'informations personnelles, voir par exemple : https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&hl=fr&rd=1
[117] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[118] Article 17 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

48. Dans l'affaire *Google Spain,* la Cour de justice de l'Union européenne avait été appelée à répondre à une question préjudicielle pour une affaire qui concernait la désindexation d'informations accessibles sur le moteur de recherche Google d'un homme d'affaires qui avait fait l'objet d'une saisie en recouvrement de dettes. La Cour, pour répondre à l'une des trois questions posées par le tribunal espagnol, fait une lecture combinée des articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46/CE, désormais abrogée, en estimant que « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite »[119]. La Cour donne donc des détails sur le droit à l'oubli sans en donner une vraie définition. À cet égard, il est intéressant de voir que la Commission nationale de l'informatique et des libertés (ci-après « CNIL ») le définit comme « la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie privée – comme publique – en ligne » [120]. La CNIL précise que « ce droit ne doit, cependant, pas être interprété comme un impératif absolu d'effacement des données et informations »[121]. Ce terme « droit à l'oubli », selon les conclusions du rapporteur public Alexandre Lallet sur l'ensemble des affaires jugées le 6 décembre 2019[122] par le Conseil d'État, serait impropre « car les pages web auxquels renvoient ces liens existent toujours ». Pour être recevables, les demandes de désindexation doivent être présentées par un individu ayant la nationalité de l'un des États membres de l'Union européenne et ce dernier, doit agir au nom d'un particulier (par exemple soi-même, un client, un membre de la famille ou un ami). Ainsi,

---

[119] *Ibid.* point 88. CJUE, GC, 13 mai 2014, *arrêt Google Spain et Google Inc c/AEPD*, aff. C 131/12, point 88
[120] CNIL, *Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*, Rapport d'activité 2013, p. 16.
Voir : https://www.cnil.fr/sites/default/files/typo/document/CNIL_34e_Rapport_annuel_2013.pdf consulté le 27 juillet 2021.
[121] *Ibid.* CNIL, *Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*, Rapport d'activité 2013, p. 16.
Voir : https://www.cnil.fr/sites/default/files/typo/document/CNIL_34e_Rapport_annuel_2013.pdf consulté le 27 juillet 2021.
[122] Conseil d'État, Droit à l'oubli : le Conseil d'État donne le mode d'emploi, 6 décembre 2019.
Disponible sur : https://www.conseil-etat.fr/actualites/actualites/droit-a-l-oubli-le-conseil-d-etat-donne-le-mode-d-emploi

les données qu'il souhaite faire déréférencer doivent respecter certains critères établis par le moteur de recherche. À cet égard, en France, après l'arrêt *Google Spain* la CNIL a publié treize critères types qui justifient une demande de désindexation[123]. Enfin, si le moteur de recherche ou la plateforme sollicitée ne donne pas une réponse sous un mois, les demandeurs peuvent saisir l'autorité de régulation.

49. Au vu de ces éléments, il faut souligner que ce droit à l'oubli s'exerce à travers un droit au déréférencement, c'est-à-dire à travers la désindexation de toute information personnelle, telle que le nom ou le prénom, visibles sur des moteurs de recherche comme Google ou Yahoo notamment. Il ne s'agit donc pas d'un droit à l'effacement. En effet, les informations resteront en ligne et pourront être retrouvées par une recherche moyennement de mots clés autres que le patronyme de la personne[124]. Ces éléments montrent les limites de ce droit vis-à-vis de la nature et des effets de la demande de déréférencement.

50. On constate également des limites quant à sa portée spatiale. En effet, par l'arrêt *Google LLC c/ CNIL* du 24 septembre 2019[125], la Grande Chambre de la Cour de justice de l'Union européenne a été appelé à déterminer si Google, après une demande de suppression de liens menant vers des pages web, devait procéder à l'effacement de ces liens sur toutes les extensions de nom de domaine[126] de son moteur de recherche ou bien si le RGPD prévoyait une portée plus restreinte. La Cour de justice de l'Union européenne a estimé que l'exploitant d'un moteur de recherche n'est pas dans l'obligation de procéder à un déréférencement mondial[127]. Cette décision pourrait s'expliquer au vu des différentes approches de pays, notamment les États hors l'Union européenne comme les États-Unis, où le droit au déréférencement n'est pas consacré.

---

[123] CNIL, Droit au déréférencement, Les critères communs utilisés pour l'examen des plaintes, 2014. Disponible sur : https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf
[124] À cet égard selon les conclusions du rapporteur public A. LALLET « le « droit au déréférencement » [est une] expression qui reste trompeuse dans la mesure où ces contenus continuent bel et bien à être référencés par le moteur de recherche par le biais de mots-clés autres que le patronyme de la personne », voir : Conseil d'État, Droit à l'oubli : le Conseil d'État donne le mode d'emploi, 6 décembre 2019. Disponible sur : https://www.conseil-etat.fr/actualites/actualites/droit-a-l-oubli-le-conseil-d-etat-donne-le-mode-d-emploi
[125] CJUE, GC, 24 septembre 2019, *Google LLC c/ CNIL*, aff. C-507/17.
[126] C'est-à-dire le suffixe situé à droit du nom de domaine par exemple l'extension française est « .fr », allemande « .de » ou encore celle des États-Unis « .us ».
[127] CJUE, GC, 24 septembre 2019, *Google LLC c/ CNIL*, aff. C-507/17, point 64.

Une autre motivation pourrait se trouver dans l'appréciation entre la protection du droit à la vie privée et les autres droits et libertés concurrentes qui n'est pas la même qu'au sein de l'Union européenne. Cependant, la Cour précise que « si […] le droit de l'Union n'impose pas, en l'état actuel, que le déréférencement auquel il serait fait droit porte sur l'ensemble des versions du moteur de recherche en cause, *il ne l'interdit pas non plus* »[128]. En effet, sous le fondement des standards nationaux de protection des droits fondamentaux la Cour prévoit que les autorités nationales des États membres peuvent enjoindre à l'exploitant de procéder au déréférencement dans l'ensemble des extensions. Cela signifie donc, en principe, que la portée géographique du droit au déréférencement pourrait s'étendre à l'ensemble des extensions des pays de l'Union européenne. En principe, l'étendu à l'ensemble des États membres semble garantir à minima un droit au déréférencement pour les ressortissants de l'Union européenne, toutefois cette protection reste limitée vis-à-vis des contenus partagés dans des extensions dans des pays tiers.

51. Le droit à l'oubli est donc à considérer comme un droit relatif, car il s'agit d'un déréférencement qui ne permet pas l'effacement des informations ; ainsi que dans sa portée géographique. Il faut ensuite ajouter que ce droit s'applique à géométries variables ce qui peut affaiblir son effectivité.

2. Un droit à l'oubli à géométries variables

52. Le droit à l'oubli est l'expression du principe de l'auto-détermination informationnelle, c'est-à-dire la possibilité pour chaque individu de décider de la communication et de l'emploi des informations le concernant. Au sein de l'Union européenne, l'article 17 du RGPD précise la mise en œuvre de ce droit. En ce sens il pose, d'un côté, les principes du droit à l'effacement (paragraphes 1 et 2) et de l'autre ses limites (paragraphe 3).

53. D'abord, le paragraphe 1 prévoit que chaque individu a le droit d'obtenir de la part du responsable du traitement l'effacement des données le concernant dans les meilleurs délais, par exemple, lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées[129] ou si elles ont fait l'objet d'un

[128] *Ibid.* point 72.
[129] Article 17, paragraphe 1 (a), du règlement général sur la protection des données.

traitement illicite[130]. Ensuite, le paragraphe 2 prévoit également que le responsable du traitement, lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, doit prendre des mesures raisonnables pour informer le responsable du traitement qui a traité les données que la personne a demandé l'effacement.

54. Enfin, certaines conditions concernant le traitement des informations publiées peuvent s'opposer à l'application des paragraphes 1 et 2, limitant de fait la portée du droit à l'oubli. En effet, le paragraphe 3 prévoit que ces derniers ne s'appliquent pas si, par exemple, le traitement des données est nécessaire à l'exercice du droit à la liberté d'expression et d'information[131] ou pour des motifs d'intérêt public dans le domaine de la santé publique[132].

55. Après ces rappels juridiques quant à son encadrement, il est important d'analyser ce qui ressort de la jurisprudence. En effet, se dégage de la jurisprudence une diversité d'approches et de mises en œuvre de ce droit. Tout contenu n'est pas déréférencé, car des droits et libertés concurrents peuvent être mis en balance, notamment la liberté d'expression et la protection de la liberté d'information et de presse.

56. Les cours nationales ainsi que les cours européennes ont pu, à plusieurs reprises, s'exprimer à cet égard et dégager des critères, conformes à l'article 17 du RGPD, pour considérer si le contenu pourrait ou pas être désindexé. Ces critères concernent notamment le contenu de la publication, en particulier, si cette dernière a un intérêt public, ainsi que la qualité de l'individu qui est à l'origine de la demande, par exemple s'il s'agit d'une personnalité médiatique, politique ou un mineur. Dans les développements qui vont suivre nous allons étudier les différentes appréciations.

57. D'abord, la Cour européenne des droits de l'Homme avait établi par sa jurisprudence[133] certains critères dans le contexte de la mise en balance de droits tels que le droit à la vie

[130] Article 17, paragraphe 1 (d), du règlement général sur la protection des données.
[131] Article 17, paragraphe 1 (a), du règlement général sur la protection des données.
[132] Article 17, paragraphe 1 (c), du règlement général sur la protection des données.
[133] Voir Cour EDH, 7 février 2012, *Von Hannover c. Allemagne* n° 2, req. n° 40660/08 60641/08 , §§ 109-113, voir aussi Cour EDH, GC, 7 février 2012, *Axel Springer AG c. Allemagne*, req. n° 39954/08, §§ 89-95 et Cour EDH, GC, 10 novembre 2015, *Couderc et Hachette Filipacchi Associés c. France*, req. n° 40454/07, §93.

privée et le droit à la liberté d'expression. Elle énumère notamment : la contribution à un débat d'intérêt général, la notoriété de la personne visée et l'objet du reportage, le comportement antérieur de la personne concernée, le mode d'obtention des informations et leur véracité, le contenu, la forme et les répercussions de la publication ainsi que la gravité de la sanction imposée aux journalistes ou aux éditeurs. La Cour a ensuite appliqué ces critères dans l'affaire *Fuchsmann c. Allemagne* en 2017[134], en effet elle avait été saisie par un homme d'affaires allemand qui demandait la désindexation d'un article du New York Times (site internet et format papier) qui le décrivait comme un escroc. La Cour considère que les juridictions allemandes avaient ménagé un juste équilibre entre les parties. En effet, elle estime que les informations partagées par le journal reposaient sur une base factuelle suffisante. Selon elle, en étant le demandeur un homme d'affaire bénéficiant d'une certaine notoriété, il pouvait être assimilé à une personnalité publique[135], de plus les informations partagées présentaient un intérêt public. Enfin, la Cour constate que le demandeur avait été informé par la presse de la publication de l'article, pour cela l'auteur de l'article avait respecté ses obligations et responsabilités journalistiques. Par cet arrêt, la Cour européenne des droits de l'Homme relativise la mise en œuvre du droit à l'oubli et confirme sa volonté de protéger les archives sur Internet comme elle l'avait fait avec son arrêt *Węgrzynowski et Smolczewski c. Pologne*[136] et précédemment dans l'arrêt *Times Newspapers Limites (nos 1 et 2) c. Royaume Uni* [137].

58. Concernant la jurisprudence nationale, d'abord la Cour de cassation italienne applique également ces critères[138] dans un arrêt du 20 mars 2018[139] par lequel elle valide la demande d'un chanteur italien très connu de faire désindexer une vidéo où il est décrit

---

[134] Cour EDH, 19 octobre 2017, *Fuchsmann c. Allemagne*, req. n° 71233/13.
[135] À cet égard voir également Cour EDH, 14 décembre 2006, *Verlagsgruppe News GmbH v. Austria* (no. 2), req. n°10520/02, §36.
[136] Cour EDH, 16 octobre 2013, *Węgrzynowski et Smolczewski c. Pologne*, req. n° 33846/07, § 66.
[137] Cour EDH, 10 mars 2009, *Times Newspapers Limites (nos 1 et 2) c. Royaume Uni*, req. n°s 3002/03 et 23676/03. Voir aussi F. DUBUISSON, « Société de l'information, médias et liberté d'expression », *Journal européen des droits de l'homme*, 2014/3, pp. 378-379.
[138] La Cour de cassation prend en considération en particulier si les contenus publiés contribuent au débat public et répondent à un intérêt public effectif et actuel, l'identité et qualité de la personne concernée ainsi que la fiabilité des informations divulguées notamment leur véracité et la qualité des sources. Elle prend en compte enfin le comportement de la personne concernée, en particulier si cette dernière a été informée préventivement de la publication et si elle a pu exercer un droit de réponse.
[139] Corte di Cassazione, sez. *I*, 20/3/2018 n. 6919.

comme l'un des personnages les plus antipathiques du monde du spectacle. La Cour considère que le contenu ne participait pas au débat public car le chanteur n'occupait pas un rôle primordial dans la vie publique italienne ainsi la diffusion de la vidéo avait comme seul but de dénigrer l'artiste sans justification. Concernant la profession d'avocat, le Garante per la protezione dei dati personali[140] ne parvient pas à la même solution dans un *provvedimento*[141] concernant la demande de désindexation d'un avocat de contenus qui reportaient sa participation à des faits de corruption. En effet, le 24 mars 2016[142] le *Garante* a estimé que, au vu de la fonction que remplit la profession d'avocat dans la société, les informations litigieuses sont à considérer d'intérêt public et de ce fait elles peuvent être diffusées.

59. En France, le Conseil d'État a pu, par treize arrêts rendus le 6 décembre 2019, clarifier la jurisprudence de la Cour de justice de l'Union européenne ainsi que donner un mode d'emploi du droit à l'oubli à la Commission nationale de l'informatique et des libertés et au moteur de recherche Google. Il précise que le droit à l'oubli n'est pas absolu et qu'il doit être balancé avec d'autres droits notamment celui à la vie privée du demandeur et le droit à l'information du public. Cet équilibre doit être trouvé, en particulier, en regardant la nature des données personnelles partagées. À cet égard, le Conseil d'État a précisé trois catégories de données personnelles qui sont concernées : les données dites sensibles – le plus intrusives dans la vie privée d'une personne qui concernent, entre autres, sa santé, ses opinions politiques, sa vie sexuelle –, les données pénales ainsi que des données qui touchent à la vie privée mais qui ne sont pas sensibles[143]. Les deux premières catégories peuvent jouir d'une plus large protection et donc le droit au déréférencement doit être assuré sauf si le partage de ces contenus est nécessaire à l'information du public. Au contraire, la troisième catégorie jouit d'une moindre protection. En outre, comme pour les critères retenus par la Cour européenne des droits de l'Homme et la Cour de

[140] Autorité administrative indépendante établie par la loi n° 675 du 31 décembre 1996 et qui a pour mandat d'assurer la défense des droits et libertés fondamentaux et le respect de la dignité dans le traitement des données personnelles. Cette autorité correspond à la Commission nationale de l'informatique et des libertés (CNIL) en France.
[141] À considérer comme une décision de la CNIL en France.
[142] *Provvedimento* n° 144 du 24 mars 2016, disponible sur : https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb- display/docweb/5242797.
[143] Conseil d'État, Droit à l'oubli : le Conseil d'État donne le mode d'emploi, 6 décembre 2019. Disponible sur : https://www.conseil-etat.fr/actualites/actualites/droit-a-l-oubli-le-conseil-d-etat-donne-le-mode-d-emploi

cassation italienne, le Conseil d'État énumère des paramètres à prendre en compte dans l'examen de la demande de déréférencement et nommant le rôle social du demandeur (s'il s'agit d'une personne qui a un rôle dans la vie publique, quelle est sa fonction dans la société), ainsi que les conditions dans lesquelles les données ont été publiées.

60. De surcroit, certaines difficultés se rencontrent également lorsque le demandeur avait lui-même posté les contenus et les informations qu'il souhaite faire désindexer. En effet, cela diffère selon les plateformes de réseaux sociaux et les moteurs de recherche. Par exemple, sur Twitter il y a la possibilité d'effacer tous les contenus publiés. Sur Facebook les utilisateurs sont propriétaires des contenus et ces derniers s'effacent, normalement[144], au moment de la suppression du compte. Toutefois, certains contenus s'ils ont été partagés par des tiers ne seront pas effacé[145]. Google, au contraire, met en cause le droit au déréférencement lorsque l'information a été mise en ligne par le demandeur lui-même[146].

61. L'une des spécificités d'Internet se situe donc dans la possibilité de créer et mettre à disposition des archives en ligne. Si, d'une part, cela permet aux individus de jouir d'un droit d'information, d'autre part, cette possibilité est aussi source d'atteinte aux droits fondamentaux tels que le droit à la vie privée. Pour cela, il ressort de la jurisprudence nationale et européenne que le droit à l'oubli n'est pas un droit absolu et qu'il est mis en balance avec d'autres droits et libertés. Mais ce qui ressort également est qu'il y a une certaine cohérence entre les critères pour examiner les demandes de déréférencement et que ce dernier est à géométries variables. En effet, il est exercé selon la nature du demandeur, le contenu des publications et leurs effets. En somme, c'est un droit utile et nécessaire mais limité et casuistique. En outre, ce droit se trouve surtout inscrit dans des instruments nationaux et du droit de l'Union européenne, l'absence d'encadrement en

---

[144] Voir notamment N. DEVILLIER, « Pourquoi vos données survivront à la suppression de votre compte Facebook et quels en sont les risques ? », *The Conversation*, 28 mars 2018. Disponible sur : https://theconversation.com/pourquoi-vos-donnees-survivront-a-la-suppression-de-votre-compte-facebook-et-quels-en-sont-les-risques-94011

[145] Par exemple lorsqu'une photo publiée par un utilisateur X est "partagée sur le mur Facebook » d'un utilisateur ou est partagée sur un autre réseau social.

[146] « Information that is published by or with the consent of the data subject himself or herself will weigh against delisting » voir le rapport du Advisory Council to Google on the Right to be Forgotten du 6 février 2015, p. 13.

droit international ne renforce pas sa protection et n'aide pas à trouver des orientations dans la balance à faire entre ce droit et les autres droits et libertés fondamentaux. Ce qui souligne à nouveau qu'Internet est un lieu propice à l'exécution des cyberviolences notamment lorsque des informations personnelles, sans intérêt public, sont publiées et diffusés sur les réseaux sociaux et référencées par les moteurs de recherche.

II. Le traitement des contenus illicites fragilisé par la dimension transnationale d'Internet

62. Internet représente un lieu où les droits se mêlent. L'exécution mais également l'amplification[147] des cyberviolences sont facilitées par la dimension transnationale d'Internet. Cette dernière complique l'établissement de la compétence juridictionnelle et, de fait, ralenti le traitement des comportements illicites (**A**). Ainsi, une conséquence de la transnationalité qui ajoute une difficulté supplémentaire dans le traitement des comportements illicites, est celle de la différence d'approches qui se heurtent entre les législations nationales et les règlements intérieurs des plateformes (**B**).

A. L'a-territorialité, complexifiant l'établissement de la compétence juridictionnelle

63. Le Professeur Philippe Lagrange parle de « a-territorialité » pour décrire la dimension intrinsèquement transnationale du cyberespace. Ce dernier, « de par sa virtualité, ne connaît pas de limites internationales, il les transcende »[148].

64. Cette a-territorialité est strictement liée aux caractéristiques du cyberespace qui, pour certains, ne connaît pas de frontière, ni spatiale ni physique (terrestre, maritime ou encore aérienne)[149]. Pour d'autres, des frontières existent mais seraient électroniques[150] et ne permettraient pas de délimiter l'exercice des compétences étatiques[151]. Il semblerait plus

---

[147] La question de l'amplification sera traitée dans le chapitre II de ces travaux.
[148] P. LAGRANGE, « Internet et l'évolution normative du droit international : d'un droit international applicable à l'internet à un DI du cyberespace ? », in *Internet et le droit international*, SFDI, Pedone, 2014, p. 65.
[149] A.T. NORODOM, « Internet et le droit international : défi ou opportunité ? », in *Internet et le droit international*, SFDI, Pedone, 2014, p. 25-26.
[150] *Ibid*, p. 26. qui cite D. VENTRE, Cyberespace et acteurs du cyberconflits, Lavoisier, 2011, p.83.
[151] *Ibid*, p. 26.

vraisemblable que ces frontières soient de « projections des frontières physiques réelles permettant de repartir l'exercice des compétences étatiques au sein du cyberespace »[152]. Ce vaste espace est règlementé par une multiplicité de droits, en particulier, par les droits étatiques à défaut d'un ou plusieurs instruments juridiques internationaux et ou européens harmonieux.

65. L'a-territorialité se traduit par plusieurs difficultés, l'une d'entre elles est celle de la compétence étatique des États concernant des contenus illicites qui se matérialisent dans un État mais qui ont des conséquences dans un ou plusieurs autres États. Il est nécessaire d'analyser donc la compétence juridictionnelle des États dans le cyberespace, avant de se pencher sur les différentes approches des États et des plateformes vis-à-vis des comportements illicites.

1. La compétence juridictionnelle

66. Il est intéressant de soulever la question de la compétence juridictionnelle des États[153]. Pour établir la compétence, d'abord, il faut analyser la nature du comportement illicite, en particulier, s'il s'agit d'un cyberdélit et un cybercrime, ensuite, chercher s'il existe un élément d'extranéité. Ce dernier peut prendre plusieurs formes, par exemple, lorsque les hébergeurs d'un site Internet où des contenus illicites ont été publiés se situent à l'étranger, mais aussi lorsque le fait dommageable a lieu dans un pays mais qu'il a des conséquences dans un autre pays ou encore lorsque l'auteur ou la victime du comportement illicite ne se trouvent pas dans l'État où le fait dommageable a eu lieu.

67. Ainsi, si les faits dommageables ne présentent pas d'éléments d'extranéité, la compétence relève des juridictions nationales. Au contraire, quand un élément d'extranéité vient s'ajouter à cette analyse, alors les principes du droit international privé en matière de juridiction peuvent s'appliquer à la matière délictuelle.

---

[152] *Ibid*, p. 27.
[153] À cet égard les cours européennes n'ont pas de compétence comme prévu par le droit international privé et confirmé notamment par la jurisprudence européenne, par exemple l'arrêt de la Cour EDH, 10 février 2011, *Premininy c. Russie*, req. n° 44973/04 et plus particulièrement dans une affaire concernant Google l'arrêt de la Cour EDH, *Ahmet Yıldırım c. Turquie* du 18 décembre 2012, req. n° 3111/10, § 67.

a. Sur les cyberdélits

68. C'est le Règlement Bruxelles I bis[154], en particulier, l'article 7 § 2 qui règle la question de la compétence en disposant qu'« une personne domiciliée sur le territoire d'un État membre peut être attraite, dans un autre État membre […] en matière délictuelle ou quasi délictuelle, devant la juridiction du lieu où le fait dommageable s'est produit ou risque de se produire »[155]. Il est intéressant de retracer l'évolution de la jurisprudence européenne et nationale pour apprécier la question de la juridiction dans le cadre de comportements illicites qui présentent un élément d'extranéité. Il y a une diversification des rattachements et différentes méthodes sont employées pour matérialiser et localiser le dommage. Nous pouvons parler de la théorie de l'accessibilité qui implique que la simple accessibilité du site peut entrainer le dommage. Cela a été le cas lors de *l'affaire Yahoo*[156] pour la Cour de justice de l'Union européenne dans le cadre de la vente en ligne d'objets nazis ou dans *l'arrêt Cristal*[157] jugé par la Cour de cassation française et qui portait sur la contrefaçon.

69. Plusieurs critiques sont portées au choix de cette approche notamment à cause du risque encouru de *forum shopping*[158], cela a été explicitement exposé par la Cour d'appel de

---

[154] Règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (règlement Bruxelles I bis), Journal officiel n° L 351/1.

[155] Article 5 §3 du règlement Bruxelles I bis.

[156] L'affaire Yahoo comporte plusieurs arrêts, en l'espèce il s'agissait de la vente d'objets nazis en France par le moteur de recherche Yahoo établi aux États-Unis. Le TGI de Paris avait demandé à Yahoo d'interrompre la possibilité pour le public français de consulter les annonces de vente d'objets nazis et de les acheter (*TGI Paris*, 22 mai 2000). Yahoo porte l'affaire devant la Cour Fédéral du District de Californie du Nord qui considère que la décision du TGI est contraire au premier amendement de la Constitution des États-Unis qui concerne la liberté d'expression et que cette dernière ne pouvait pas s'appliquer aux États-Unis. Les demandeurs, en l'espèce la Ligue Internationale contre le Racisme et l'Antisémitisme (LICRA) et l'Union des Étudiants Juifs de France (UEJF), font appel de cette décision devant la Cour d'appel de Paris le 22 août 2004 qui se déclare incompétente mais toutefois décide que la vente de ces objets sera interdite en France (Cour d'Appel de Paris, 22 août 2004). Enfin, la Cour d'appel du District de Californie a déclaré que cette dernière décision de la CA de Paris ne violait pas la liberté d'expression et qu'elle était donc applicable à Yahoo.

[157] Dans cet arrêt les juridictions françaises se sont déclarées compétentes, en l'espèce il s'agissait d'un ressortissant français qui s'estimait victime de contrefaçon du fait des agissements d'une société espagnole qui vendait des vins sur Internet sous la marque « Crystal », voir Civ. 1re, 9 déc. 2003, D. 2004. 276.

[158] Le Forum Shopping « consiste à assurer l'accès au for le plus favorable, que ce soit sur le plan procédural […] ou sur le terrain du fond, voir : D. BUREAU et H. MUIR WATT, *Droit international privé*, Tome I, partie générale, 4ème édition, 2017, p. 261.

Paris dans un arrêt du 6 juin 2007[159]. La Chambre commerciale de Paris[160] avait retenu, à plusieurs reprises, la théorie de la focalisation qui conduit « à donner compétence, non pas aux différents ordres juridictionnels dans lesquels le site Internet est accessible, mais uniquement à ceux des États visés par le diffuseur du contenu litigieux »[161].

70. En ce qui concerne les atteintes aux droits de la personnalité, la Cour de justice de l'Union européenne, plus réticente à la théorie de la focalisation, a consacré la théorie de l'accessibilité dans son désormais célèbre *affaire eDate et Martinez*[162]. La décision de la Cour diffère de ses précédents *affaires Pammer* et *Hotel Aplenhof*[163] qui concernaient les règles de compétence protectrices des consommateurs. Selon la Cour « en cas d'atteinte alléguée aux droits de la personnalité au moyen de contenus mis en ligne sur un site Internet, la personne qui s'estime lésée a la faculté de saisir d'une action en responsabilité, au titre de l'intégralité du dommage causé, soit les juridictions de l'État membre du lieu d'établissement de l'émetteur de ces contenus, soit les juridictions de l'État membre dans lequel se trouve le centre de ses intérêts »[164]. Ainsi, la Cour inscrit dans cet arrêt deux autres possibilités pour le demandeur, outre à la compétence ouverte par l'article 4, paragraphe 1, du Règlement Bruxelles I bis qui prévoit que « les personnes domiciliées sur le territoire d'un État membre sont attraites, quelle que soit leur nationalité, devant les juridictions de cet État membre »[165]. La première possibilité est le résultat de la transposition par la Cour de justice de l'Union européenne de *l'arrêt*

---

[159]Cour d'appel de Paris, 6 juin 2007, n° 06/14890 « Compte tenu de l'universalité de ce réseau, appliquer le critère de la simple accessibilité aurait nécessairement pour conséquence d'institutionnaliser la pratique du *forum shopping* ». *Voir* F. JAULT-SESEKE, « Internet, vecteur d'affinement des règles de compétence juridictionnelle », in *Internet et le droit international*, *SFDI*, Pedone, 2014, p. 175.

[160] Cass. Com., 9 mars 2010, n° 08-16.752 ; 13 juillet 2010, n°06-20.230 ; 23 novembre 2010, n° 07-19.543 ; 20 septembre 2011, n° 10-16.569 ; 3 mai 2021, n° 11-10.505, n° 11-10.507 et n° 11-10.508, voir F. JAULT-SESEKE, « Internet, vecteur d'affinement des règles de compétence juridictionnelle », in *Internet et le droit international*, *SFDI*, Pedone, 2014, p. 171.

[161] F. JAULT-SESEKE, « Internet, vecteur d'affinement des règles de compétence juridictionnelle », in *Internet et le droit international*, *SFDI*, Pedone, 2014, p. 170. Voir également O. CACHARD, *La régulation internationale du marché electronique*, LGDJ, Tome 365, pp. 65-73.

[162] CJUE, GC, 25 octobre 2011, *eDate Advertising Gmbh c. X*, affaires jointes C-509/09 et C-161/10.

[163] « La Cour avait jugé que la simple accessibilité du site Internet du professionnel ne pouvait suffire à caractériser l'existence d'activités « dirigées » vers l'État membre du domicile du consommateur », voir S. BOLLÉE, B. HAFTEL, « Les nouveaux (dés)équilibres de la compétence internationale en matière de cyberdélits après l'arrêt eDate Advertising et Martinez », *Recueil Dalloz*, 2012, p. 1285, voir CJUE, 7 décembre 2010, *Peter Pammer c. Reederei Karl Schlüter GmbH & Co. KG et Hotel Alpenhof GesmbH c. Oliver Heller*, affaires jointes C-585/08 et C-144/09.

[164] CJUE, GC, 25 octobre 2011, *eDate Advertising Gmbh c. X*, affaires jointes C-509/09 et C-161/10.

[165] Article 4, paragraphe 1, du règlement Bruxelles I.

Shevill[166]en matière de diffamation par voie de presse qui prévoit la compétence de l'État membre de l'éditeur. La seconde est une nouveauté de l'arrêt qui ouvre au demandeur la possibilité de saisir l'État membre dans lequel se trouve le centre de ses intérêts. La Cour parvient à cette conclusion après avoir considéré, sans vraiment donner une justification, qu'il fallait adapter les critères de rattachement de l'*arrêt Shevill*[167] à Internet, en effet, selon elle « étant donné que l'impact d'un contenu mis en ligne sur les droits de la personnalité d'une personne peut être le mieux apprécié par la juridiction du lieu où la prétendue victime a le centre de ses intérêts, l'attribution de compétence à cette juridiction correspond à l'objectif d'une bonne administration de la justice »[168]. Cette possibilité est conforme, selon la Cour, à l'objectif de prévisibilité des règles de compétences « étant donné que l'émetteur d'un contenu attentatoire est, au moment de la mise en ligne de ce contenu, en mesure de connaître les centres des intérêts des personnes qui font l'objet de celui-ci »[169].

Nous pouvons également citer un autre arrêt de la Cour de Justice de l'Union européenne « qui marque un coup d'arrêt à l'évolution jusqu'ici très libérale de la jurisprudence de la Cour en matière de protection des droits de la personnalité »[170]. La Cour était appelée à s'exprimer au sujet d'une demande de décision préjudicielle portant sur l'interprétation de l'article 7, point 2 du règlement (UE) n°12/2012 du parlement européen et du Conseil, du 12 décembre 2012, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, et, en particulier, sur prétendue violation des droits de la personnalité d'un individu résultant de la publication d'un article sur un site Internet. En l'espèce, le demandeur n'était pas visé directement

[166] CJUE, 7 mars 1995, *Fiona Shevill c. Presse Alliance SA*, C-68/93.
[167] C'est-à-dire pour la victime la possibilité d' « intenter contre l'éditeur une action en réparation soit devant les juridictions de l'État contractant du lieu d'établissement de l'éditeur de la publication diffamatoire, compétentes pour réparer l'intégralité des dommages résultant de la diffamation, soit devant les juridictions de chaque État contractant dans lequel la publication a été diffusée et où la victime prétend avoir subi une atteinte à sa réputation » voir CJUE, GC, 25 octobre 2011, *eDate Advertising Gmbh c. X*, affaires jointes C-509/09 et C-161/10 §42.
[168] CJUE, GC, 25 octobre 2011, *eDate Advertising Gmbh c. X*, affaires jointes C-509/09 et C-161/10 §48.
[169] *Ibid*, §50, voir également M-E. ANCEL, « Un an de droit international du commerce électronique », *Communication-commerce électronique*, 2012, p.4.
[170] F. MAILHÉ, CJUE, 1re ch., 17 juin 2021, Mittelbayerischer Verlag KG c/ SM, aff. C-800/19, ECLI:EU:C:2021:489, Jurisprudence de la CJUE 2021, Décisions et commentaires 2022.

ou indirectement par le contenu publié, en effet, ce dernier avait fondé sa demande sur l'atteinte à son identité et à sa dignité nationale résultant de l'utilisation de l'expression « camp d'extermination polonais de Treblinka », estimant une atteinte à ses droits de la personnalité eu égard à son appartenance au peuple polonais. Or, une prétendue atteinte aux droits de la personnalité doit reposer sur des éléments objectifs et vérifiables et non pas uniquement sur la sensibilité individuelle ou des éléments exclusivement subjectifs. Le demandeur n'était manifestement pas identifié en tant qu'individu ni indirectement ni directement dans le contenu publié sur Internet. Pour cela, la Cour estime que « la juridiction du lieu où se trouve le centre des intérêts d'une personne prétendant que ses droits de la personnalité ont été violés par un contenu mis en ligne sur un site Internet n'est compétente pour connaître, au titre de l'intégralité du dommage allégué, d'une action en responsabilité introduite par cette personne que *si ce contenu comporte des éléments objectifs et vérifiables permettant d'identifier, directement ou indirectement, ladite personne en tant qu'individu* »[171].

71. Après avoir analysé la jurisprudence des cours européennes, il convient de se tourner vers les travaux de l'Institut du droit international[172] qui s'est penché sur la question de conflits transfrontaliers en matière d'atteinte aux droits à la personnalité. À cet égard, une résolution[173] a été adoptée, « sous la forme d'une loi uniforme de droit international privé »[174]. Cette dernière vise à trouver un équilibre entre, « d'une part, la protection de la vie privée et des autres droits de la personnalité et, de l'autre part, la sauvegarde de la liberté d'expression, en traitant, dans la mesure du possible et s'il y a lieu, les parties au litige sur un pied d'égalité, tout en créant un système de règles qui soit efficace et facile d'application »[175]. Pour garantir une égalité entre les parties la résolution propose quatre chefs de compétence : deux associés au défendeur c'est-à-dire l'État du domicile du

---

[171] CJUE,1re chambre, 17 juin 2021, *Mittelbayerischer Verlag KG c. SM*, aff. C-800/19.
[172] L'institut du droit international a été fondé en 1873, il est une institution indépendante qui a comme objectif de contribuer au développement du droit international et d'agir pour qu'il soit appliqué. L'institut publie régulièrement des résolutions qui sont portées à la connaissance des gouvernements, des organisations internationales et de la communauté scientifique.
[173] Institut du droit international, « Internet et les atteintes à la vie privée : problèmes de conflit de lois et de juridictions », résolution, 8 RES FR, 31 août 2018. Disponible sur : https://www.idi-iil.org/app/uploads/2019/09/8-RES-FR.pdf.
[174] E. JAYME et S. C. SYMEONIDES (rapp.), « Internet et les atteintes à la vie privée : problèmes de conflits de loi et juridiction », Institut du droit international, 2019, p. 249.
[175] *Ibid.*

défendeur ou l'État où il a commis le comportement présumé illicite ; les deux autres sont associés au demandeur, c'est-à-dire l'État de résidence du demandeur ou l'État où les effets du comportement du défendeur sont survenus.

b. Sur les cybercrimes

72. Concernant les crimes, la juridiction est, entre autres, attribuée selon la localisation du « fait constitutif ». La question de la territorialité pose certaines difficultés, notamment à cause du fait que les règles de compétence établies par les États membres ne prennent pas en compte l'universalité d'Internet. Selon Jacques Francillon « tous les pays du monde sont […] susceptibles de se déclarer compétents, ce qui revient à consacrer une *compétence universelle* – et non plus seulement territoriale, personnelle ou réelle – en faveur des juges pénaux nationaux, au risque de multiplier les conflits positifs de compétence »[176]. Cette multiplicité de compétences peut poser problème là où les droits nationaux ne prévoient pas les mêmes dispositions et ne pénalisent pas les comportements illicites de la même façon. Un exemple qui peut illustrer ce propos est celui de l'arrêt *Yahoo* précédemment cité. Comme le signale J. Francillon ces différences peuvent entraîner un risque d'insécurité juridique pour les justiciables découlant de la légalité criminelle de la loi pénale qui doit être accessible et prévisible[177].

73. Au niveau international, il n'existe pas d'instruments juridiques qui ont pu clarifier et améliorer le risque d'insécurité juridique. En effet, l'un des seuls instruments juridiques contraignants en matière de cybercriminalité, la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), prévoit des règles de compétence mais ne résout pas le problème de la litispendance parce qu'elle laisse aux États la faculté de se concerter[178].

74. Concernant la Cour européenne des droits de l'Homme, il est intéressant de rappeler les conditions d'exercice de sa juridiction. Le premier article de la Convention européenne

---

[176] J. FRANCILLON, « Le droit pénal face à la cyberdélinquance et à la cybercriminalité », *Revue Le Lamy Droit de l'immatériel*, Nº 81, 1er avril 2012, p. 5. Italique par l'autrice.
[177] *Ibid.*
[178] Article 22 (5) de la Convention du Conseil de l'Europe sur la cybercriminalité.

de sauvegarde des droits de l'homme et des libertés fondamentales prévoit que « les Hautes Parties contractantes reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au titre I de la […] Convention ». Or, à plusieurs reprises la Cour a pu s'exprimer, notamment à travers de sa jurisprudence, sur la signification du terme « juridiction » et sur l'apport de cet article[179]. Elle considère que « du point de vue du droit international public, la compétence juridictionnelle d'un État est principalement territoriale »[180]. À plusieurs reprises, elle a confirmé que « la juridiction d'un État, au sens de l'article 1, est principalement territoriale »[181] et qu'« elle est présumée s'exercer normalement sur l'ensemble de son territoire »[182]. Elle ajoute qu'« à l'inverse, les actes des États contractants accomplis ou produisant des effets en dehors de leur territoire ne peuvent que dans des circonstances exceptionnelles s'analyser en l'exercice par eux de leur juridiction, au sens de l'article 1 »[183]. Face à une situation exceptionnelle la Cour devra examiner « l'ensemble des éléments factuels objectifs de nature à limiter l'exercice effectif de l'autorité d'un État sur son territoire et, d'autre part, le comportement de celui-ci »[184]. Elle a également établi que la juridiction est une condition *sine qua non,* en effet « elle doit avoir été exercée pour qu'un État contractant [à la Convention européenne des droits de l'Homme] puisse être tenu pour responsable des actes ou omissions à lui imputables qui sont à l'origine d'une allégation de violation des droits et libertés énoncés dans la Convention »[185]. Ainsi, cette allégation doit relever de la juridiction de l'État contractant, à défaut la Cour pourra se considérer incompétente *rationae personae* et/ou *rationae loci.*

75. Concernant Internet, il est nécessaire de mentionner l'arrêt *Perrin c. Royaume-Uni* dans lequel la question de la juridiction avait été soulevée. Dans cet affaire la Cour confirme la condamnation d'un ressortissant français, habitant au Royaume-Uni et qui avait publié

---

[179] Voir également le guide sur l'article 1 de la Convention européenne des droits de l'Homme, 30 avril 2021. Disponible sur : https://www.echr.coe.int/Documents/Guide_Art_1_FRA.pdf
[180] Cour EDH, GC, 12 décembre 2001, B*anković et autres c. Belgique et autres*, req. n° 52207/99, §§ 59-61.
[181] Cour EDH, 7 juillet 2011, *Al-Skeini et autres c. Royaume-Uni*, req. n°55721/07, §131.
[182] Cour EDH, 8 juillet 2004, *Ilaşcu et autres*, req. n° 48787/99, § 312.
[183] Cour EDH, GC, 12 décembre 2001, B*anković et autres c. Belgique et autres*, req. n° 52207/99, §67.
[184] Cour EDH, 8 juillet 2004, *Ilaşcu et autres*, req. n° 48787/99, § 311.
[185] Cour EDH, 19 octobre 2012, *Catan et autres c. République de Moldova et Russie*, req. nos 43370/04, 8252/05 et 18454/06, §103. Voir également Cour EDH, 8 juillet 2004, *Ilaşcu et autres*, req. n° 48787/99, § 311 et Cour EDH, GC, 7 juillet 2011, *Al-Skeini et autres* c. Royaume Uni, n° 55721/07, § 130.

des images obscènes sur un site hébergé aux États-Unis, au motif que les lois du Royaume-Uni prohibant de telles publications lui étaient raisonnablement accessibles. Cet argumentaire était renforcé par le fait que le site où le demandeur avait publié ces contenus illicites était utilisé pour son activité professionnelle, ce pourquoi la Cour a considéré qu'il lui incombait de faire preuve d'une grande prudence et de prendre les avis juridiques nécessaires[186] pour sa bonne utilisation. La Cour clarifie ensuite un point important sur Internet et la proportionnalité des peines[187]. En effet, la Cour a établi qu'un État n'outrepasse pas sa marge d'appréciation en interdisant la diffusion de contenus qui n'auraient rien eu d'illégal dans un autre État, en l'espèce les États-Unis[188].

76. La dimension transnationale multiplie les difficultés dans l'établissement de la compétence juridictionnelle et dans le traitement des comportements illicites, en ouvrant la voie au risque d'insécurité juridique. Cette insécurité s'amplifie également à cause des approches différentes adoptées par les acteurs d'Internet. En effet, les comportements illicites peuvent être accomplis depuis un État qui n'encadre pas de la même manière certains droits et libertés. Ces différentes approches étatiques se mêlent également avec les appréciations faites par les plateformes en conformité avec leurs règlementations, qu'il faut rappeler, sont prises unilatéralement.

B. Des appréciations divergentes des cyberviolences par les acteurs d'Internet

77. Une autre difficulté liée à l'ubiquité et à l'a-territorialité est celle des différences d'approches sur les comportements illicites en ligne adoptées par les États (**1**) et les plateformes numériques (**2**). Ces divergences peuvent mener à une absence de cohérence vis-à-vis du traitement des contenus partagés sur Internet.

1. Les différentes approches des États

78. Au sein de l'Union européenne les approches concernant la protection des droits fondamentaux et des droits humains sur Internet sont assez cohérentes, même si des vides

[186] Cour EDH, 18 octobre 2005, *Perrin c. Royaume- Uni*, req. n° 5446/03.
[187] La proportionnalité sera étudiée dans le chapitre VIII de cette thèse.
[188] *Ibid.*

juridiques subsistent pour certains États en matière de contenus illicites en ligne. Cette cohérence est due notamment à la ratification d'instruments internationaux comme la Convention européenne des droits de l'Homme ou de la transposition des directives européennes[189]. Différentes approches se heurtent notamment entre la conception européenne du droit à la liberté d'expression et du discours de haine et celle des États-Unis où plusieurs plateformes, dont les plus connues telles que Facebook, Twitter et YouTube, sont domiciliées.

79. En effet, aux États-Unis « la liberté d'expression […] est conçue comme une « liberté négative », ne prescrivant aucun comportement »[190]. Le premier amendement de la Constitution des États-Unis protège cette liberté et énonce :

> « Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances »[191].

La Cour suprême des États-Unis a, à plusieurs reprises, clarifié le sens de la liberté d'expression. Nous pouvons citer l'arrêt *Clarence Brandenburg v. State of Ohio* dans lequel la Cour estime que « […] the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action »[192].

---

[189] Voir entre autres la directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants et la directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique.

[190] E. ZOLLER, « La Cour suprême des États-Unis et la liberté d'expression », in E. ZOLLER (dir.), *La liberté d'expression aux États-Unis et en Europe*, Dalloz, 2008, p. 288 cité par C. RUET, « Chapitre 5. - Liberté d'expression et lutte contre le discours de haine sur Internet » in C. DE TERWANGNE, et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 174.

[191] 1er amendement de la Constitution des États-Unis. « 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 », traduction disponible ici : https://mjp.univ-perp.fr/constit/us1787a.htm.

[192] Cour Suprême, 9 juin 1969, *Clarence Brandenburg v. State of Ohio*, n°492, point 7. Traduction par l'autrice : « […] les garanties constitutionnelles de la liberté d'expression et de la liberté de la presse ne permettent pas à un État d'interdire ou de proscrire l'apologie du recours à la force ou de la violation de la loi,

Le premier amendement veut éviter le musèlement de l'expression de certaines idées[193]. Cet article permet donc de tenir des propos fondés sur l'intolérance raciale, religieuse ou encore sexiste. Le principe du droit à la liberté d'expression ne se fonde pas sur le contenu de propos mais sur la façon d'exprimer de tels propos. En effet, la limite à la protection de cette liberté est très haute car elle est franchie seulement si la publication vise à inciter ou à produire une action illégale imminente et est susceptible d'inciter ou de produire une telle action. La Cour européenne des droits de l'Homme avait pu éclaircir l'approche adoptée par les États-Unis dans son arrêt *Vona c. Hongrie* dans lequel la Cour explique que « le premier amendement à la Constitution des États-Unis permettait à un État d'interdire les « vraies menaces », ce qui englobait les déclarations par lesquelles l'auteur entendait communiquer à un individu ou groupe d'individus particulier son intention de commettre un acte de violence illégale »[194].

80. L'approche des États de l'Union européenne et celle adoptée par le Conseil de l'Europe est alors très différents de celle des États-Unis, car « tout écrit, image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes »[195] est sanctionné. D'ailleurs, dans certains États

---

sauf si cette apologie vise à inciter ou à produire une action illégale imminente et est susceptible d'inciter ou de produire une telle action ».

[193] C. RUET, « Chapitre 5. - Liberté d'expression et lutte contre le discours de haine sur Internet » in C. DE TERWANGNE, et Q. VAN ENIS (dir.*), L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 174.

[194] Cour EDH, 9 juillet 2013, *Vona c. Hongrie*, aff. 35943/10, § 31.

[195] Article 2 du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Voir également l'article 17 de la Convention européenne des droits de l'Homme. Pour avoir un aperçu de la jurisprudence de la Cour européenne des droits de l'Homme sur le discours de haine voir https://www.echr.coe.int/Documents/FS_Hate_speech_FRA.pdf. Concernant l'Union européenne à ce sujet voir la décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008F0913&from=en* ; voir également l'action commune du 15 juillet 1996 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, concernant l'action contre le racisme et la xénophobie, disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31996F0443&from=EN. Ainsi que la résolution législative du Parlement européen sur la proposition de décision-cadre du Conseil concernant la lutte contre le racisme et la xénophobie (COM(2001) 664 — C5-0689/2001 — 2001/ 0270(CNS)), disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52002AP0363&from=FR). Voir enfin CJUE, 22 septembre 2011,

de tradition de *common law* cette approche semble être partagée[196] comme au Canada où le Tribunal des droits de l'Homme a établi qu'un site révisionniste hébergé aux États-Unis mais édité au Canada était illégal[197] ou en Australie où la Cour fédérale australienne a pris une décision similaire en septembre 2002[198].

81. Cette différence d'approches s'est manifestée également dans la conception et ratification des instruments internationaux. Cela a été le cas lors de la création de la Convention du Conseil de l'Europe sur la cybercriminalité. En effet, à l'origine la Convention devait avoir des dispositions sur la haine en ligne, la xénophobie et la lutte contre le racisme et l'incitation à la violence. Toutefois, compte tenu des divergences d'approches et de l'absence de consensus notamment avec les États-Unis et certains États européens[199], le Conseil de l'Europe a préféré faire adopter la Convention sans ces dispositions et ajouter un protocole additionnel sur ces thématiques[200], que, toutefois n'a pas été ratifié par tous les États membres de la Convention[201]. Avant cela, il est opportun de rappeler la réserve apportée à l'article 2 de la Convention Internationale sur l'élimination de toutes les formes de discrimination raciale du 21 décembre 1965 et

---

Mesopotomia Broadcast A/S METV, Roj TV/ AS c. BundesrepublikDeutschland, aff. jointes C-244/10 et C-245/10, § 42.

[196] F. DUBUISSON et I. RORIVE, « La liberté d'expression à l'épreuve d'Internet », in *Entre ombres et lumières : cinquante ans d'application de la Convention européenne des droits de l'homme en Belgique*, Centre de droit public de l'Université libre de Bruxelles, Bruxelles, Bruylant, 2008, pp. 368-369.

[197] Human Rights Tribunal, *Enst Zundel v. The Queen*, 2002, n° 953/2000 cité par F. DUBUISSON et I. RORIVE précité.

[198] Federal Court of Australia, 17 septembre 2002, *Jones v. Toben*, FCA 1150 cité par F. DUBUISSON et I. RORIVE précité.

[199] Certains États européens traditionnellement hostiles à la pénalisation du discours de haine.

[200] Le Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Voir F. DUBUISSON et I. RORIVE, « La liberté d'expression à l'épreuve d'Internet », in *Entre ombres et lumières : cinquante ans d'application de la Convention européenne des droits de l'homme en Belgique*, Centre de droit public de l'Université libre de Bruxelles, Bruxelles, Bruylant, 2008, pp. 366-367. Voir également, Conseil de l'Europe, *Rapport explicatif du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, 28 janvier 2003, point 4.

[201] Un grand nombre d'États membres du Conseil de l'Europe n'a pas encore ratifié le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, c'est le cas de l'Autriche, l'Azerbaïdjan, la Belgique, la Bulgarie, l'Estonie, la Russie, la Géorgie, la Hongrie, l'Irlande, l'Islande, l'Italie, le Liechtenstein, Malte, la République Slovaque, le Royaume Uni, la Suisse et la Turquie alors que la Convention de Budapest contre la cybercriminalité a été ratifié par l'ensemble des pays membres sauf la Russie et l'Irlande.

ratifiée par les États-Unis le 21 octobre 1994[202]. Ainsi que, la réserve faite par les États-Unis à l'article 20[203] du *Pacte international relatif aux droits civils et politiques* de 1966 ratifié par les États-Unis en 1992.

82. Cette différence d'approches se manifeste également dans la jurisprudence et un exemple emblématique est celui de *l'affaire Yahoo*[204] entre les États-Unis et la France dans lequel il était question de la vente d'objets nazis en France sur le site *Yahoo* basé de l'autre côté de l'Atlantique. Se heurtaient alors le droit à la liberté d'expression protégé aux États-Unis par le premier amendement et l'article R.645-1 du Code pénal français qui interdit le porte et l'exhibition en public d'un uniforme, insigne ou emblème nazi. En effet, le Tribunal de grande instance de Paris considérait que l'exposition d'objets nazis en vue de leur vente constituait une contravention à la loi française mais également une offense à la mémoire collective du pays[205]. Le Tribunal a ainsi ordonné au site Yahoo de prendre toutes les mesures pour dissuader et rendre impossible la consultation de ces offres par les internautes basés en France. L'affaire se poursuivra ensuite aux États-Unis devant la Cour Fédéral du District de Californie du Nord qui considère que la décision du Tribunal de grande instance était contraire au premier amendement de la Constitution des États-

[202] L'article 4 de la Convention Internationale sur l'élimination de toutes les formes de discrimination raciale prévoit que « les États parties condamnent toute propagande et toutes organisations qui s'inspirent d'idées ou de théories fondées sur la supériorité d'une race ou d'un groupe de personnes d'une certaine couleur ou d'une certaine origine ethnique, ou qui prétendent justifier ou encourager toute forme de haine et de discrimination raciales; ils s'engagent à adopter immédiatement des mesures positives destinées à éliminer toute incitation à une telle discrimination » et précisait que les États s'engagent à « déclarer délits punissables par la loi toute diffusion d'idées fondées sur la supériorité ou la haine raciale, toute incitation à la discrimination raciale, ainsi que tous actes de violence, ou provocation à de tels actes, dirigés contre toute race ou tout groupe de personnes d'une autre couleur ou d'une autre origine ethnique […] ». La réserve des États-Unis énonçait par conséquent que : « la Constitution et les lois des États-Unis prévoient des garanties étendues en faveur de la liberté de parole, d'expression et d'association des individus. En conséquence, les États-Unis n'acceptent aucune obligation en vertu de la présente Convention, en particulier ses articles 4 et 7, de nature à restreindre ces droits par l'adoption d'une législation ou de toute autre mesure, pour autant que ces derniers sont protégés par la Constitution et les lois des États-Unis.

[203] L'article 20 du *Pacte international relatif aux droits civils et politiques* prévoit que « 1. Toute propagande en faveur de la guerre est interdite par la loi. 2. Tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence est interdit par la loi ». Les États-Unis ont adopté la réserve suivante vis-à-vis en particulier du point 2 : « L'article 20 n'autorise pas les États-Unis et n'exige pas d'eux qu'ils adoptent des lois ou autres mesures de nature à restreindre la liberté d'expression et d'association protégée par la Constitution et les lois des États-Unis ». Voir : https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_fr#EndDec

[204] Précité, voir note 156.

[205] TGI de Paris, 22 mai 2000.

Unis. Les demandeurs, en l'espèce, la Ligue Internationale contre le Racisme et l'Antisémitisme (LICRA) et l'Union des Étudiants Juifs de France (UEJF), feront ensuite appel de cette décision devant la Cour d'appel de Paris le 22 août 2004 qui se déclare incompétente mais qui décide, toutefois, que la vente de ces objets sera interdite en France. Enfin, la Cour d'appel du District de Californie a déclaré que cette dernière décision de la juridiction d'appel de Paris ne violait pas la liberté d'expression protégée par le premier amendement et qu'elle était donc applicable à Yahoo qui devait prendre les mesures nécessaires demandées par les autorités françaises. Or, ce cas d'espèce se termine avec la protection du droit français en dépit de la protection de la liberté d'expression entendue au sens du premier amendement de la Constitution des États-Unis. Cependant, on constate que ces différences d'approches ralentissent le traitement des contenus illégaux.

83. Cette différence d'appréciations ne doit pas être un motif pour affaiblir la protection des droits fondamentaux sur Internet, mais plutôt faire prévaloir des réglementations qui les défendent et qui prônent le respect de droits humains même en dehors des États de l'Union européenne. De plus, les approches divergentes des États entre eux ne sont pas le seul obstacle au traitement respectueux de l'ensemble des droits fondamentaux sur Internet. En effet, les acteurs numériques et, en particulier, les plateformes de réseaux sociaux ont adopté des dispositions sur les contenus illicites dans le cadre de conditions d'utilisations imposées à leurs utilisateurs. Ces dernières, crées et adoptées de façon unilatérale, peuvent comporter des dispositions qui ne convergent pas avec celles prévues par les autorités nationales.

2. Les différentes approches des plateformes

84. Après avoir analysé les différences d'approches des États, il est intéressant de s'intéresser aux plateformes des réseaux sociaux. En effet, ces dernières élaborent des lignes directrices et de « standards de communauté »[206] qui peuvent diverger des

[206] Les « standards » ou « standards de communauté » sont les règles que les plateformes intègrent dans leurs Conditions Générales d'Utilisation (CGU). Ces règles définissent les catégories de contenus dont la plateforme autorise la publication sur les pages de son site.

dispositions contenues dans les législations nationales. Au sein même du panorama des plateformes des réseaux sociaux ces règlementations changent[207] et chaque réseau social adopte ses propres règles et définitions.[208]Ainsi, comme décrit par le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, « les conditions d'utilisations sont souvent formulées d'une manière tellement générale qu'il peut être difficile de savoir à l'avance avec une certitude raisonnable quel contenu peut faire l'objet d'une restriction »[209]. Il faut toutefois souligner que les principales plateformes américaines – YouTube, Facebook et Twitter – ont développé et amélioré progressivement leurs règlementations en adoptent des définitions et mesures d'actions assez similaires[210].

85. Ces différentes approches entre les plateformes et les dispositions nationales soulèvent plusieurs problèmes : d'un côté, l'absence d'effacement des contenus qui devraient être considérés illicites et de l'autre côté, la sur-censure des contenus et le blocage des auteurs de ces derniers. Ce faisant se produisent des atteintes à la liberté d'expression[211] ou à d'autres droits fondamentaux. Un exemple qui vient élucider ces réflexions est la suppression, ou plutôt la censure, par Facebook d'une célèbre photo de Nick Ut représentant un groupe d'enfants près de Trang Bang fuyant un bombardement au

---

[207] Le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression pointait notamment les définitions divergentes sur le discours de haine. Certaines plateformes qui adoptaient des définitions précises, d'autres vagues ou tout simplement elles n'en adoptent pas. Voir le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, point 46.

[208] Pour consulter les standards de Facebook, voir : https://www.facebook.com/communitystandards/. Le réseau social Twitter les appelle quant à lui « Règles et politiques de Twitter ». Voir : https://help.twitter.com/fr/rules-and-policies#twitter-rules

[209] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Conseil des droits de l'Homme, 11 mai 2016, A/HRC/32/38, point 52. Disponible sur : https://www.undocs.org/fr/A/HRC/32/38.

[210] Voir le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, point 46. Disponible sur : https://documents-dds ny.un.org/doc/UNDOC/GEN/N19/308/14/PDF/N1930814.pdf?OpenElement

[211] Voir par exemple J. C. WONG, « Facebook Blocks Pulitzer-Winning Reporter over Malta Government Exposé », 19 mai 2017, *The Guardian*. Disponible sur : https://www.theguardian.com/world/2017/may/19/facebook-blocks-malta-journalist-joseph-muscat-panama-papers

napalm avant la fin de la guerre du Vietnam[212]. Cette suppression était causée par les politiques établies par Facebook sur la nudité. Ainsi, par le même motif, plusieurs tableaux ont été censurés comme le fameux tableau de Courbet « L'Origine du monde » représentant un sexe féminin, « La descente de Croix » de Rubens ou encore « La liberté guidant le peuple » de Delacroix. Ces décisions ont été abandonnées très vite par le réseau social qui a autorisé ensuite leur publication[213] face aux soulèvements de l'opinion publique et du milieu artistique.

86. D'autres exemples peuvent être ajoutés à cet argumentaire. En Allemagne, plusieurs affaires ont opposé Facebook à certains de ses utilisateurs. Les plaignants y contestaient la suppression par ce dernier de contenus qui étaient licites en application des lois allemandes, mais à propos desquels la plateforme avait choisi de faire primer ses propres standards pour les considérer comme étant illicites. Cependant, les juridictions allemandes, pour juger de la légitimité de ces suppressions, n'ont pas adopté le même positionnement. D'un côté, certains juges ont condamné la plateforme pour la suppression des contenus licites au regard de la loi allemande[214]. De l'autre côté, d'autres juges ont confirmé l'appréciation de Facebook et débouté les demandeurs. C'est le cas dans l'*affaire OLG Dresden* du 8 août 2018[215] où les juges allemandes ont estimé légitime la suppression par les modérateurs de Facebook de contenus qualifiés, selon les standards de communauté du réseau, de discours de haine. Ainsi que le blocage du compte de l'auteur de publications. Cela, alors que les contenus ne violaient pas les dispositions de la loi allemande[216]. Cette affaire montre une certaine autonomie des plateformes dans le choix de comportements à censurer. Il faut aussi souligner qu'en

---

[212] Voir P.F DOCQUIR, « Chapitre 2. - La confrontation entre droits fondamentaux et puissances privées vue à travers le prisme de la liberté d'expression » in C. DE TERWANGNE, et Q. VAN ENIS (dir.*), L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 75.
[213] Voir : M. UNTERSINGER et M. TUAL, « Après avoir censuré une photo de la guerre du Vietnam, Facebook fait machine arrière », *Le Monde*, 9 septembre 2016, disponible sur : https://www.lemonde.fr/pixels/article/2016/09/09/censure-le-plus-grand-journal-norvegien-attaque-facebook_4995029_4408996.html ; M.C avec l'AFP, « Facebook s'excuse après avoir censuré les seins nus de « La Liberté guidant le peuple » », *20 Minutes*, 19 mars 2018, disponible sur : https://www.20minutes.fr/high-tech/facebook/2239719-20180319-facebook-excuse-apres-avoir-censure-seins-nus-liberte-guidant-peuple
[214] *OLG München* du 28 août 2018.
[215] *OLG Dresden* du 8 août 2018.
[216] Voir W. ECHIKSON and O. KNODT, « Germany's NetzDG: A key test for combatting online hate », *CEPS Research Reports*, November 2018, No. 2018/09, p.11.

Allemagne certains choix opérés par les plateformes peuvent être adoptés au vu des obligations de la *Loi Netzwerkdurchsetzungsgesetz (*« *NetzDG* ») entrée en vigueur le 1er octobre 2017 et qui prévoit de sanctions pour les plateformes qui n'effacent pas des contenus manifestement illicites sous les 24h qui suivent le signalement par un ou plusieurs utilisateurs. Comme il a été souligné par le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression « les ambiguïtés de la réglementation étatique et les obligations onéreuses liées à la responsabilité des intermédiaires risquent d'entraîner un filtrage excessif »[217], toujours selon le Rapporteur « le filtrage fait dans un État peut avoir des effets sur l'expression numérique des utilisateurs d'autres États. Si les sociétés peuvent configurer des filtres qui ne s'appliquent qu'à un État ou à une région donnée, il est arrivé que ces filtres se propagent sur d'autres réseaux ou dans d'autres espaces de la plateforme »[218].

87. Ainsi, il faut ajouter que même parmi les modérateurs des réseaux sociaux il y a une différence d'appréciation et de jugement vis-à-vis d'un même contenu. Selon une enquête[219] de Propublica[220] qui a analysé plus de 900 messages, certaines décisions des modérateurs de Facebook étaient incohérentes. Propublica a ensuite choisi un échantillon de 49 publications envoyées par des utilisateurs qui estimaient que la décision prise par la plateforme était erronée et les a soumises à Facebook. Dans 22 cas Facebook a déclaré que ses modérateurs avaient fait une erreur, dans 19 cas la plateforme a défendu les jugements et dans les six derniers cas il a estimé qu'il s'agissait bien des contenus qui allaient à l'encontre des règles de Facebook mais soit les auteurs du signalement avaient mal signalé le contenu soit l'auteur l'avait supprimé. Les utilisateurs donc sont face à un

[217] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Conseil des droits de l'Homme, 11 mai 2016, A/HRC/32/38, point 47. Disponible sur : https://www.undocs.org/fr/A/HRC/32/38.

[218] *Ibid*. Le Rapporteur spécial mentionne notamment le filtrage demandé en 2013 par l'État indien et exécuté par Airtel India qui s'est étendu à un partenaire d'Airtel India, Omantel à Oman. Voir : Citizen Lab, « Routing gone wild: documenting upstream filtering in Oman via India » (2012).

[219] A. TOBIN, M. VARNER et J. ANGWIN, Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up, 28 décembre 2017. Disponible sur : https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes. Voir également Council of Europe, Steering Committee for Media and Information Society (CDMSI), Guidance note, Content Moderation, Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, adopted by the at its 19th plenary meeting, 19-21 May 2021, p. 17.

[220] Association américaine spécialisée en journalisme d'enquête d'intérêt public.

double problème, d'un côté, l'absence de modération pour des contenus illicites, de l'autre, la sur-censure pour des contenus licites.

88. La Commission interaméricaine des droits de l'Homme a fait observer que les acteurs privés n'ont pas the « ability to weigh rights and to interpret the law in accordance with freedom of speech and other human rights standards »[221]. C'est d'ailleurs pour cela que l'auto-régulation des plateformes, souvent menée par l'intelligence artificielle, et une augmentation de leurs responsabilités concernant l'effacement des contenus sont souvent décriées[222]. À cet égard, le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, après avoir attiré l'attention sur les défaillances des systèmes de tri automatique reposant sur l'intelligence artificielle[223], affirme que les entreprises privées si elles « veulent réellement protéger les droits fondamentaux de leurs utilisateurs, elles doivent fixer des règles claires et se fier au jugement d'humains »[224]. Il ajoute : « autrement dit, les modérateurs doivent pouvoir comprendre les codes du langage des utilisateurs, qui peut être employé pour dissimuler les appels à la violence, apprécier les intentions de l'auteur du message, prendre en compte la nature de cette

---

[221] La Commission interaméricaine des droits de l'Homme a fait observer que les acteurs privés « n'ont pas la capacité d'évaluer les droits et d'interpréter la loi en tenant dûment compte de la liberté d'expression et d'autres normes relatives aux droits de l'homme ». Voir Commission interaméricaine des droits de l'Homme, Freedom of Expression and the Internet, OEA/Ser.L/V/II. CIDH/RELE/INF, 11/13, 31 December, 2013, point 105, disponible sur https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf et citée par le Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Conseil des droits de l'Homme, 11 mai 2016, A/HRC/32/38, point 44. Disponible sur : https://www.undocs.org/fr/A/HRC/32/38.

[222] Voir notamment les débats en France sur la loi Avia ou encore les controverses sur l'efficacité de la loi allemande NetzDG traités au §453 de cette thèse. Voir Council of Europe, Steering Committee for Media and Information Society (CDMSI), Guidance note, Content Moderation, Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, adopted by the at its 19th plenary meeting, 19-21 May 2021, pp. 19-20. Voir P.-F Docquir, « Chapitre 2. - La confrontation entre droits fondamentaux et puissances privées vue à travers le prisme de la liberté d'expression » in C. DE TERWANGNE, et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, pp. 83-85.

[223] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, point 49. Voir également Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-treizième session, A/73/348 du 29 aout 2018.

[224] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, point 49.

personne et de son auditoire et évaluer les environnements dans lesquels les discours haineux peuvent mener à la violence »[225]. En somme, le traitement doit être fin, suivre des règles claires et la solution cohérente et justifiée.

89. Plusieurs points ont également été soulevés par le « Steering Committee for Media and Information Society » du Conseil de l'Europe sur la difficulté de la modération menée par les plateformes, notamment sur les conflits d'intérêts qui pouvaient se présenter lorsque les plateformes profitent de certains contenus illégaux et des réactions que ces derniers suscitent pour augmenter leurs profits[226].

90. Enfin, la difficulté se trouve également dans le manque de transparence concernant les moyens mis en place par les plateformes pour modérer les contenus illicites[227] ; ainsi que, concernant les décisions de retrait prises par les plateformes. Il y a un véritable besoin d'adopter une démarche transparente vis-à-vis des utilisateurs en ce qui concerne la suppression ou pas des contenus et le blocage des comptes des auteurs[228].

91. Il devrait donc y avoir plus de cohérence dans les définitions de règlements et dans le traitement des contenus pour permettre le respect de droits humains et ne pas atteindre

---

[225] *Ibid*, point 50.

[226] Council of Europe, Steering Committee for Media and Information Society (CDMSI), Guidance note, Content Moderation, Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, adopted by the at its 19th plenary meeting, 19-21 May 2021, pp.35-36. À cet égard, il est intéressant de souligner les révélations de la lanceuse d'alerte Frances Haugen en 2021 voir https://www.wsj.com/articles/the-facebook-files-11631713039.

[227] Voir notamment la décision du Tribunal judiciaire de Paris du 6 juillet 2021 qui oblige le réseau social Twitter à communiquer aux demandeurs (des associations) dans le délai de deux mois les informations concernant les moyens mises en place pour lutter contre la haine en ligne. Twitter doit notamment produire : « tout document administratif, contractuel, technique ou commercial relatif aux moyens matériels et humains mis en œuvre dans le cadre du service Twitter pour lutter contre la diffusion des infractions d'apologie de crimes contre l'humanité, l'incitation à la haine raciale, à la haine à l'égard de personnes [en] raison de leur sexe, de leur orientation ou identité sexuelle, l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que [l]es atteintes à la dignité humaine ».

[228] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, points 45 et 49. Disponible sur : https://documents-dds ny.un.org/doc/UNDOC/GEN/N19/308/14/PDF/N1930814.pdf?OpenElement. Voir également Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Conseil des droits de l'Homme, 11 mai 2016, A/HRC/32/38, point 89. Disponible sur : https://www.undocs.org/fr/A/HRC/32/38.

les droits des utilisateurs (qu'ils soient sur-censurés ou au contraire victimes de contenus illicites que les plateformes refusent d'effacer).

92. Après avoir vu que les comportements illicites peuvent s'exercer grâce à la dimension transnationale d'Internet. Il est intéressant de se pencher sur d'autres caractéristiques d'Internet qui exposent les utilisateurs aux atteintes à leurs droits fondamentaux.

Section II : L'appréciation d'Internet comme un lieu exposant les individus à des atteintes à leurs droits fondamentaux

93. D'autres caractéristiques d'Internet montrent qu'il s'agit d'un lieu où les atteintes aux droits fondamentaux sont fréquentes. Cela est causé par l'exposition étendue de la vie privée des utilisateurs, qu'elle soit volontaire ou involontaire. On constate que plusieurs atteintes aux droits fondamentaux constituent des cyberviolences et la naissance et l'évolution va de plus en plus vers l'incitation à l'exposition de la vie privée des utilisateurs. La conception de la vie privée et sa protection ont ainsi évolué dans le temps pour s'adapter aux nouvelles transformations mais il n'en reste pas moins qu'un individu en se connectant à Internet n'est pas à l'abri d'atteintes à sa vie privée et à ses données personnelles. Ainsi, outre à l'exposition massive de la vie privée, Internet permet également d'être « anonyme », ce qui comporte des avantages et des inconvénients. Si d'un côté, il assure aux agresseurs un sentiment d'impunité, de l'autre, il favorise la liberté d'expression de certains individus qui pourraient faire l'objet de poursuite ou menaces.

94. Au vu de ces éléments, il d'agira, d'une part, d'analyser l'atteinte aux droits fondamentaux à travers l'exposition de la vie privée des utilisateurs (**§I**) et, de l'autre part, d'étudier les risques et les avantages de l'anonymat (**§II**).

I. L'atteinte aux droits fondamentaux par l'exposition étendue de la vie privée de l'utilisateur

95. Internet et les réseaux sociaux sont devenus un lieu de partage de la vie privée soit de façon volontaire (par la publication de plein gré d'informations personnelles) soit involontaire (par le vol d'informations à caractère personnel). Plusieurs comportements illicites sur Internet mènent à une atteinte à la vie privée, par exemple : la violation des correspondances, la diffamation, le partage de contenus à caractère sexuel sans le consentement de la personne. Les cours européennes ont pu, à plusieurs reprises, s'exprimer sur ce sujet. La protection de la vie privée a, en effet, évoluée pendant ces dernières années (**A**) pour répondre à ces nouveaux risques et à ces nouvelles formes d'atteintes liées aux technologies de l'information et de la communication (**B**).

A. La protection évolutive du droit à la vie privée au vu des nouvelles atteintes sur Internet

96. Le droit à la vie privée est notamment inscrit à l'article 8, paragraphe 1, de la Convention européenne des droits de l'Homme, qui prévoit que : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».

97. Dans un premier temps la vie privée était vue comme la protection de l'intimité de l'individu contre les immixtions extérieures notamment les intrusions par l'État ou par d'autres individus (par exemple la presse), c'est ce qu'aux États-Unis on nomme « the right to be left alone » (le droit d'être laissé seul). De là ce droit à évolué pour devenir un droit à l'auto-détermination[229]. C'est d'ailleurs par un arrêt[230] récent que la Cour européenne des droits de l'Homme reconnaît le rattachement du droit à l'auto-détermination informationnelle au droit à la protection de la vie privée[231]. Il s'agit désormais « de donner à l'individu la mainmise sur son identité numérique »[232]. Ce droit

[229] K. BENYEKHLEF et P. TRUDEL, *État de droit et virtualité*, Les éditions Thémis, 2009, p. 204
[230] Cour EDH, 27 juin 2017, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, req. n° 931/13.
[231] Cour EDH, 27 juin 2017, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, req. n° 931/13, § 137. Voir C. DE TERWANGNE, « Internet et la protection de la vie privée et des données à caractère personnel », in Q. VAN ENIS et C. DE TERWANGNE, *L'Europe de droits de l'homme à l'heure d'Internet,* Bruyant, 2019, p. 330.
[232] B. TAXIL, « Internet et l'exercice de droits fondamentaux », in *Internet et le droit international*, Colloque de Rouen, SFDI, p. 120.

et sa protection sont depuis des années défiés par les nouvelles technologies, les réseaux sociaux, la création des nouveaux dispositifs GPS ou logiciels espions[233]. En outre, il est considéré comme un droit fondamental relatif[234] car sa protection doit être évaluée selon le contexte qui peut être perçu différemment selon les époques et les États. Aujourd'hui, Internet permet de toucher un public de plus en plus large donc si dans le passé, la publication dans la presse écrite pouvait toucher une nation, aujourd'hui l'information peut aller outre océan en un clic.

L'article 8 de la Convention européenne des droits de l'Homme ne décrit pas le droit à la vie privée ce qui rend le champ d'application assez large. Les contours de son application sont posés par la jurisprudence de la Cour européenne des droits de l'Homme et ses juges qui considèrent que la vie privée est un concept qui « ne se prête pas à une définition exhaustive »[235]. La notion de vie privée touche notamment l'intégrité physique de la personne mais aussi psychologique et morale[236] ; son identité physique et sociale, le droit au développement personnel, le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur[237]. Ainsi, selon la Cour, la garantie offerte par l'article 8 est destinée à assurer le développement de la personnalité de chaque individu dans les relations avec ses semblables[238], cela est très intéressant pour faire un lien avec les réseaux sociaux et les relations que ces derniers permettent de créer entre les individus. L'article 8 de la Convention s'apparente également à l'article 7 de la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») qui énonce que « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications »[239]. Les champs d'application sont les mêmes pour les deux articles

---

[233] « Les logiciels espions sont généralement définis, au sens large, comme des logiciels conçus pour recueillir les données d'un ordinateur ou d'un autre appareil et les transférer à un tiers sans que le propriétaire de l'ordinateur ne donne son accord ou n'en soit informé », pour plus d'informations voir : https://www.kaspersky.fr/resource-center/threats/spyware

[234] K. BENYEKHLEF et P. TRUDEL, *État de droit et virtualité*, Les éditions Thémis, 2009, p. 177.

[235] Cour EDH, 25 mars 1993, *Costello-Roberts c. Royaume-Uni*, req n° 13134/87, § 36.

[236] Cour EDH, 9 mars 2004, *Glass c. Royaume-Uni*, n° 61827/00, §70.

[237] F. PICOD et S. VAN DROOGHENBROECK, *Charte des droits fondamentaux de l'Union européenne*, commentaire article par article, Bruxelles, Bruylant, 2018, 14 p. Et les arrêts : Cour EDH, 16 décembre 2010, *A.B.C. c: Irlande*, req. 25579/05 ; Cour EDH, 20 juillet 2010, *Dadouch c. Malte*, req. 38816/07 ; Cour EDH, 29 avril 2002, *Pretty c. Royaume Uni*, req. 2346/02.

[238] Cour EDH, *Botta c. Italie* du 24 février 1998, 21439/93, § 32.

[239] Voir article 7 de la Charte des droits fondamentaux, voir également N. CARIAT, « Article 7 respect de la vie privée et familiale », in F. PICOD, C. RIZCALLAH, S. VAN DROOGHENBROECK, *Charte des droits*

afin d'assurer une cohérence entre les deux instruments et une protection effective de ce droit. De plus, l'article 17 du Pacte international relatif aux droits civils et politiques défend également le droit à la vie privée contre les immixtions arbitraires et illégales ; ainsi, il protège aussi contre les atteintes à l'honneur et à la réputation de l'individu. Dans l'arrêt *Copland c. Royaume-Uni* de la Cour européenne des droits de l'Homme, l'article 17 du Pacte et l'article 8 de la Convention ont pu etre invoqués « pour préciser que toute donnée transmise par Internet ou accessible par ce biais relève de la vie privée de l'individu, à moins qu'elle ne soit volontairement destinée à un accès public »[240]

98. Si, dans le passé, l'atteinte à la vie privée était surtout commise à travers la presse écrite ou les médias traditionnels, aujourd'hui le curseur s'est déplacé vers les réseaux sociaux et, plus généralement, les espaces d'expression en ligne (entre autres : les forums, les messageries, les blogs). Les textes ont dû, pour cela, s'adapter à ces nouveaux modes de diffusion. La Convention 108+, modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[241], inscrit le droit à la vie privée dans son article premier, ce qui montre l'importance de ce droit. Dans le rapport explicatif de cette dernière, le Conseil de l'Europe explique que, ouverte à la signature en 1981, elle devait être modernisée « pour mieux répondre aux nouveaux défis en matière de protection de la vie privée découlant de l'utilisation croissante des nouvelles technologies de l'information et de la communication, de la mondialisation des opérations de traitement et des flux toujours plus importants de données à caractère personnel »[242]. L'intrusion dans la vie privée est très forte lorsqu'il s'agit de violences sur Internet car il est plus simple de s'introduire dans la vie d'autrui

---

fondamentaux de l'Union européenne, Commentaire article par article, 2ème édition, Bruylant, 2020, pp. 185-210.

[240] Voir P. LAGRANGE, « Internet et l'évolution normative du Droit international : d'un Droit international applicable à l'internet à un DI du cyberespace ? », in *Internet et le droit international*, SFDI, Pedone, 2014, p. 70 qui cite l'arrêt Cour EDH, 3 juillet 2007, *Copland c. Royaume Uni*, n°62617/00.

[241] La Convention 108 est la première convention internationale juridiquement contraignante concernant le domaine de la protection des données. Ouverte à la signature en 1981 elle est modifiée en 2018. Voir : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0

[242] La modernisation de la Convention ouvre la voie à une question très important concernant le besoin ou pas de mettre à jour les instruments juridiques vu les avancées technologiques qui se transforment de plus en plus vite. L'exemple de la Convention 108 est assez positif car il s'agit d'une convention technologiquement neutre qui la rend un instrument ouvert et à vocation universelle. Voir Conseil de l'Europe, rapport explicatif du protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE 223, 10 octobre 2018. Disponible sur : https://rm.coe.int/16808ac91b

en ligne que hors ligne. Cela devient encore plus facile quand les victimes potentielles s'exposent elles-mêmes sur les réseaux sociaux en publiant leurs informations personnelles et en n'adoptant pas des mesures de sécurité efficaces pour accéder à leurs comptes. C'est le cas lorsqu'un utilisateur utilise un mot de passe très facile ou indique sa position GPS quand il publie une photo ou une vidéo, ce qui rend sa géolocalisation très aisée.

99. Enfin, la protection de la vie privée est souvent confondue avec la protection des données personnelles[243]. En droit de l'Union européenne, le droit à la protection des données personnelles est un droit fondamental inscrit à l'article 8 de la Charte des droits fondamentaux, ce qui marque une différence importante avec la Convention européenne des droits de l'Homme qui ne protège pas les données personnelles en tant que telles, mais uniquement la vie privée[244]. Cela est mentionné clairement dans la jurisprudence de la Cour de justice de l'Union européenne : « l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci qui n'a pas d'équivalent dans la CEDH »[245]. Selon la maîtresse de conférences Olivia Tambou, le droit au respect de la vie privée est conçu comme un droit-liberté qui comporte des obligations de ne pas faire. Au contraire le droit de la protection des données repose sur des obligations positives à mettre en place par les États membres [de l'Union européenne][246]. Elle poursuit en disant que ce dernier s'applique « indépendamment de l'existence ou non d'une ingérence dans la vie privée des individus »[247].

---

[243] Pour approfondir voir : C. DOCKSEY, « Chapitre 3 - Articles 7 and 8 of the EU Charter: two distinct fundamental rights » in A. GROSJEAN (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e edition, Bruxelles, Larcier, 2015, p. 71-97 et F. MOYSE, « Chapitre 4 - La protection des données personnelles entre droits de l'homme et droits fondamentaux » in A. GROSJEAN (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e édition, Bruxelles, Larcier, 2015, p. 99-113

[244] C. DOCKSEY, « Chapitre 3 - Articles 7 and 8 of the EU Charter: two distinct fundamental rights » in A. GROSJEAN (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1e edition, Bruxelles, Larcier, 2015, p. 74.

[245] CJUE, 21 décembre 2016, *Tele2 Sverige c. Post- och telestyrelsen*, aff. C-203/15, point 129.

[246] O. TAMBOU, « Chapitre 1. - Droit autonome du droit au respect de la vie privée », in *Manuel de droit européen de la protection des données à caractère personnel*, 1e édition, Bruxelles, Bruylant, 2020, p. 22.

[247] *Ibid.*

B. Les atteintes élargies à la vie privée sur Internet

100. On constate que « les contours juridiques de la vie privée numérique sont de plus en plus vagues et sa protection effective limitée »[248]. L'atteinte à la vie privée est une violation qui caractérise très souvent les cyberviolences. D'abord, l'utilisation des messageries comme Messenger, Whatsapp mais encore les courriers électroniques peuvent faire naître des risques d'atteintes à la vie privée. C'est ce que la Cour européenne des droits de l'Homme a observé dans son arrêt *Muscio c. Italie* qui concernait la réception sans le consentement de l'utilisateur de spams[249] dans sa boîte mail avec des images pornographiques. La Cour a établi que « la diffusion d'Internet et des systèmes d'échange de courriers électroniques a fait naître des possibilités de communication qui n'existaient pas auparavant. En même temps, une fois connectés au réseau Internet, les utilisateurs de ces systèmes ne jouissent plus d'une protection effective de leur vie privée, s'exposant à la réception de messages, images et informations souvent non sollicités »[250]. Au moment même de la connexion sur Internet les utilisateurs s'exposent aux cyberviolences.

101. Les atteintes à la vie privée peuvent se concrétiser également par la diffusion des contenus à caractère sexuel qui constituent une atteinte à l'intimité sexuelle de la personne car les contenus partagés comportent soit des images prises sans le consentement de la personne (par exemple lors des actes apparentés au voyeurisme digital), soit des images prises avec le consentement de la personne concernant la production du contenu mais non pas concernant leur diffusion. On peut d'ailleurs parler du concept de vie privée ou intimité sexuelle (« sexual privacy »), qui est défini par Danielle Citron comme un concept qui « involves the extent to which others have access to and information about people's naked bodies (notably the parts of the body associated with sex and gender); their sexual desires, fantasies, and thoughts; communications

[248] B. TAXIL, « Internet et l'exercice de droits fondamentaux », in *Internet et le droit international*, SFDI, Pedone, 2014, p. 120.
[249] Messages envoyés à plusieurs reprises sans le consentement de la personne qui les reçoit.
[250] Cour EDH, 13 novembre 2007, *Muscio c. Italie*, req. n° 31358/03, section B. appréciation de la Cour.

related to their sex, sexuality, and gender; and intimate activities […] »[251]. D. Citron considère cette intimité comme fondamentale pour la dignité humaine. Elle est vue comme la pierre angulaire de l'autonomie sexuelle et du consentement[252].

102. L'atteinte à la vie privée sur Internet peut se matérialiser par la violation de la correspondance de la victime, ce qui résulte notamment du piratage des appareils électroniques ou de la mise en place de logiciels espions. Cette question a notamment été étudiée par la Cour européenne des droits de l'Homme dans sa décision *Buturuga c. Roumanie*[253] où elle estime, pour la première fois, que « la cyberviolence est actuellement reconnue comme un aspect de la violence à l'encontre des femmes et des filles et peut se présenter sous diverses formes dont les violations informatiques de la vie privée, l'intrusion dans l'ordinateur de la victime et la prise, le partage et la manipulation des données et des images, y compris des données intimes »[254]. Cet arrêt est important car, pour la première fois, la Cour parle de « cyberviolence » et fait référence à plusieurs rapports sur les cyberviolences et à la définition retenue par le Comité de la Convention sur la cybercriminalité [255]. Toutefois, il n'est pas clair si les faits en l'espèce concernant les cyberviolences tombent, selon la Cour, dans le champ d'application de l'article 3 ou 8 de la Convention européenne des droits de l'Homme. Il semblerait *prima facie* que la Cour considère que les violences domestiques relèvent de l'article 3 et les cyberviolences de l'article 8[256]. Cela montrerait le lien entre les violences en ligne et l'atteinte à la vie privée. Cependant, limiter les cyberviolences à l'article 8 serait regrettable car elles touchent plusieurs infractions et non seulement la violation de la vie privée.

---

[251] D. K. CITRON, « Sexual Privacy », *128 Yale Law Journal 1870*, 2019, p. 1880.
[252] *Ibid*. pp. 1882 et suivantes.
[253] Cour EDH, 11 février 2020, *Buturuga c. Roumanie*, req. n° 56867/15.
[254] *Ibid.* §74.
[255] *Ibid.* §40. La définition de cyberviolence sera analysée dans le Titre II, Chapitre III de cette thèse.
[256] F. VAN LEEUWEN, « Cyberviolence, domestic abuse and lack of gender sensitive approach - Reflections on Buturuga v. Romania », *Strasbourg Observers*, 11 mars 2020. Disponible sur : https://strasbourgobservers.com/2020/03/11/cyberviolence-domestic-abuse-and-lack-of-a-gender-sensitive-approach-reflections-on-buturuga-versus-romania/

103. De plus, l'atteinte peut se matérialiser lors de l'envoi d'images à caractère sexuel non sollicitées à travers des infractions qui s'apparentent à l'exhibition sexuelle ou au harcèlement sexuel si l'envoi est répété. Très souvent ce sont les mineurs qui sont les plus exposés à ces types de violations[257]. À cet égard, la Cour européenne des droits de l'Homme a pu réaffirmer les obligations positives qu'ont les États afin de protéger les individus des violations contre leur intimité et notamment celle des mineurs. C'est le cas dans l'affaire *Söderman c. Suède*[258] où la Cour conclut à la violation de l'article 8 de la Convention européenne des droits de l'Homme car le droit suédois n'avait pas assuré le droit à la vie privée à une mineure. En effet, le beau-père de cette dernière avait tenté de la filmer à son insu dans son domicile à des fins sexuelles.

104. La diffamation peut aussi consister à dévoiler des informations de la vie privée d'un individu afin de nuire à sa réputation. La Cour européenne des droits de l'Homme a affirmé, à plusieurs reprises, que la protection de la réputation rentrait dans le champ d'application de l'article 8 de la Convention européenne des droits de l'Homme[259]. C'est en effet sur le fondement de l'article 8 que la Cour avait été saisie dans son arrêt *Tamiz c. Royaume-Uni.* En l'espèce, le requérant soutenait que le Royaume-Uni avait manqué à son obligation positive de protéger son droit au respect de sa réputation. En effet, l'État refusait de notifier une action à Google suite à la publication sur un blog géré par Google Inc. de commentaires que le requérant jugeait diffamatoires[260].

105. Une autre atteinte à la vie privée sur Internet est le « swatting », c'est-à-dire un canular téléphonique où une personne qui souhaite rester anonyme envoie d'urgence et inutilement les services de police chez la victime dont l'adresse a été dévoilée. Nous pouvons également ajouter le doxing, pratique qui consiste à rechercher et à divulguer

---

[257] ECPAT INTERNATIONAL, *Violence against children in cyberspace*, 2005. Disponible sur : https://www.ecpat.org/wp-content/uploads/legacy/Cyberspace_ENG_0.pdf, voir également ECPAT INTERNATIONAL, *Online child sexual exploitation*, disponible sur : https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf

[258] Cour EDH, GC, 12 novembre 2012, *Söderman c. Suède*, req n° 5786/08.

[259] Voir notamment Cour EDH, 19 mars 2019, *Høiness c. Norvège*, req. n° 43624/14, § 63, Cour EDH, GC, 29 mars 2016, *Bédat v. Switzerland*, req, n°56925/08, § 72.

[260] La Cour en l'espèce jugera que les juridictions internes avaient agi dans la limite de leur marge d'appréciation et avaient ménagé un juste équilibre entre le respect de la vie privée (art. 8) et le droit à la liberté d'expression (art. 10) – Cour EDH, 19 septembre 2017, *Tamiz c. Royaume Uni*, req. n° 3877/14, § 90.

les informations d'une personne sans son consentement. Enfin, l'usurpation d'identité qui constitue le vol et l'utilisation d'informations personnelles de la victime[261].

106. On constate ainsi que l'atteinte à la vie privée sur Internet est importante. C'est notamment grâce à ses caractéristiques que la vulnérabilité des utilisateurs et par conséquent le risque de cyberviolences augmentent.

II. Les risques et les avantages liés au droit à l'anonymat

107. L'anonymat[262] peut être considéré comme un facilitateur pour le partage des contenus illicites, notamment d'un point de vue sociologique. Selon Prince et Dalgliesh « un des facilitateurs clés du cyberharcèlement est le sentiment d'anonymat qu'offre Internet et les autres outils électroniques de communication »[263]. En effet, sur Internet tout internaute peut agir sous une fausse identité en créant un compte avec un pseudonyme, en usurpant l'identité de quelqu'un d'autre ou en utilisant des moyens technologiques pour ne pas se faire tracer et identifier. Selon Richard Donegan, l'anonymat permet à l'agresseur d'insulter plus facilement une victime sans voir sa réaction physique[264]. Ainsi, un autre danger de l'anonymat est celui de la « desindividuation »[265]. C'est-à-dire le sentiment ressenti par les utilisateurs d'Internet qui mène à la perte d'auto-conscience et de capacité d'appréciation et qui les encourage à être plus impulsifs et désinhibés surtout quand ils sont plusieurs à commettre un

---

[261] Ces infractions seront étudiées plus largement dans le chapitre II de cette thèse.

[262] Pour approfondir sur l'histoire de l'anonymat et la liberté d'expression voir : F. TREGUER, « Anonymat et chiffrement, composantes essentielles de la liberté de communication ». Q. VAN ENIS ET C. DE TERWANGNE. *L'Europe des droits de l'homme à l'heure d'Internet*, Bruylant, 2019.

[263] PRINCE et DALGLIESH, 2010, p.51 traduction libre, voir également C. BLAYA, « Le cyberharcèlement chez les jeunes », *Enfance*, 2018/3 N°3, p. 424.

[264] R. DONEGAN, « Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis », *Strategic Communication Elon University*, 2010. Donegan dit que « This anonymity makes it easier for the offender to strike blows against a victim without having to see the victim's physical response. The distancing effect that technological devices have on today's youth often leads them to say and do crueler things compared to what is typical in a traditional face-to-face bullying situation ».

[265] Voir L. FESTINGER, A. PEPITONE, et T. NEWCOMB, « Some consequences of de-individuation in a group », *The Journal of Abnormal and Social Psychology*, *47* (2, Suppl), 1952, 382–389. Voir également I. SAILLOT, « Psychopathologie implicite de l'anonymat sur Internet », *Les Cahiers Internationaux de Psychologie Sociale, Presses universitaires de Liège*, Numéro 106, 2015/2, pp. 193-207, M. BALFE, B. GALLAGHER et autres, « Internet Child Sex Offenders' Concerns about Online Security and their Use of Identity Protection Technologies: A Review », *Child Abuse Review*, 24(6), 2015. Voir également F. DI TANO, *Hate speech e comportamenti d'odio in rete: un'analisi comparatistica in prospettiva de iure condendo*, Thèse de doctorat, Alma Mater Studiorum – Università di Bologna, 2017, p.42.

comportement illicite (par exemple lors de raids numériques[266]). Depuis des années, surtout à la suite de campagnes de harcèlement, un débat s'est installé auprès de l'opinion publique, en France[267] et dans d'autres États[268], pour lever l'anonymat sur Internet afin de réduire les comportements illicites et l'impunité.

108. Toutefois, du point de vue juridique, l'anonymat ne garantit pas l'impunité des agresseurs. Pour analyser cette question, il est important d'étudier la définition de l'« anonymat » et son encadrement en droit (**A**). Ensuite, il sera intéressant de démontrer que l'exercice du droit à l'anonymat est souvent perçu comme l'une des principales causes de cyberviolences à limiter. Toutefois, si son encadrement limite les atteintes aux droits fondamentaux, sa levée constituerait une menace pour la protection d'autres droits humains (**B**).

A. La nécessité de distinguer anonymat et pseudonymat

109. Il n'existe pas une véritable définition juridique d'anonymat. Ce dernier a été défini par J-Ch. Saint-Pau comme « l'état dans lequel une personne se trouve ou non suivant qu'une règle de droit lui permet ou non de ne pas s'identifier dans ses relations avec autrui »[269]. Etienne Davio parle de deux attitudes vis-à-vis de l'anonymat, d'une part, une attitude passive « qui consiste à rester à l'écart des interactions sociales pour éviter

---

[266] Le « raid numérique » appelé également « harcèlement de meute » se définit comme des propos ou comportements imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles.

[267] Voir entre autres M. UNTERSINGER et D. LELOUP, « Hollande et le PS s'en prennent de nouveau à « l'anonymat sur Internet » » , *Le Monde*, 17 décembre 2013, disponible sur https://www.lemonde.fr/technologies/article/2013/12/17/hollande-et-le-ps-s-en-prennent-de-nouveau-a-l-anonymat-sur-Internet_4335593_651865.html et H. BAUDINO, « L'anonymat sur le web, un éternel marronnier politique », *L'observatoire*, 20 novembre 2020.

[268] Voir notamment A. SMITH, « Calls to end social media anonymat give plate-forme more power without actually fixing the problem, experts say », *Indipendent*, 14 juin 2021, disponible sur : https://www.independent.co.uk/life-style/gadgets-and-tech/euro-2020-racism-social-media-england-b1883969.html et H. KESVANI, « Abolishing online anonymity won't tackle the underlying problems of racist abuse », *The Guardian*, 15 juin 2021, disponible sur : https://www.theguardian.com/commentisfree/2021/jul/15/abolishing-online-anonymity-racist-abuse-id-verification

[269] Voir J-Ch. SAINT-PAU, *L'anonymat et le droit*, Thèse de doctorat, Bordeaux IV, 1998 cité par M. ZWOLINSKA, *Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international*, Thèse de doctorat, Université Nice Sophia Antipolis, 2015, p. 130.

de faire l'objet d'identifications »[270] et, d'autre part, une attitude active quand l'anonymat consiste « à ne pas être identifié alors qu'on agit »[271]. Il sépare également des catégories d'anonymat : l'anonymat de l'auteur de certains faits juridiques régis par des textes spéciaux (par exemple l'accouchement sous X), celui pour assurer la sauvegarde des intérêts des parties au contrat, ensuite l'anonymat pour assurer la liberté d'expression et, enfin, l'anonymat comme rempart de la vie privée[272]. Plus intéressante encore est l'analyse faite par le Dr. Graeme Horsman qui s'interesse spécifiquement au cyberespace. D'abord, il explique le concept de « perceived anonymity »[273] en le définissant ainsi : « although many online services do not claim to be anonymous, a failure to understand the underlying technology often encourages a user to believe they are acting anonymously, an issue believed to have contributed to a rising number of individuals who interact with online illegal material »[274]. Dans ce principe d'anonymat perçu, il y a également une idée d'impunité qui peut conduire à des comportements violents et désinhibés[275]. Ensuite, il distingue également deux autres catégories d'anonymat : l'« approved anonimity » ainsi que le « full anonimity »[276]. Le premier est un terme inventé par Horsman pour indiquer les « services, which despite maintaining the anonymity of a user utilizing a particular service, in terms of user-to-user, user identification information is securely maintained for a finite amount of time by the service provider »[277]. Ces informations sont stockées par les plateformes ou/et les fournisseurs de service et utilisées lors d'une violation des politiques d'utilisations ou

---

[270] E. DAVIO, « Anonymat et autonomie identitaire sur Internet », in *Droit des technologies de l'information*, sous la direction de Etienne Montero, CRID, Bruyant, 1999, p. 298.
[271] *Ibid.* p. 298.
[272] *Ibid.* pp. 300-303.
[273] G. HORSMAN, « The Challenges Surrounding the Regulation of Anonymous Communication Provision in the United Kingdom », *Computers & Security*, 2015, p. 3.
[274] *Ibid.* p. 3. Traduction de l'autrice : « bien que de nombreux services en ligne ne prétendent pas être anonymes, le fait de ne pas comprendre la technologie sous-jacente encourage souvent l'utilisateur à croire qu'il agit de manière anonyme, un problème qui aurait contribué à l'augmentation du nombre de personnes qui interagissent avec du matériel illégal en ligne ».
[275] Voir F. DI TANO, *Hate speech e comportamenti d'odio in rete: un'analisi comparatistica in prospettiva de iure condendo*, Thèse de doctorat, Alma Mater Studiorum – Università di Bologna, 2017, p. 222.
[276] G. HORSMAN, « The Challenges Surrounding the Regulation of Anonymous Communication Provision in the United Kingdom », *Computers & Security*, 2015, p. 3.
[277] *Ibid.* p. 3. Traduction de l'autrice : « des services qui, malgré le maintien de l'anonymat d'un utilisateur utilisant un service particulier, en termes d'utilisateur à utilisateur, les informations d'identification de l'utilisateur sont conservées de manière sécurisée pendant une durée limitée par le fournisseur de services ».

des standards de communauté[278]. En particulier, elles peuvent être communiquées aux autorités de police lors d'enquêtes criminelles. Enfin, le « full anonimity » utilisé par les personnes qui ont plus de compétences techniques, notamment avec l'utilisation de TOR[279] ou d'autres techniques (par exemple des services de proxies anonymes) qui assurent un anonymat total.

110. Après avoir cherché à définir l'anonymat, il faut ensuite se pencher sur la définition de « droit à l'anonymat » ou « droit au respect de l'anonymat ». Le droit à l'anonymat avait été consacré indirectement comme un outil indispensable pour les journalistes, mais il faudra attendre 1994 pour que le Conseil de l'Europe consacre la protection de la confidentialité des sources d'information utilisées par les journalistes[280]. Ce principe sera protégé ensuite par la jurisprudence de la Cour européenne des droits de l'Homme[281]. Ensuite, en 1995, ce droit a été étendu à tous les particuliers, d'abord aux États-Unis à commencer par l'État de l'Ohio sous le fondement du premier amendement[282] en faisant « de ce dernier l'une des modalités possibles de la liberté d'expression »[283], et plus tard en Europe[284].

111. La doctrine est partagée sur le droit à l'anonymat. En effet, pour certains auteurs, il ne peut pas « être légitimement considéré comme le droit à la non-identification totale »[285], alors que pour d'autres cela signifie que « toute personne physique est libre de

---

[278] Les standards de communauté sont les règles internes d'utilisation que la plateforme définit et qui sont acceptées par l'utilisateur afin d'accéder à la plateforme.
[279] Le TOR est un service de réseau mondial qui permet d'anonymiser l'origine des connexions. Il permet d'empêcher la localisation des appareils connectés ainsi que la traçabilité des recherches en ligne, pour plus d'informations voir : https://www.torproject.org/.
[280] Voir F. TRÉGUER, « Anonymat et chiffrement, composantes essentielles de la liberté de communication » in Q. VAN ENIS et C. De TERWANGNE, *L'Europe des droits de l'homme à l'heure d'Internet*, Bruylant, pp-301-302 et Comité des Ministres du Conseil de l'Europe, *Résolution n°2 sur « les libertés journalistiques et les droits de l'Homme »*, Rapp. tech. Prague.
[281] Voir notamment Cour EDH, GC, 27 mars 1996, *Goodwin contre Royaume-Uni*, n°17488/90.
[282] Cour suprême des États-Unis, 19 avril 1995, *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, voir F. TRÉGUER précité p. 303. Voir également G. RESTA, « Anonimato, responsabilità, identificazione: prospettive di diritto comparato », *Il diritto dell'informazione et dell'informatica*, Anno XXX, Fasc. 2 -2014, p. 177.
[283] E. E. DAVIO, « Anonymat et autonomie identitaire sur Internet », in *Droit des technologies de l'information*, sous la direction de Etienne Montero, CRID, Bruyant, 1999, p. 302.
[284] Voir notamment Cour EDH, 2 décembre 2008, *K.U. c. Finlande*, req. n° 2872/02, § 49.
[285] Voir M. ZWOLINSKA, *Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international*, Thèse de doctorat, Université Nice Sophia Antipolis, 2015, p. 130.

l'utilisation de son identité numérique et a notamment le droit de crypter cette identité à des fins de confidentialité et d'anonymat »[286]. Il s'agirait concrètement de « « brouiller » son identité sur Internet, que ce soit par l'usage d'un pseudonyme, par la rétention de certaines informations, par la multiplication d'adresses e-mail utilisées ou encore par des déclarations mensongères »[287]. Selon J-Ch. Saint-Pau, l'objet du droit au respect de l'anonymat est d'abord « l'anonymat de l'identité qui peut être préservé. Chacun dispose ainsi du pouvoir de s'opposer à la recherche ou à la divulgation, sans autorisation, de son identité »[288] et ensuite « l'anonymat de l'intimité que toute personne est en droit d'exiger »[289]. Selon la Cour européenne des droits de l'Homme, l'anonymat est un « moyen d'éviter les représailles ou l'attention non voulue », ainsi il est « de nature à favoriser grandement la libre circulation des informations et des idées, notamment sur Internet […] »[290]. Ce droit à l'anonymat est donc le corollaire d'autres droits comme celui à la protection de la vie privée, de l'intimité et de la liberté d'expression et communication.

112. Pour analyser la question de l'anonymat, il faut également parler du pséudonymat. En effet, le plus souvent, les utilisateurs d'Internet et des réseaux sociaux utilisent un pseudonyme, du grec ψευδώνυμος (pseudônumos) qui signifie faux nom[291]. L'utilisation d'un simple pseudonyme permet de ne pas dévoiler son identité, permet de s'exprimer plus librement et d'éviter le profilage et le ciblage de publicité ou d'autres techniques commerciales. Toutefois, ce dernier ne garantit pas à l'utilisateur la non traçabilité[292] et identification. Pour cela, Internet devrait être considéré plutôt comme un lieu de

---

[286] Voir M. ZWOLINSKA, *Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international*, Thèse de doctorat, Université Nice Sophia Antipolis, 2015, p. 131 qui cite le Groupe de travail TIC, « Déclaration des droits de l'homme numérique », *Livre blanc* d'A. Santini et d'A. Bensoussan, 20 nov. 2000, Mairie d'Issy-les-MoulineauX, p. 18.
[287] *Ibid.* p. 131 qui cite G. BELL, « Secret, lies & the possible perils of truthful technology », conférence prononcée dans le cadre du programme Lift de la Fing, 2008.
[288] J-Ch. SAINT-PAU, *L'anonymat et le droit*, Thèse de doctorat, Bordeaux IV, 1998, p. 518.
[289] *Ibid.*
[290] Cour EDH (GC), 16 juin 2015, *Delfi AS c. Estonie*, req. n° 64669/09 §147, voir plus récemment Cour EDH, 7 septembre 2021, *Camak c. Turquie*, req. n° 45016/18 §47.
[291] En droit français le pseudonyme est protégé contre l'usurpation (voir TGI. Paris, 5 juillet 1995) et l'utilisation comme marque (voir Cass. civ. 1ère, 19 février 1975).
[292] La traçabilité sur Internet est une trace virtuelle, enregistrée sous forme de données, que nous laissons lorsque nous utilisons Internet.

pséudonymisation que d'anonymisation[293]. En effet, la plupart des utilisateurs peuvent être tracés et retrouvés moyennant leur adresse IP[294] malgré l'utilisation d'un faux nom. L'article 4 (5) du Règlement général sur la protection des données définit la « pseudonymisation » comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[295]. L'utilisateur pourra être anonyme vis-à-vis des autres utilisateurs moyennant un pseudonyme mais il ne le sera pas pour les plateformes d'hébergement ou les autorités de police, sauf s'il utilise, comme mentionné plus haut, des techniques spécifiques (le TOR notamment). Il pourra donc être identifié et toutes ses actions pourront être répertoriées par le fournisseur d'accès. Au vu de ses éléments, sauf de cas très spécifiques, l'anonymat sur Internet n'existe pas.

113. En droit de l'Union européenne, la 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, connue sous le nom de directive e-commerce, précise qu'elle « ne peut pas empêcher l'utilisation anonyme de réseaux ouverts tels qu'Internet »[296].

---

[293] Voir notamment M. BALFE, B. GALLAGHER et autres, « Internet Child Sex Offenders' Concerns about Online Security and their Use of Identity Protection Technologies: A Review », *Child Abuse Review*, 2014, p. 4.

[294] L'adresse IP est le numéro d'identification de chaque appareil connecté à un réseau utilisant le protocole Internet.

[295] Article 4 (5) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[296] Considérant 14 de la 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. Le droit allemand prévoit une obligation pour les fournisseurs d'accès de garantir l'accès et le paiement des services de manière anonyme ou sous un pseudonyme selon le §13 (6) de la *Telemediengesetz* (Loi sur les télémédias) voir https://www.gesetze-im-Internet.de/tmg/ 13.html et G. RESTA, « Anonimato, responsabilità, identificazione: prospettive di diritto comparato », *Il diritto dell'informazione et dell'informatica*, Anno XXX, Fasc. 2 -2014, p. 181.

114. Le Comité des ministres du Conseil de l'Europe en 1999 s'exprimait en la faveur de l'utilisation de l'anonymat, en précisant que « l'accès et l'utilisation anonyme des services [...] constituent la meilleure protection de la vie privée »[297]. Cette utilisation est souhaitée et conseillée également par le Groupe international de travail sur la protection des données personnelles dans les télécommunications[298]. Ce dernier dans son Memorandum de Rome, document qui contient des orientations à destination des utilisateurs, fournisseurs ainsi que des autorités nationales, invite les États à introduire un droit à l'anonymat[299]. En outre, le Memorandum encourage, d'un côté, les plateformes de réseaux sociaux à donner la possibilité d'utiliser des pseudonymes[300] et, de l'autre, les utilisateurs à s'inscrire en utilisant un pseudonyme[301]. D'une manière analogue, au sein de l'Union européenne, le G29[302] incitait les fournisseurs de réseaux sociaux à permettre l'utilisation de pseudonymes aux utilisateurs et à garantir leur anonymat[303]. La défense de l'utilisation de pseudonymes et du droit à l'anonymat trouve son fondement dans le principe de la protection de la vie privée et de la liberté de communication. Selon Stefano Rodotà, l'anonymat est la précondition de la liberté de la manifestation de la pensée. En effet, selon lui c'est l'élément constitutif de la version

---

[297] Voir II, 3° de l'Annexe à la recommandation N° R (99) 5 du Comité des ministres du Conseil de l'Europe sur la protection de la vie privée sur Internet, du 23 février 1999 et L. PAILLER, « Chapitre 1 - La garantie du libre accès au réseau social par la vie privée sociale » in *Les réseaux sociaux sur Internet et le droit au respect de la vie privée*, 1e édition, Bruxelles, Larcier, 2012, p. 61.

[298] Également connu comme le « Groupe de Berlin » il été créé en 1983 à l'initiative de diverses autorités nationales chargées de la protection des données. Pour plus d'informations voir : https://edps.europa.eu/data-protection/data-protection/glossary/g_fr

[299] International Working Group on Data Protection in Telecommunications, *Report and guidance on privacy in social networks services* - « Rome Memorandum », adopté le 4 mars 2008 à Rome, p. 4. Disponible sur : https://www.gpdp.it/documents/10160/10704/1531476. Voir également L. PAILLER, « Chapitre 1 - La garantie du libre accès au réseau social par la vie privée sociale » in *Les réseaux sociaux sur Internet et le droit au respect de la vie privée*, 1e édition, Bruxelles, Larcier, 2012, pp. 60-64.

[300] *Ibid.* p. 5.

[301] *Ibid.* p. 7.

[302] Le Groupe de travail « Article 29 sur la protection des données (G29) » était le groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 (avant l'entrée en vigueur du Règlement Général sur la Protection des Données - RGPD). À partir de cette date il a été remplacé par le Comité européen de la protection des données. Pour plus d'informations voir : https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_fr

[303] Voir Groupe de travail « Article 29 » sur la protection des données, avis 5/2009 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009. Voir également L. PAILLER, « Chapitre 1 - La garantie du libre accès au réseau social par la vie privée sociale » in *Les réseaux sociaux sur Internet et le droit au respect de la vie privée*, 1e édition, Bruxelles, Larcier, 2012, p. 62 et G. RESTA, « Anonimato, responsabilità, identificazione: prospettive di diritto comparato », *Il diritto dell'informazione et dell'informatica*, Anno XXX, Fasc. 2 -2014, p. 180.

digitale de la citoyenneté[304]. L'anonymat est un allié de la liberté d'expression, en particulier, il permet aux citoyens, aux défenseurs des droits humains, aux ONG et aux membres de l'opposition de s'exprimer librement dans des pays où la parole est muselée.

115. Ce droit à l'anonymat a progressivement été consacré et encadré en Europe en essayant de respecter le droit à la vie privée des utilisateurs. Son encadrement a été bâti avec l'intention de permettre l'identification des personnes ayant commis de faits illicites afin de punir les agresseurs et protéger les victimes.

B. Un arsenal juridique à l'efficacité mitigée

116. Le droit à l'anonymat a été construit au niveau européen, d'un côté, en cherchant à respecter le droit au respect de la vie privée et de communication, et, de l'autre, en essayant de permettre l'identification d'une personne ayant commis un acte illicite. Le Comité des ministres du Conseil de l'Europe exprime ce souhait clairement dans sa Déclaration sur la liberté de communication du 28 mai 2003, « un équilibre doit être trouvé entre le respect de la volonté des usagers de l'Internet de ne pas divulguer leur identité et la nécessité pour les autorités chargées de l'application de la loi de retrouver la trace des responsables d'actes délictueux »[305].

117. Avant d'analyser la transmission d'informations par les plateformes aux autorités, il est important de parler de la conservation des données et de leur encadrement. Concernant les États de l'Union européenne, la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[306] prévoit que les données relatives aux communications électroniques

---

[304] Voir F. DI TANO, *Hate speech e comportamenti d'odio in rete: un'analisi comparatistica in prospettiva de iure condendo*, Thèse de doctorat, Alma Mater Studiorum – Università di Bologna, 2017, p. 45 qui cite S. RODOTÀ, *Il diritto di avere diritti*, 2012, Roma-Bari: Laterza, pp. 392 et suivantes. Ainsi que S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, 2014, Roma-Bari: Laterza, pp. 23 et suivantes.
[305] Comité des ministres du Conseil de l'Europe, Déclaration sur la liberté de la communication sur l'Internet, 28 mai 2003, 840e réunion des Délégués des Ministres du Conseil de l'Europe.
[306] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

doivent être effacées dès l'achèvement de la communication. Cependant, quatre ans après son adoption, ce principe avait connu une exception avec la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications[307]. Cette directive prévoyait une obligation pour les fournisseurs de service de communications téléphoniques ou électroniques de collecter et conserver les données de trafic et de localisation des communications. Ainsi, elle imposait aux États membres de garantir la conservation d'une série de données[308] pendant au minimum six mois et au maximum deux ans[309]. La directive ne prévoyait pas la conservation du contenu des échanges mais des informations plus techniques comme l'heure, le destinataire, et là où c'était possible, la durée ou la localisation. L'objectif était celui de garantir la conservation de ces données pour les besoins d'une éventuelle enquête. Toutefois, cette directive a été invalidée par la Cour de justice de l'Union européenne au motif qu'elle portait atteinte de manière disproportionné aux droits fondamentaux[310].

118. La directive e-commerce[311] prévoit à l'article 15-2 que « les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites allégués qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement »[312]. De plus, à l'article 12-3 la directive prévoit qu'une « juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, [a la possibilité] d'exiger du prestataire qu'il mette un

---

[307] Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE (JO L 105, p. 54).
[308] *Ibid.*, article 5.
[309] *Ibid.*, article 6.
[310] Voir CJUE, GC, 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a*, affaires jointes C-293/12 et C-594/12 ; ainsi que R. TINIÈRE, Commentaire de l'arrêt Digital Rights Ireland in F. PICOD, *Jurisprudence de la CJUE 2014 - Décisions et commentaires*, Collection Droit de l'Union Européenne, Bruylant, 2015, p. 90.
[311] 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.
[312] Article 12-3 de la directive n° 2000/31/CE du 8 juin 2000 relative au commerce électronique.

terme à une violation ou qu'il prévienne une violation »[313]. Cette disposition a été transposée en droit interne par les États de l'Union européenne[314]. En France, c'est la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (ci-après « loi LCEN »)[315] qui a transposé cette disposition, en particulier, l'article 6-III-2 qui prévoit que les éditeurs non professionnels ont la possibilité de rester anonymes mais ont l'obligation de communiquer leurs informations aux hébergeurs. En effet, la loi dispose que : « les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire […], *sous réserve de lui avoir communiqué les éléments d'identification personnelle* […] »[316]. Ainsi, l'article 6-II de la loi LCEN impose aux intermédiaires techniques une obligation de conserver les « données de nature à permettre l'identification de quiconque a contribué à la création d'un contenu ou de l'un des contenus des services dont elles sont prestataires »[317]. La loi LCEN s'applique donc aux fournisseurs d'accès et aux hébergeurs qui ont l'obligation de conserver pendant un an les données des utilisateurs et de les communiquer à l'autorité judiciaire en cas de requête. Elle concerne exclusivement les contenus accessibles au public, en effet les contenus échangés dans les messageries privées (entre autres : emails, Messenger, WhatsApp) sont régis par le Code des postes et des communications électroniques et en particulier l'article L 34-1-I. Depuis la loi du 23 janvier 2006 relative à la lutte contre le terrorisme[318], l'obligation de conservation des données vis-à-vis des fournisseurs d'hébergement et d'accès a été étendue à toute personne dont l'activité est d'offrir « une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre

[313] Article 12-3 de la directive n° 2000/31/CE du 8 juin 2000 relative au commerce électronique.
[314] La transposition a été assuré en droit italien par l'article 31 de la loi du 1er mars 2002 n°39, « Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2001 », publié à la Gazzetta Ufficiale n. 72 du 26 mars 2002. Disponible sur : https://www.camera.it/parlam/leggi/02039l.htm
[315] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, disponible sur : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/
[316] Article 6-III-2 de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, italique de l'autrice.
[317] *Ibid.* article 6-II.
[318] Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

gratuit »[319]. Plusieurs décrets ont ensuite encadré l'obligation de communication et de mise à disposition des données[320]. Ces données doivent être conservées pendant un an à partir du jour de la création des contenus, du jour de la résiliation du contrat ou de la fermeture du compte ou à compter de la date d'émission de la facture ou de l'opération de paiement[321]. Cette durée avait été prise en conformité de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, désormais abrogée. Pour le moment, la Cour de justice de l'Union européenne n'a pas donné des précisions concernant la durée maximale de conservation. Selon l'avis de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique[322], il faudrait « tirer les conséquences juridiques adéquates de l'arrêt de la Cour de justice de l'Union européenne *Digital Rights Ireland et Seitlinger* [arrêt qui a conduit à l'abrogation de la Directive 2002/58/CE] du 8 avril 2014 en limitant la durée de conservation des données techniques de connexion au strict nécessaire ainsi que l'étendue de l'accès donné à ces données aux autorités publiques »[323].

---

[319] Article L 34-1-II du Code des postes et des communications électroniques, voir également C. FÉRAL-SCHUHL, *Cyberdroit - Le droit à l'épreuve de l'Internet* 2020-2021, 02/2020, 8è édition, p. 290.

[320] Voir notamment le décret n° 2007-1538 du 26 octobre 2007 relatif aux demandes de mise à disposition de données par voie électronique et modifiant le code de procédure pénale qui prévoit une obligation de communication de données pour certains organismes publics et privés ; ainsi que le décret n° 2014-1162 du 9 octobre 2014 portant création d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires » et le décret d'application de la loi du 24 juillet 2015 relative au renseignement. Ainsi que le 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. Pour approfondir voir également C. FÉRAL-SCHUHL, *Cyberdroit - Le droit à l'épreuve de l'Internet* 2020-2021, 02/2020, 8è édition, pp. 290-291. Voir également G. GUIZIOU-PÉRONNE, *Les cyberdélits et le droit international privé*, Thèse de doctorat, Université Paris I Panthéon-Sorbonne, 2013, pp. 240-243.

[321] Article 3 du 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.

[322] Cette commission, crée par l'Assemblée nationale, est une instance mixte, composée par des parlementaires et des personnalités qualifiées, qui a été chargée de définir une doctrine et de principes durables et transversaux en matière de protection des droits et libertés à l'âge numérique. Pour plus d'informations voir : https://www2.assemblee-nationale.fr/14/autres-commissions/numerique/a-la-une/creation-de-la-commission-de-reflexion-et-de-propositions-sur-le-droit-et-les-libertes-a-l-age-du-numerique

[323] Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, *Numérique et libertés : un nouvel âge démocratique*, Rapp. N°3119 du 8 octobre 2015, recommandation n°76.

119. Les fournisseurs de services et les plateformes sont ainsi les garants du droit à l'anonymat pour les utilisateurs et sont soumis à l'obligation de donner accès aux autorités judiciaires aux données personnelles[324] sous peine de sanction[325]. Cependant, l'efficacité de la transmission est à apprécier avec nuance. En effet, le problème lié au droit à l'anonymat, mis à part la dimension sociologique étudiée au début de cette réflexion, serait plutôt à trouver dans le partage d'informations entre les plateformes des réseaux sociaux et les autorités ou dans le traitement des comportements illicites. Un exemple illustrant ce propos est celui en France de *l'affaire Mila*. En l'espèce, la jeune Mila avait proféré des propos insultants sur l'Islam sur le réseau Instagram et, à la suite de cette première vidéo, elle a été victime de cyberharcèlement et de plusieurs raids numériques. Après une première enquête, une personne a été condamnée pour menace de mort et de viol. Ensuite, Mila s'exprime à nouveau dans une deuxième vidéo pour répondre aux menaces qu'elle reçoit. Après cela, elle sera à nouveau victime de cyberharcèlement et de raids numériques. À cet égard, une autre enquête est ouverte et treize personnes ont été interpellées et en juin 2021 onze de ces dernières ont été condamnées à des peines de quatre à six mois de prison avec sursis. Or, il faut souligner que Mila avait reçu, selon son avocat, plus de 100 000 messages insultants, de menaces de mort et de viol, ce qui montre que seulement une faible partie des agresseurs a été punie. La transmission de l'information est souvent empêchée par les acteurs du web, ce qui fragilise le recours des victimes pour découvrir l'identité des auteurs de publications illicites et ainsi faire retirer les contenus et les sanctionner. En effet, les plateformes ne collaborent pas toujours avec les autorités, par exemple elles refusent de transmettre les informations demandées pour poursuivre les enquêtes. Cela a été évoqué par la jurisprudence, un exemple est celui de l'arrêt du 6 juillet 2021 dans lequel le tribunal d'instance de Paris a contraint le réseau Twitter à partager les informations sur des contenus et des utilisateurs à deux associations qui estimaient que Twitter n'avait pas modéré un certain nombre de contenus illicites[326]. Cette décision a ensuite était confirmé

[324] Voir par exemple l'ordonnance du 4 avril 2013 par le président du Tribunal de grande instance de Paris qui a enjoint à Twitter de communiquer les données relatives à l'identification d'une personne ayant été à l'origine de la création d'un faux profil Twitter usurpant l'identité d'un tiers.
[325] Un an d'emprisonnement et 75 000 euros d'amende selon l'article 6-VI-2 de la loi LCEN.
[326] TJ Paris, 6 juill. 2021, n° 20/53181.

par la Cour d'appel[327] et la Cour de cassation[328]. Il n'est pas rare que les avocats des victimes ainsi que les associations se plaignent de la réticence des hébergeurs à diffuser les informations nécessaires[329].

120. De son côté, la Cour européenne des droits de l'Homme a créé une obligation positive pour les États parties à la Convention européenne des droits de l'Homme visant à garantir l'identification de personnes ayant commis des comportements illicites sur Internet. En effet, par son arrêt *KU c. Finlande*[330], la Cour condamne l'État finlandais pour ne pas avoir prévu des dispositions en droit interne qui permettent d'identifier un individu qui avait commis une infraction sur Internet. La Cour applique *mutatis mutandis* au domaine de la cybercriminalité sur Internet les principes consacrés dans l'arrêt *M.C. c. Bulgarie*[331]. L'obligation positive des États, qui relève de l'article 8 de la Convention européenne des droits de l'Homme, les oblige à adopter des dispositions qui sanctionnent les infractions contre la personne, y compris les tentatives et de renforcer l'effet dissuasif de l'incrimination[332]. En l'espèce, la Cour considère que si la confidentialité des communications est essentielle ainsi que la liberté d'expression, ces dernières ne peuvent pas être absolues face à des comportements illicites comme la pédocriminalité[333]. Cette même logique se retrouve dans les infractions au droit d'auteur. En effet, la directive 2004/48/CE, du 29 avril 2004, du Parlement européen et du Conseil relative au respect des droits de propriété intellectuelle[334] a harmonisé les procédures d'identification des internautes. Elle permet « aux ayants droit [par son article 8] d'obtenir, par voie d'injonction judiciaire, l'identification des abonnés dont l'adresse IP a été relevée sur les

[327] CA Paris, 20 janv. 2022, n° 21/14325.
[328] Cass., 23 mars 2023, n° 22-13.600.
[329] Voir C. BERTRAND, « Tout comprendre au débat sur l'anonymat sur Internet », *Les Echos*, 20 juillet 2020, disponible sur : https://www.lesechos.fr/tech-medias/hightech/tout-comprendre-au-debat-sur-lanonymat-sur-Internet-1224872
[330] Cour EDH, 2 décembre 2008, *K.U c. Finlande*, req. n° 2872/02, §49.
[331] Cour EDH, 4 décembre 2003, *M.C. c. Bulgarie*, req. n° 39272/98.
[332] Voir Cour EDH, 4 décembre 2003, *M.C. c. Bulgarie*, n° 39272/98, § 150 et Cour EDH, 2 décembre 2008, *K.U c. Finlande*, n° 2872/02, §43 et §46.
[333] Voir S. TURGIS, « La coexistence d'Internet et des médias traditionnels sous l'angle de la Convention européenne des droits de l'homme », *RTDH* 2013, nr. 93, p. 19.
[334] Voir article 8 de la directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle.

réseaux peer-to-peer où s'échangent sans autorisation des œuvres artistiques protégées par le droit d'auteur »[335].

121. Aux États-Unis, malgré la protection étendue de la liberté d'expression et du droit à l'anonymat[336], il a été affirmé par la jurisprudence qu'obtenir par un fournisseur d'accès à Internet les coordonnées de l'auteur anonyme ayant tenu des propos diffamatoires sur un Forum ne porte pas atteinte au premier amendement[337]. L'anonymat de l'auteur, toutefois, peut être protégé après une condamnation civile lorsque les contenus litigieux ont été supprimés[338].

122. L'anonymat permet aux utilisateurs de se sentir protégés par l'écran, en particulier, à travers un sentiment d'impunité. Cependant, il ne faut pas le voir ce droit comme la principale cause à laquelle s'attaquer pour lutter contre les cyberviolences. En effet, d'un côté, il s'agit le plus souvent d'un pseudonymat. Et de l'autre, l'encadrement qui est fait du droit à l'anonymat limite sa dangerosité, en particulier les dispositions en vigueur qui permettent aux plateformes numériques d'obtenir les informations des utilisateurs ayant un pseudonyme et de les communiquer aux autorités en cas d'enquêtes. Ainsi, il faut souligner que les agresseurs ne se cachent pas tous derrière un pseudonyme. Pour cela, faire de l'anonymat un bouc émissaire et s'attaquer à ce droit pour faire diminuer les cyberviolences n'est pas très efficace à long terme. Surtout, cela peut être dangereux pour la protection d'autres droits fondamentaux comme le droit à la vie privée et la liberté d'expression.

Comme souligné précédemment, la difficulté n'est pas tant dans l'identification des personnes, mais dans la transmission de l'information par les plateformes et dans l'analyse des milliers de messages haineux passibles des sanctions.

---

[335] Voir F. TRÉGUER précité, p. 310. F. TRÉGUER, « Anonymat et chiffrement, composantes essentielles de la liberté de communication » in Q. VAN ENIS et C. DE TERWANGNE, *L'Europe des droits de l'homme à l'heure d'Internet*, Bruylant, p. 310

[336] Voir notamment *Talley v. California*, *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), *Watchtower Bible & Tract Soc'y of New York, Inc. v. Vill. Of Stratton*, 536 U.S. 150 (2002), *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010).

[337] Cour Suprême de l'État de Virginie, *AOL c./Nam tai Electronics* du 1er novembre 2002.

[338] Voir notamment Cour d'appel américaine du 6ème circuit, *Signature Management Team, LLC v. Doe*, No. 16-2188 (6th Cir. 2017), à cet égard voir G. CRIQUI-BARHALAIS, *La protection des libertés individuelles sur le réseau Internet*, Université Paris II Panthéon Assas, Thèse de doctorat, 2018, note p. 279.

Conclusion du Chapitre I

123. La caractérisation des cyberviolences demeure complexe à cause des spécificités du cyberespace. En effet, Internet est un lieu d'archivage et d'oubli relatif où le traitement des comportements illicites peut être fragilisé par la dimension transnationale de ces derniers. De plus, par l'exposition de soi et la publication d'informations personnelles, les utilisateurs sont exposés au risque accru d'atteinte à leur vie privée. D'autant plus qu'Internet et les réseaux sociaux permettent de se cacher derrière l'anonymat et le pseudonymat qui donne aux potentiels agresseurs un sentiment d'impunité facilitant l'exécution de violences en ligne.

Chapitre II : L'amplification : caractéristique des comportements illicites sur Internet et danger pour les droits fondamentaux

124. Nous pouvons parler de l'amplification des comportements illicites à travers l'utilisation d'appareils de communication et d'information. En effet, depuis plusieurs années, l'utilisation d'Internet s'intensifie et ce dernier est perçu comme un espace de sociabilité, dans lequel les utilisateurs s'expriment pour partager, entre autres, leurs émotions. Selon Haydée Popper-Gurassa, dans cet espace « tout ou chacun peut se déterminer comme il le souhaite et croire ou non à ce qu'il voit »[339]. Internet est devenu ces dernières décennies un espace de plus en plus complexe et riche de contenus.

125. Dans les développements précédents, nous avons analysé le lien de causalité entre certaines caractéristiques d'Internet et l'exécution des comportements illicites. Or, dans les développements qui vont suivre, il s'agira d'étudier plus en détail le phénomène de l'amplification et les caractéristiques d'Internet qui rendent ce dernier un moyen pour la diffusion des contenus illicites. D'une part, il conviendra d'examiner les caractéristiques d'Internet qui facilitent l'amplification des cyberviolences (**Section I**) et, d'autre part, il s'agira d'analyser les conséquences de l'amplification vis-à-vis des comportements illicites (**Section II**).

Section I : L'identification des caractéristiques d'Internet comme facilitatrices de l'amplification des cyberviolences

126. Internet permet aux contenus, illicites ou non, d'être diffusés massivement en ligne. Cela se traduit par le phénomène de la viralité. Si dans les développements qui ont précédé nous avons focalisé notre analyse sur les caractéristiques qui facilitent l'exécution des violences en ligne. Il s'agira dans les développements qui vont suivre d'étudier les caractéristiques techniques qui conduisent à la viralité, en particulier les composantes techniques d'Internet (**§I**) et l'impossible maîtrise des contenus publiés (**§II**).

[339] P. HAYDÉE, « De l'idéal virtuel à l'autre réel », *Dialogue*, 2009/4 (n° 186), p. 75-86.

I. Les causes « techniques » de la viralité amplifiant les comportements illicites en ligne

127. Avant d'analyser les conséquences de la viralité, il faut d'abord chercher à la définir. T. Beavisage et d'autres chercheurs[340] ont passé en revue un certain nombre de travaux analysant les phénomènes de viralité sur Internet[341]. De cette analyse il a été observé que trois démarches se distinguent pour analyser ces phénomènes. D'abord, une approche temporelle qui étudie la temporalité de la diffusion des contenus et qui relève que la viralité correspond à la *concentration temporelle* de l'attention sur un contenu donné. Ensuite, une deuxième approche identifie les mécanismes de circulation des contenus ; dans ce cas, la notion de viralité prend une signification différente et concerne l'identification qui contribue à focaliser l'attention sur certains contenus. Enfin, une troisième démarche étudie comment les réseaux sociaux influencent la diffusion des contenus et cherche à expliciter les mécanismes de contagion d'un individu à l'autre. À cet égard, la viralité est définie comme « un ensemble de transmissions directes d'un individu à un autre, sur un réseau social préexistant »[342]. Cette analyse démontre qu'il est difficile d'identifier la viralité pure, qui est définie comme « la transmission directe d'un contenu entre deux individus, sans autre médiation »[343].

La viralité se base avant tout sur le contenu. L'objet du contenu peut être informatif, symbolique ou émotionnel. C'est cette dernière dimension émotionnelle qui facilite la diffusion[344] et ce principe n'est pas typique d'Internet. En effet, comme le rappelle Pierre Morelli, « la recherche de l'émotion est […] parfaitement maîtrisée par les grands

---

[340] T. BEAUVISAGE, J-S. BEUSCART (et autres), « Le succès sur Internet repose-t-il sur la contagion ? Une analyse des recherches sur la viralité », 21/2011, Tracés. *Revue de Sciences humaines*, p. 151-166.
[341] Entre autres : Katz et Lazarsfeld, 2008 et Coleman *et al.*, 1966
[342] T. BEAUVISAGE, J-S. BEUSCART (et autres), « Le succès sur Internet repose-t-il sur la contagion ? Une analyse des recherches sur la viralité », 21/2011, Tracés. *Revue de Sciences humaines*, p. 151-166.
[343] *Ibid*. point 27.
[344] P. MORELLI, *La viralité entre métaphore communicationnelle et approche esthétique*, Madarat, n°29-30. Dialogue des révolutions : la viralité, 2017, p. 276.

médias dans la conception de leurs programmes »[345]. Il est important ici de s'intéresser en particulier à la viralité dans sa dimension temporelle ainsi que spatiale.

128. Certains outils d'Internet permettent une large diffusion des contenus, c'est le cas des mots-dièse « hashtags » (**A**) qui permettent d'organiser les discussions en ligne sur un sujet donné, mais également des « bots » (**B**), agents autonomes capables de diffuser une information massivement. Enfin, un lien est recherché également entre la viralité et les « bulles de filtres » (**C**) sélections algorithmiques qui peuvent alimenter la haine en ligne et la diffusion de comportements illicites.

A. La contribution des mots-dièse (hashtags) au phénomène de la viralité

129. D'abord, il est intéressant de parler de l'utilisation de hashtags, c'est-à-dire l'utilisation de mots précédées par le symbole dièse (#). Ces mots peuvent être inventés, reprendre le nom ou prénom d'une personne, d'une ville ou autre encore. Les Hashtags organisent les discussions autour d'un sujet spécifique ou un évènement[346]. Leur utilisation permet de retrouver un contenu sur un réseau social par une recherche par mots clés et être une façon d'exprimer de la solidarité[347], de la colère ou d'autres émotions sur un évènement ou un contenu donné. Les exemples de viralité liés à un # sont multiples : #MeToo contre les violences sexuelles ou #JeSuisCharlie en soutien aux victimes de l'attentat de Charlie Hebdo[348]. Il peut s'agir aussi d'évènements plus futiles, par exemple l'utilisation du #Messi du nom du joueur espagnol lors de compétitions sportives ou encore d'un nom d'une ville lorsqu'il y a des évènements, importants ou pas, qui s'y passent. À posteriori, l'utilisation des hashtags est utile pour mesurer

---

[345] *Ibid*. point 276.
[346] L. FITTON, M. GRUEN, and L. POSTON, *Twitter for dummies*, Hoboken, NJ: John Wiley & Sons, 2009, p. 127.
[347] M. NISBETH BRØGGER, K. L. NIELBO and A. FAGE-BUTLER, *#detkuhaværetmig How twitter enabled the expression and propagation of solidarity among healthcare professionals*, Conjunctions: transdisciplinary journal of cultural participation, vol. 8, no. 1, 2021. DOI: 10.7146/TJCP.V8I1.123040, p. 6 qui cite Ince et al., 2017; Margolin & Liao, 2018; Narayan, 2013.
[348] Il s'agit d'une attaque terroriste islamiste contre le journal satirique Charlie Hebdo qui a eu lieu dans les locaux du journal à Paris le 7 janvier 2015. Le slogan et le hashtag « JeSuisCharlie » est utilisé pour soutenir le droit à la liberté d'expression.

l'impact d'un contenu ou d'un évènement et pour retrouver des informations sur le contenu reporté par l'hashtag. Ils sont aussi utiles pour identifier les profils des groupes d'utilisateurs qui s'expriment et pour identifier les sujets contemporains[349].

130. Les mots-dièse produisent une concentration temporelle de l'attention des utilisateurs sur un contenu donné et aident à sa diffusion massive (image, information ou commentaire). Sur Twitter, par exemple, les hashtags peuvent également influencer le débat car les utilisateurs en regardant quels # sont dans les « trending topics »[350] sont en quelque manière invités à s'exprimer sur le sujet et à augmenter la volume des contenus. La force des mots-dièse est qu'ils peuvent être créés et diffusés par tout le monde, qu'il s'agisse d'un utilisateur « connu » (c'est-à-dire suivi par un nombre conséquent d'utilisateurs) ou « inconnu ». Cela peut être un avantage pour mettre en lumière des causes peu connues, notamment pour dénoncer des violations des droits humains mais également un désavantage lorsqu'ils sont utilisés pour diffuser des fausses informations de façon massive. À cet égard, les hashtags ont pu aider les réseaux terroristes à diffuser leur propagande, par exemple l'État islamique a, à plusieurs reprises, détourné des hashtags pour faire connaître leurs vidéos de propagande djihadiste, cela a été le cas lors de la coupe du monde de football de 2014 via les #WC2014 ou #Brazil2014[351].

131. L'utilisation des mots-dièse est normalement faite par des individus mais ces derniers peuvent également être diffusés largement par des « bots ». Il est intéressant d'approfondir ce point pour comprendre les conséquences de l'utilisation de programmes informatiques autonomes sur le partage massif d'informations.

---

[349] C. RATHNAYAKE and W. BUENTE, *Incidental Effects of Automated Retweeting: An Exploratory Network Perspective on Bot Activity During Sri Lanka's Presidential Election in 2015*, Bulletin of Science, Technology & Society 1–9, 2017.

[350] Les trending topics ou « TT » ce sont des sujets de tendance sur Twitter affiché sur le réseau social qui peuvent durer plusieurs heures voir jours. Il s'agit des Hashtags les plus utilisés qui génèrent le plus d'interactions.

[351] M. HECKER, *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015, p. 17.

B. L'utilisation malveillante des bots

132. La viralité est également caractérisée par l'utilisation de « bots », des programmes informatiques autonomes capables de comprendre et d'agir sur Internet. Les bots peuvent être considérés comme des agents positifs d'Internet mais également négatifs. En effet, certains chercheurs[352] ont identifié des qualités propres aux bots comme le fait de générer un grand volume de tweets bénins[353]. D'autres[354] y voient également des instruments pour minimiser le cyberharcèlement. Il s'agit ici de « blockbots » des bots autonomes développés pour aider les utilisateurs à se protéger contre les cyberviolences. En même temps, certains bots sont utilisés à des fins malveillantes, par exemple pour répandre des spams[355] et partager une influence négative, comme le relatent Chamil Rathnayake and Wayne Buente : « bots have been employed to fulfill political objectives such as smear an opponent (Ratkiewicz et al., 2011), embarrass a political candidate (Oremus, 2012), and drown out political dissent (Thomas, Grier, & Paxson, 2012). Bessi and Ferrara (2016) presented evidence on the adverse effects of bots during the 2016 U.S. presidential election »[356]. En effet, les bots ont, à plusieurs reprises, été utilisés en période électorale. Un exemple est celui de l'élection présidentielle au Sri Lanka en 2015 dans laquelle un bot, et un en particulier appelé « Siripalabot », a largement partagé des contenus ayant l'hashtag #PresPollSL utilisé dans les conversations politiques en ligne pour faciliter les débats et l'échange d'informations durant la période électorale.

---

[352] Z. CHU, S. GIANVECCHIO, H. WANG and S. JAJODIA, *Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?*, IEEE Transactions on Dependable and Secure Computing, November 2012.
[353] *Ibid.* p. 2.
[354] R. Stuart GEIGER, *Bot-based collective blocklists in Twitter: the counter public moderation of harassment in a networked public space*, Information, Communication & Society, 19:6, 787-803, 2016 DOI: 10.1080/1369118X.2016.1153700.
[355] Un SPAM c'est un envoi répété et en grand nombre sans le consentement du destinataire, il peut s'agir, par exemple, de contenus commerciaux. Voir : Z. CHU, S. GIANVECCHIO, H. WANG and S. JAJODIA, *Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?*, IEEE Transactions on Dependable and Secure Computing, November 2012, p. 2.
[356] C. RATHNAYAKE and W. BUENTE, *Incidental Effects of Automated Retweeting: An Exploratory Network Perspective on Bot Activity During Sri Lanka's Presidential Election in 2015*, Bulletin of Science, Technology & Society 1–9, 2017, p. 2. Traduction de l'autrice : « Les bots ont été employés pour atteindre des objectifs politiques tels que le dénigrement d'un adversaire (Ratkiewicz et al., 2011), l'embarras d'un candidat politique (Oremus, 2012) et l'étouffement de la dissidence politique (Thomas, Grier et Paxson, 2012). Bessi et Ferrara (2016) ont présenté des preuves des effets négatifs des bots lors de l'élection présidentielle américaine de 2016 ».

Selon une étude qui a analysé les effets de l'utilisation de retweets[357] automatiques[358], le Siripalabot était « more powerful than other human or organizational actors, and it makes content of less powerful actors available to a wider group »[359]. Ainsi, cela a pu montrer le rôle que les bots jouent pendant les élections. Dans le cas d'espèce, le bot partageait des contenus des deux candidats en lice sans faire de préférence, mais le plus intéressant est qu'il a diffusé surtout des contenus publiés par des utilisateurs inconnus en leur donnant une certaine visibilité. Un autre exemple est celui des bots crées et utilisés pour influencer les votes pendant le referendum sur le futur du Royaume-Uni au sein de l'Union européenne (« Brexit ») en 2016 et, comme évoqué par Bessi et Ferrara, un an plus tard pendant la campagne présidentielle aux États-Unis. Ces deux temps forts ont été marqués par des publicités et une propagande ciblée sur la base de données personnelles touchant des millions d'utilisateurs de Facebook dont les données avaient été volées ou acquises sans donner une explication de leur utilisation[360]. Cette influence est causée par des acteurs gouvernementaux mais également privés. Ce phénomène s'appelle « Cyberturfing » et il est défini par Mark Leiser comme « the practice by state actors and commercial entities using digitally mediated platforms to facilitate a commercial benefit or to advance a political objective »[361]. Ce dernier est possible non seulement à travers des bots mais également des êtres humains à l'aide notamment des Hashtags[362]. Des actions d'astroturfing ont été enregistrées pendant les élections aux États-Unis et la Brexit, mais aussi ailleurs comme par exemple lors de campagnes réalisées par la société civile japonaise pro nucléaire et financées par les groupes

[357] Un retweet est une fonctionnalité de Twitter qui consiste à repartager un contenu déjà publié. Sur Facebook cette action existe également mais sous le nom de « Partage ».
[358] C. RATHNAYAKE and W. BUENTE, *Incidental Effects of Automated Retweeting: An Exploratory Network Perspective on Bot Activity During Sri Lanka's Presidential Election in 2015*, Bulletin of Science, Technology & Society 1–9, 2017.
[359] *Ibid.* p. 8. Traduction de l'autrice : « plus puissant que d'autres acteurs humains ou organisationnels, et il rend[ait] le contenu d'acteurs moins puissants accessible à un groupe plus large ».
[360] Cette campagne ciblée a été menée par Cambridge Analytica ainsi que par AggregateIQ, deux sociétés de technologies numériques qui ont désormais fermé leurs portes au vu du scandale qui a suivi les déclarations des lanceurs d'alertes qui ont signalé l'utilisation abusive des données personnelles pour influencer les votes. Voir pour plus d'informations : The Globe and mail, *Cambridge Analytica, AggregateIQ and the Facebook scandal: A guide to who's accused of what*, 5 avril 2018. Disponible sur : https://www.theglobeandmail.com/world/article-what-is-cambridge-analytica-and-what-did-it-do-a-guide/
[361] M. LEISER, *AstroTurfing,'CyberTurfing' and other online persuasion campaigns*, European Journal of Law and Technology, 2016, vol. 7, n° 1, p. 1.
[362] *Ibid*. p. 2.

nucléaires[363]. Mais encore, d'autres campagnes ont été suspectées, comme celle menée, d'après une enquête du New York Times, par les autorités chinoises sur Twitter pendant la pandémie de Covid-19 pour acclamer la bonne gestion de la crise par le gouvernement chinois[364].

133. Pour conclure, les bots ont une grande facilité à partager et créer du contenu, ce qui permet une plus large diffusion de l'information et, le cas échéant, de contenus illicites. Contrairement aux êtres humains, ils peuvent être actifs 24h sur 24h et continuer à publier des contenus en augmentant leur viralité.

C. Le risque de « bulles de filtre » amplifiant de réseaux de haine

134. Après avoir analysé l'utilisation de Hashtags et bots, il est intéressant d'étudier les « bulles de filtres ». Théorisées par Eli Pariser[365], activiste, les « filter bubbles » correspondent aux sélections algorithmiques proposées par les moteurs de recherche et les réseaux sociaux, sur la base de recherches et choix personnalisés émis par l'utilisateur lui-même, qui mènent à une sorte d'isolation intellectuelle. Selon Eli Pariser, cela créerait une bulle où l'utilisateur visualise seulement des contenus qui lui conviennent. Selon Pariser les individus ne sont pas confrontés à des idées et opinions qui diffèrent de la leur. Par exemple, un électeur de gauche sera exposé principalement à des contenus de gauche. Il sera également amené dans ses recherches sur les moteurs de recherche à voir des contenus différents d'un autre utilisateur, par exemple de droite, pour des mêmes mots clés. En pratique, il explique que si un électeur de gauche cherche sur Google le terme « BP » il aura probablement des informations sur la marée noire dans le Golfe du Mexique alors qu'un électeur de droite aura comme résultat les informations qui

---

[363] T. WEISS, *Japan's 'pro-nuclear civil society': Power in the analysis of social capital and civil society*, Journal of Civil Society, vol. 15, no 4, 26 septembre 2019, point 3.1, p. 4.
[364] Voir R. ZHONG, A. KROLIK, P. MOZUR et R. BERGMAN, *Behind China's Twitter Campaign, a Murky Supporting Chorus*, The New York Times, 8 juin 2020. Disponible sur : https://www.nytimes.com/2020/06/08/technology/china-twitter-disinformation.html
[365] E. PARISER, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin, 2012. Voir aussi TED, *Eli Pariser nous met en garde contre les « bulles de filtres » en ligne*, mars 2011. Disponible sur : https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=fr

concernent les investissements dans la British Petroleum. La même chose se répéterait également sur les réseaux sociaux, par exemple les algorithmes de Facebook proposeraient à l'utilisateur que des contenus qui lui plaisent. Pariser, plutôt à gauche politiquement, avait mis en avant que les contenus de ses amis conservateurs avaient disparu de son mur[366] Facebook. Selon Eli Pariser, ces caractéristiques permettent d'entrainer une polarisation des idées des utilisateurs et de les enfermer dans leurs croyances.

135. Toutefois, les recherches de cet activiste américain ont été fortement critiquées à plusieurs reprises par d'autres experts. En effet, selon différentes études il n'est pas démontré que les bulles de filtres existent et puissent avoir ces effets sur les utilisateurs[367]. D'abord, le chercheur Richard Fletcher, qui a mené une étude sur les bulles de filtres, met en avant plusieurs conclusions. Premièrement, dans son étude comparée concernant plusieurs États, il analyse par quels moyens les individus s'informent et montre que selon des pourcentages différents ces derniers s'informent en particulier au moyen de la télévision et Internet (y compris les réseaux sociaux). Concernant Internet, un tiers des utilisateurs se rend directement sur les sites des organes d'informations mais les deux autres tiers utilisent une « side door » c'est-à-dire une recherche générique sur les moteurs de recherche ou sur les réseaux sociaux. Dans ce cas, la recherche et les résultats associés peuvent être influencés par les algorithmes. Ensuite, il continue en reportant que, selon une étude[368], deux types de personnalisation peuvent se distinguer : la « self-selected personalisation » où les individus choisissent par eux-mêmes les contenus qu'ils souhaitent visualiser/lire et la « pre-selected personalisation » qui est faite par les algorithmes à l'insu des individus. Or, selon Fletcher les médias sociaux combinent ces deux types de personnalisation et exposent

---

[366] « Mur » ou « Journal » définissent le lieu où les informations sont concentrées.

[367] Dr. R. FLETCHER, The truth behind filter bubbles: Bursting some myths, Reuters Institute, disponible sur : https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths, voir également F. J. ZUIDERVEEN BORGESIUS, D. TRILLING, J. MÖLLER, B. BODÓ, C. H DE VREESE, N. HELBERGER, *Should we worry about filter bubbles?*. Internet Policy Review, 5(1), 2016. Voir aussi E. NECHUSHTAI and S.C LEWIS, *What kind of news gatekeepers do we want machines to be? Filter bubbles, fragmentation, and the normative dimensions of algorithmic recommendations*, Computers in Human Behavior, 2018 ainsi que E. BAKSHY, S. MESSING, L. A. ADAMIC, *Exposure to ideologically diverse news and opinion on Facebook*, Science, Vol 348, Issue 6239, 5 Jun 2015, pp. 1130-1132.

[368] F. J. ZUIDERVEEN BORGESIUS, D. TRILLING, J. MÖLLER, B. BODÓ, C. H DE VREESE, N. HELBERGER, *Should we worry about filter bubbles?*, Internet Policy Review, 5(1), 2016.

les utilisateurs à différentes sources d'information et notamment à plus de sources, comparé aux individus qui n'utilisent pas les médias sociaux, cela même de façon accidentelle lorsque les utilisateurs ne sont pas intéressés par l'information. Mais rien ne semble démontrer que les informations les enferment dans leurs croyances (courants politiques, religion ou autre). Dans le cas des moteurs de recherche, le chercheur démontre[369] que, lorsqu'un individu recherche une information dans un moteur de recherche, la sélection des contenus proposée est faite par des algorithmes basés lors de son utilisation passée. Selon Fletcher, les personnes qui utilisent les moteurs de recherche pour s'informer ont accès en moyenne à plus de sources d'information, par rapport à ceux qui ne le font pas, et sont susceptibles d'utiliser des sources de gauche et de droite[370].

136. Selon une autre étude[371] qui a comparé les résultats des recherches des individus républicains et démocrates aux États-Unis, la solution est similaire aux conclusions de Fletcher car elle démontre que les résultats qui s'affichaient étaient plus au moins les mêmes pour les votants de gauche et de droite. En accord avec l'argumentation de Fletcher et de l'auteur Axel Bruns[372], il ne faudrait pas s'attaquer aux bulles de filtres sans regarder les causes profondes derrière la polarisation de la société. Ce phénomène doit être étudié comme l'une des composantes d'Internet qui peut avoir une certaine influence mais sans pour autant être à l'origine de la haine sur Internet.

137. Après avoir clarifié ces points, on peut constater qu'à minima une personnalisation est faite sur les réseaux sociaux qu'elle soit volontaire (« self-selected personalisation ») ou involontaire (« pre-selected personalisation »). En effet, même en acceptant l'inexistence des bulles de filtres, il est certain que les réseaux sociaux et d'autres

---

[369] R. FLETCHER and R. KLEIS NIELSEN, *Automated Serendipity*, Digital Journalism, 6:8, 976-989, 2018.
[370] Par exemple "In the UK and Germany, people that use search engines for news have news repertoires with a 3:1 ratio between sources from their preferred side of the spectrum and sources from the other side. For people that do not use search engines, the ratio is 6:1. However, in Spain and the US the difference between these two groups is much smaller » voir R. FLETCHER and R. KLEIS NIELSEN, *Automated Serendipity*, Digital Journalism, 6:8, p. 984, 2018.
[371] E. NECHUSHTAI and S.C LEWIS, *What kind of news gatekeepers do we want machines to be? Filter bubbles, fragmentation, and the normative dimensions of algorithmic recommendations*, Computers in Human Behavior, 2018.
[372] A. BRUNS, *Are filter Bubbles real?*, Polity, 2019.

plateformes, telles que YouTube, utilisent des logiciels de recommandation qui suggèrent, sur la base de ces activités précédentes, des contenus intéressants pour l'utilisateur. Ce point est important dans l'amplification, car certains utilisateurs peuvent être amenés à avoir accès à des informations qui augmentent leur engagement et leurs croyances. Ainsi, cela peut devenir dangereux quand les informations reçues alimentent la haine à l'égard d'un ou plusieurs groupes définis qui peut se concrétiser avec des comportements illicites, en ligne ou hors ligne. Par exemple, concernant le recrutement terroriste, il a été démontré que sur Facebook si un utilisateur commence à montrer de l'intérêt par des contenus de l'État Islamique (ci-après « EI »), il sera facile pour lui d'avoir accès à d'autres contenus sur la propagande de l'EI et sur les moyens de se rendre en Syrie[373]. Ces mécanismes facilitent également l'élargissement d'autres communautés comme celle des QAnons[374], désormais banni par plusieurs réseaux sociaux comme Facebook[375] et Twitter[376].

138. Après avoir analysé ces caractéristiques d'Internet, il convient également d'analyser l'absence de maîtrise des contenus publiés sur Internet qui alimente la viralité.

II. L'impossible maîtrise des contenus publiés sur Internet amplifiant les atteintes aux droits fondamentaux

139. La maîtrise des contenus sur Internet est une question à ne pas sous-estimer. La maîtrise, ou plutôt l'absence de maîtrise, est une spécificité d'Internet, en effet, en ligne il est facile de perdre le contrôle d'un contenu publié. Qu'est-ce qu'il faut entendre

---

[373] M. HECKER, *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015, p. 24 qui cite notamment G. KRISTANADJAJA, *Comment Facebook m'a mis sur la voie du jihad, L'OBS avec* Rue 89, 21 octobre 2014.

[374] R. HARFOUSH définit QAnon comme « un mouvement conspirationniste américain d'extrême droite qui a combiné plusieurs théories du complot populaires (nouvel ordre mondial, État profond, réseaux de trafic d'enfants, etc.) en un récit spécifique centré sur une bataille biblique entre l'ancien président américain Donald Trump et une cabale mondiale de pédophiles sataniques qui dirigeraient le monde en secret », voir : R. HARFOUSH, *QAnon, la culture numérique et les élections françaises*, CNAMM, juin 2021, pp. 2-3.

[375] J. LAUSSON, *QAnon est désormais systématiquement banni de Facebook, qu'importe ce qui est publié*, Numerama, 7 octobre 2020. Disponible sur : https://www.numerama.com/tech/655774-qanon-est-desormais-systematiquement-banni-de-facebook-quimporte-ce-qui-est-publie.html

[376] *Twitter supprime 70 000 comptes liés à la mouvance conspirationniste pro-Trump QAnon*, France Info, 12 janvier 2021. Disponible sur : https://www.francetvinfo.fr/monde/usa/presidentielle/donald-trump/twitter-supprime-70-000-comptes-lies-a-la-mouvance-conspirationniste-pro-trump-qanon_4254175.html

comme « maîtrise » ? La maîtrise d'un contenu est ici entendue comme le fait de pouvoir publier un contenu (texte, photo ou vidéo) sur Internet ou sur un ou plusieurs réseaux sociaux, de pouvoir le modifier, l'effacer de ces espaces et contrôler son utilisation par les autres utilisateurs.

140. L'absence de maîtrise des contenus se situe d'abord dans la difficulté de l'auteur de faire disparaître un contenu après sa publication (**A**). Ensuite, dans la difficulté de maîtriser des contenus déjà retirés car estimés illicites mais qui apparaissent à nouveau sur internet (**B**).

A. L'impossible maîtrise des contenus illicites publiés

141. La difficulté liée à la maîtrise des contenus se situe dans le contrôle que l'utilisateur a du contenu une fois publié. En effet, après la publication un contenu peut être réutilisé par un ou plusieurs internautes sans la permission de l'auteur initial, cela notamment avec la sauvegarde du contenu par le téléchargement ou bien à travers les captures d'écran (qui permettent la fixation et la reproduction d'un contenu donné). Pour cela, même lorsque l'auteur du contenu et supprime sa publication, cette dernière sera bien sûr supprimée sur son compte mais il est possible qu'elle soit encore présente ailleurs (dans le même réseau social ou dans un autre). Un exemple est celui de la publication de photos intimes sans le consentement de la personne qui y est représentée. Un individu A peut avoir publié une photo de B sur Facebook sans son consentement et une personne C peut avoir fait une capture d'écran de cette photo et l'avoir partagée sur Facebook ainsi que sur Instagram. Si A décide de la supprimer sur Facebook, cette photo sera toujours en circulation car publiée par C sur d'autres réseaux sociaux. Ce risque avait été souligné par la Chambre de la Cour européenne des droits de l'Homme dans l'arrêt *Delfi AS c. Estonie* dans laquelle elle avait considéré que les contenus publiés sur Internet pouvaient continuer à circuler indéfiniment[377]. Dans le même arrêt, la Cour relevait également que « la facilité, l'ampleur et la vitesse avec lesquelles les informations sont diffusées sur Internet, et leur *caractère persistant après leur publication sur ce média*, […] peuvent

[377] Cour EDH, 10 octobre 2013, *Delfi AS c. Estonie*, req. n° 64569/09, § 92.

considérablement aggraver les effets des propos illicites circulant sur Internet par rapport à ceux diffusés dans les médias classiques »[378].

142. Or, il peut s'ajouter à cette rediffusion un autre problème, c'est-à-dire le fait que la victime ignore que le contenu est encore présent en ligne. En reprenant l'exemple précité, B ne sera probablement pas au courant de la nouvelle publication, ce qui pourrait compliquer les poursuites légales ou tout simplement laisser l'auteur de la rediffusion illicite impuni.

B. La réapparition et rediffusion des contenus illicites déjà effacés

143. L'absence de maîtrise se manifeste également après que la suppression d'un contenu jugé contraire au droit ou aux règles de plateformes. Il s'agit ici d'aborder la question de la réapparition des contenus illicites déjà retirés. La Cour de justice de l'Union européenne avait d'ailleurs reconnu ce risque en relevant qu'« [é]tant donné qu'un réseau social facilite la transmission rapide des informations stockées par l'hébergeur entre ses différents utilisateurs, *il existe un risque réel de voir une information ayant été qualifiée d'illicite être ultérieurement reproduite et partagée par un autre utilisateur de ce réseau »*[379].

144. Concernant la réapparition des contenus déjà qualifiés d'illicites, en France le projet de loi Avia prévoyait dans son article 4 (III) 2 bis que :

> « III. – Le Conseil supérieur de l'audiovisuel encourage les opérateurs mentionnés aux premier et deuxième alinéas du I de l'article 6-2 de la loi n° 2004-575 du 21 juin 2004 précitée à mettre en œuvre :
>
> […]

[378] Cour EDH, 10 octobre 2013, *Delfi AS c. Estonie*, req. n° 64569/09, § 147 (italique de l'autrice), voir N. DE BACKER, *Le principe de proportionnalité à l'épreuve de la liberté d'expression numérique*, JEDH, 2019/4, p. 257.
[379] CJUE, 3 octobre 2019, *Glawischnig-Piesczek v. Facebook Ireland*, aff. C-18/18, point 36. Italique par l'autrice.

« 2° bis Des outils de coopération dans la lutte contre la rediffusion massive de contenus, en particulier de vidéos ou d'images, identiques ou spécifiquement équivalents à ceux retirés en application de l'article 6-2 ; ».

145. Cependant, comme la majeure partie du projet de loi, le Conseil Constitutionnel a déclaré cet article non conforme à la Constitution[380]. Or, ce n'était pas la première fois que cette question de la réapparition des contenus illicites était soulevée. La CNCDH, par exemple, dans son Avis sur la lutte contre les discours de haine en ligne, de la même façon que l'article 4, (III), 2 bis, recommandait qu'une autorité administrative indépendante puisse disposer « du pouvoir d'imposer à tout prestataire d'[…] empêcher la réapparition ou la duplication [d'un contenu jugé illicite][381]. Dans une étude du Conseil d'État sur le numérique et les droits fondamentaux, il y a également une proposition qui va dans ce sens et qui énonce qu'il faudrait « prévoir une obligation pour les hébergeurs et les plateformes d'empêcher, durant un délai déterminé, la réapparition des contenus ayant fait précédemment l'objet de retrait. Cette obligation serait prononcée par l'autorité administrative »[382]. Mireille Imbert-Quaretta, conseillère d'État, parlait en 2014 d'une « injonction de retrait prolongé » pour mettre fin aux réapparitions des atteintes aux droits d'auteur. Elle proposait « de confier à l'autorité administrative la possibilité d'enjoindre à un site de communication au public en ligne de faire cesser et de prévenir, pendant une durée déterminée, la réapparition de contenus qui lui ont été signalés comme constituant une atteinte aux droits d'auteur ou aux droits voisins sur le site »[383]. Dans son argumentaire, la conseillère d'État, invoquait la licéité de cette injonction vis-à-vis du droit de l'Union européenne et notamment par le biais de l'article

---

[380] Voir le texte provisoire adopté par le Conseil constitutionnel, p. 11 qui montre en détail les suppressions faites par le Conseil. Disponible sur : https://www.assemblee-nationale.fr/dyn/15/textes/l15t0419_texte-adopte-provisoire.pdf. Ainsi que la décision n° 2020-801 DC du 18 juin 2020, disponible ici : https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2020801dc/2020801dc.pdf

[381] CNCDH, Recommandation n°14, *Avis sur la lutte contre les discours de haine en ligne*, 12 février 2015, p. 38. Disponible sur : https://www.cncdh.fr/sites/default/files/15.02.12_avis_lutte_discours_de_haine_internet_cncdh_0.pdf

[382] Conseil d'État, Proposition n°28, *Le numérique et les droits fondamentaux*, Le rapports du Conseil d'État (ancienne collection Étude et documents du Conseil d'État), 9 septembre 2014, p. 344. Disponible sur : https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux

[383] M. IMBERT-QUARETTA, *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne*, Rapport à Madame la ministre de la culture et de la communication, mai 2014, p. 16.

14, paragraphe 3, de la directive e-commerce qui prévoit « qu'une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, [exige] du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation »[384]. Ainsi l'article prévoit également que les États membres ont la possibilité : « d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible »[385]. Toutefois, et comme le rappelle Mme Imbert-Quaretta en évacuant rapidement la question, l'article 15, paragraphe 1, de la même directive interdit aux États membres d'imposer aux hébergeurs « une obligation générale de surveiller les informations » stockées[386]. La Cour de justice de l'Union européenne avait, à plusieurs reprises, refusé une surveillance *ex ante* des contenus potentiellement illicites en se fondant sur cet article 15[387]. Ce principe a toutefois été atténué par la même Cour dans son l'arrêt *Glawischnig-Piesczek c. Facebook Ireland*[388] où, en répondant à une question préjudicielle formulée par la Cour suprême autrichienne, elle établit qu'il est possible pour une juridiction d'un État membre, sans violer l'article 15 de la directive, d' « enjoindre à un hébergeur de supprimer les informations qu'il stocke et dont le contenu est *identique* à celui d'une information déclarée illicite précédemment ou de bloquer l'accès à celles-ci, quel que soit l'auteur de la demande de stockage de ces informations »[389]. Elle ajoute ensuite qu'il est également possible de faire supprimer un contenu *équivalent.* Elle s'exprime premièrement en posant la définition des termes « informations de contenu équivalent » c'est-à-dire « des informations véhiculant un message dont le contenu reste, en substance, inchangé et, dès lors, diverge très peu de celui ayant donné lieu au constat d'illicéité »[390]. Ensuite, en précisant que les différences de formulation du contenu équivalent par rapport au contenu déjà déclaré illicite « ne

---

[384] Article 14, paragraphe 3, de la 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.
[385] *Ibid.*
[386] Article 15, paragraphe 1, de la 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.
[387] Voir notamment CJUE, 24 Novembre 2011, *Scarlet v. SABAM*, aff. C-70/10, point 40 ainsi que CJUE, 16 février, 2012, *SABAM v. Netlog NV*, aff. C-360/10, points 34, 37 et 38. Voir également M. C. KETTEMANN, *Follow-up to the Comparative Study on Blocking Filtering and Take-down of Illegal Internet Content* (Country Report for Germany 2016-2019) (Strassburg: Europarat, 2019), mai 2019, p. 5. Disponible sur : https://rm.coe.int/dgi-2019-update-chapter-germany-study-on-blocking-and-filtering/168097ac51.
[388] CJUE, 3 octobre 2019, *Glawischnig-Piesczek v. Facebook Ireland*, aff. C-18/18.
[389] *Ibid.* point 37. Italique par l'autrice.
[390] *Ibid.* point 39.

doivent pas, en tout état de cause, être de nature à contraindre l'hébergeur concerné à procéder à une appréciation autonome dudit contenu »[391].

146. La Cour de justice précise enfin l'application territoriale de ces dispositions. En particulier, elle précise qu'en vertu de l'article 19, paragraphe 1, de la directive il n'y a aucune limitation territoriale des mesures prises par les États membres[392] et, pour cela, les mesures d'injonction peuvent avoir une portée mondiale[393]. Elle établit donc qu'il est possible « d'enjoindre à un hébergeur de supprimer les informations visées par l'injonction ou de bloquer l'accès à celles-ci au niveau mondial, dans le cadre du droit international pertinent »[394]. Cela suppose que la question de la territorialité se situe en dehors du champ d'application matériel du droit de l'Union européenne. Il est donc possible d'estimer qu'une juridiction nationale puisse demander la suppression d'un contenu publié dans un autre État. La Cour parvient à cette conclusion, sans instituer à la charge de l'hébergeur une obligation de surveiller, de manière générale, les informations qu'il stocke, ni une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites, conformément à l'article 15 de la directive précitée.

147. Cette décision a naturellement suscité de vives critiques, notamment vis-à-vis des possibles atteints à la liberté d'expression. Selon l'association Article 19, cette décision menace la liberté d'expression, en particulier, selon son directeur exécutif Thomas Hughes, la Cour n'a pas pris en compte les limites de la technologie en matière de filtres automatiques. En effet, la suppression automatique de contenus pourra porter atteinte à la liberté d'expression et limiter le droit à l'information[395]. Il met également en garde sur la portée territoriale de l'arrêt qui pourrait mener un tribunal national d'un État membre à ordonner la suppression d'un contenu qui ne serait pas illégal dans un autre État. Cette

---

[391] *Ibid.* point 45.
[392] *Ibid.* point 49.
[393] *Ibid.* point 50.
[394] À ce sujet l'interprétation de la Cour semble être favorable à une approche mondiale de la mesure, approche qu'elle n'avait pas adopté quelques jours avant dans sa décision concernant la portée territoriale du droit au déréférencement CJUE, GC, *Google LLC c/ CNIL* du 24 septembre 2019, aff. C-507/17. Voir à ce sujet le Chapitre I – Section I - §I de cette thèse.
[395] Voir Article 19, *CJEU judgment in Facebook Ireland case is threat to online free speech*, 3 October 2019. Disponible sur https://www.article19.org/resources/cjeu-judgment-in-facebook-ireland-case-is-threat-to-online-free-speech/

décision a naturellement été critiquée également par l'un des principaux intéressés, Facebook, qui par l'un de ses porte-paroles a fait savoir que « Ce jugement soulève d'importantes questions en matière de liberté d'expression et concernant le rôle que doivent jouer les entreprises d'Internet dans la surveillance, l'interprétation et la suppression de messages illégaux » en ajoutant qu'il « […] sape le principe ancien selon lequel un pays n'a pas le droit d'imposer ses lois à d'autres pays. […] »[396]. Ce qui est sûr c'est que la Cour ne mentionne jamais la liberté d'expression dans son affaire et que les États membres devront mettre en balance l'atteinte aux droits individuels par la publication de contenus considérés illicites et la liberté d'expression.

148. En somme, si la conclusion prise par la Cour de justice semble aller dans le sens de la protection des libertés individuelles, beaucoup de détails doivent être clarifiés. En particulier, sur les modalités de la mise en œuvre de cette injonction et sur les possibles effets néfastes vis-à-vis de la liberté d'expression. Après avoir vu les possibilités qu'Internet et les réseaux sociaux « offrent » en termes d'amplification, diffusion et rediffusion de contenus illicites, il est important de comprendre les conséquences de l'amplification, en particulier vis-à-vis des droits fondamentaux.

Section II : Des illustrations significatives des conséquences de l'amplification sur les droits fondamentaux

149. Après avoir analysé les caractéristiques d'Internet qui rendent possible l'amplification des comportements illicites, il est important de connaître les conséquences de cette amplification à travers des illustrations concrètes.

---

[396] M. UNTERSINGER, *Modération du Web : la justice européenne favorable au filtrage automatique des messages déjà jugés haineux*, *Le Monde*, 3 octobre 2019, disponible sur : https:// www.lemonde.fr/pixels/article/2019/10/03/moderation-du- web-la-justice-europeenne-favorable-au-filtrage-automatique- des-messages-deja-juges-haineux_6014086_4408996.html
Voir à cet égard : S. PEYROU, « Société de l'information, vie privée et protection des données à caractère personnel : des précisions attendues CJUE Gde ch. 24 septembre 2019, aff. C-507/17, Google LLC - CJUE Gde ch. 24 septembre 2019, aff. C-136/17, GC e.a. - CJUE 1er octobre 2019, aff. C-673/17, Planet49 – CJUE, 3 octobre 2019, aff. C-18/18, Eva Glawischnig-Piesczek c. Facebook Ireland Limited », *RDUE*, 2020/1, p. 210-219.

150. Cette analyse n'est pas exhaustive car l'amplification peut avoir des conséquences multiples. Au vu de l'analyse et des limites posées dans l'introduction, certaines conséquences de l'amplification sont analysées et, plus particulièrement, celles à l'égard des atteintes aux droits de la personnalité (**§I**) et du recrutement à de fins de terrorisme ou de traite des êtres humains (**§II**).

I. L'amplification des atteintes aux droits de la personnalité

151. Les conséquences de l'amplification peuvent se mesurer à travers l'étude de certains comportements illicites. Les atteintes aux droits de la personnalité sont un exemple qui nous permet de témoigner de la puissance d'Internet par rapport aux comportements illicites hors ligne.

152. Dans les développements qui vont suivre, il s'agira, d'une part, de se concentrer plus spécifiquement sur les atteintes à la vie privée et aux données personnelles (**A**), et, d'autre part, d'analyser les atteintes sexuelles en ligne qui se sont multipliées ces dernières années (**B**).

A. L'amplification des atteintes à la vie privée et aux données personnelles

153. Les atteintes à la vie privée et aux données personnelles peuvent être multiples. Premièrement, il y a des atteintes qui concernant les systèmes d'information et qui permettent de commettre des actes illicites à large échelle. Ces dernières peuvent être le point de départ d'autres comportements illicites.

154. Il s'agira d'étudier, d'un côté, les infractions contre les systèmes d'information (**1**) et, de l'autre, leur extension à travers l'analyse du doxing, c'est-à-dire le fait de partager illicitement d'informations personnelles d'un tiers sans son consentement (**2**).

1. Les infractions contre les systèmes d'information

155. Les atteintes aux systèmes d'information sont multiples, entre autres, l'hameçonnage, le piratage, le « spamming » c'est-à-dire le fait d'envoyer des communications non sollicitées à large échelle, l'usurpation d'identité ou le « scamming » (arnaques)[397]. Ces pratiques frauduleuses sont d'accès facile et très peu coûteuses. Il est intéressant de se pencher sur l'hameçonnage ou filutage, en anglais « phishing » de la contraction entre le mot « phreaking » (fraude informatique) et fishing (pêche), car il peut être à l'origine de plusieurs infractions de contenu. L'hameçonnage ou filutage consiste « à obtenir des informations confidentielles et personnelles d'un internaute, au moyen d'un courrier électronique l'invitant à se connecter à un faux site web imitant celui d'une société connue »[398], autre entité ou individu qui serait en apparence légitime à demander des informations. L'objectif est donc celui d'obtenir des informations personnelles et sensibles, comme des coordonnées bancaires. En pratique, les victimes reçoivent un courrier dans leur adresse mail, très souvent obtenu grâce au piratage auprès d'une entreprise ou administration, qui leur demande de compléter certaines informations et/ou de se connecter à une page web via un lien hypertexte. Ces informations peuvent ensuite être utilisées pour commettre plusieurs infractions, par exemple, l'usurpation d'identité afin d'ouvrir des nouveaux comptes (bancaires, sur les réseaux sociaux) ou autres types de crimes ou délits qui comportent l'utilisation d'informations personnelles.

156. L'usurpation d'identité peut aussi entraîner d'autres infractions, c'est le cas du recrutement à des fins sexuelles, lorsqu'un individu se fait passer par une agence de mannequinat ou de travail afin d'attirer des femmes ou des filles pour les faire prostituer[399]. Mais encore des individus peuvent, à travers le piratage de l'ordinateur de la victime, obtenir non seulement des informations personnelles mais également de

---

[397] D. MARTIN, *Cybercriminalité : l'importance du facteur humain,* in La criminalité numérique, Cahiers de la sécurité n° 6, INHES octobre-décembre 2008, p. 133.
[398] P. BELLOIR, *La répression pénale du « phishing »*, Revue Lamy Droit de l'Immatériel, N° 12, 1er janvier 2006.
[399] A. P. SYKITOU, *Traite des êtres humains : recrutement par internet*, pour la Direction générale des droits de l'Homme et des affaires juridiques du Conseil de l'Europe, 2007, p. 124.

contenus tels que des photos ou vidéos à caractère sexuel. Ces derniers peuvent ensuite être diffusés sur Internet ou envoyés à des proches dans le but de gagner de l'argent ou simplement nuire à la victime ; il peut également s'agir de documents confidentiels et personnels qui, s'ils sont publiés, portent atteinte à la vie privée de la victime ou constitueraient un délit de diffamation.

2. Le « doxing » : la divulgation d'informations personnelles

157. Certains individus partagent illicitement des informations personnelles d'un tiers sans son consentement. Il s'agit de la pratique du doxing, c'est-à-dire le fait de partager des informations personnelles d'une personne sur Internet, que ce soit son nom, son adresse, des actes qui lui sont attribués ou des activités dont elle prendrait part. Ce terme vient de l'abréviation anglaise de documents « docs » et correspond à la volonté de partager des informations personnelles d'une personne sur Internet.

158. Ce phénomène est apparu dans les années 90 et est aujourd'hui très présent sur Internet.

Selon une étude menée par des chercheurs américains[400] le plus souvent cette infraction est commise, entre autres, par vengeance, pour rechercher de la justice[401] ou pour des raisons politiques[402]. Les risques dont s'expose la personne qui publie ces informations sont multiples. L'auteur pourrait être poursuivi pour atteinte à la vie privée ou à l'image, mais aussi violation du secret de correspondances ou bien atteinte à la présomption d'innocence.

159. Le chercheur David M. Douglas distingue parmi trois types de doxing : le « deanonymizing doxing » qui consiste à dévoiler l'identité d'une personne jusque-là

[400] P. SNYDER, P. DOERFLER, C. KANICH, et D. MCCOY, *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*. In Proceedings of IMC '17. ACM, New York, NY, USA, 2017.
[401] Selon l'étude de P. SNYDER, P. DOERFLER, C. KANICH, et D. MCCOY cela signifie que le doxeur attaque le doxé parce que ce dernier a commis un acte immoral ou injuste vis-à-vis d'un tiers.
[402] Des actes de doxing ont été menés par le collectif « Anonymous » qui a dévoilé, entre autres, plusieurs informations personnelles sur des personnes qui participaient à des activités du Ku Klux Klan, voir : https://www.vice.com/en/article/kb7eyv/anonymous-hackers-officially-dox-hundreds-of-alleged-kkk-members. Un autre exemple est l'épisode de doxing qui a vu comme protagonistes des personnes ayant participé aux rassemblements d'extrême droite à Charlottesville en 2020.

anonyme, le « targeting doxing » qui signifie partager des informations personnelles qui relèvent des détails privés ou obscurs d'une personne et, enfin, le « delegitimizing doxing », le fait de révéler des informations personnelles intimes qui nuisent à la crédibilité de cette personne[403]. Selon le même auteur, certains types de doxing seraient justifiables, notamment quand il existe une « justification impérieuse d'intérêt public »[404] pour dévoiler l'identité d'une personne et s'il s'agit de rendre public des preuves d'une atteinte aux intérêts publics. Cependant les informations partagées doivent être suffisantes pour démontrer qu'un acte répréhensible a eu lieu mais il ne doit pas s'agir d'une diffusion d'informations injustifiées qui augmenteraient les risques de dommages sur la personne visée.

160. La pratique du doxing est souvent en lien avec ce qu'on appelle le « name and shame » (en français « nommer et couvrir de honte ») utilisé pour dénoncer des actions présumées fautives par des particuliers ou des entreprises qui seraient à l'origine d'atteintes aux droits des tiers.

En 2017 pendant la vague mondiale de libération de la parole concernant les agressions sexuelles et sexistes à travers l'hashtag #MeToo[405], la journaliste Sandra Muller lance en France #BalanceTonPorc qui invite les victimes d'agressions sexuelles et sexistes à partager le nom de leur présumé agresseur. L'hashtag lancé par Sandra Muller, à la différence des autres hashtag partagés dans le monde (#MeToo, #MeAussi, #QuellaVoltaChe), exhortait les victimes à dévoiler le nom de leur présumé agresseur. Or, cela a suscité plusieurs critiques, en effet, cette pratique aurait pu être qualifié comme une diffamation si l'agresseur n'avait pas encore été condamné et pouvait également devenir une pratique assimilable au doxing si les informations personnelles du présumé

---

[403] D. M. DOUGLAIS, *Doxing: A Conceptual Analysis*, Ethics Inf Technol (2016), 28 june 2016, p. 199. Traduction libre de l'autrice, texte original : « I distinguish between three types of doxing: deanonymizing doxing, where personal information establishing the identity of a formerly anonymous individual is released; targeting doxing, that discloses personal information that reveals specific details of an individual's circumstances that are usually private, obscure, or obfuscated; and delegitimizing doxing, which reveals intimate personal information that damages the credibility of that individual ».

[404] Dans le texte original, en anglais : « compelling public interest justification ».

[405] Le #Metoo, déjà existant depuis 2007, a été connu par le grand public dès 2017 après un tweet de l'actrice Alyssa Milano que suite à l'affaire Weinstein, producteur américain plusieurs fois accusé de viol et agression sexuelle et puis reconnus coupable, invitait les femmes et les filles à parler de leur agression sexuelle ou sexiste.

agresseur étaient dévoilées. D'ailleurs, Sandra Muller en personne avait été reconnue coupable en première instance[406] de diffamation, après la plainte portée par Eric Brion qui avait été cité dans l'une de ses publications sur Twitter. Cette dernière a, toutefois, gagné son procès en appel le 31 mars 2021[407] et en cassation[408]. D'autres exemples peuvent être cités, en particulier, les publications des utilisateurs qui dénoncent des personnes à cause de leur origine, leur orientation sexuelle, leur identité de genre ou encore leur religion. Un exemple vient du Mali où, pour dénoncer les personnes homosexuelles, des groupes se répandent sur plusieurs réseaux sociaux, Facebook, YouTube, WhatsApp, avec des photos et des informations personnelles de personnes homosexuelles ou présumées afin de « lutter contre l'homosexualité »[409]. Cela met en danger les personnes dénoncées. En effet, suite à la diffusion de leurs informations personnelles, ces dernières peuvent être victimes de violences hors ligne (agressions physiques, sexuelles ou encore menaces de mort). D'autres atteintes sont dirigées vers des personnes dépositaires de l'autorité publique ou qui exercent une mission de service public. C'est le cas lorsque des internautes partagent l'identité et d'autres informations personnelles sur un gendarme, un policier ou encore un enseignant. Dans le passé, cela a pu être source de violences extrêmement graves comme l'assassinat du professeur Samuel Paty[410] en France dont l'identité et son lieu de travail avaient été partagés sur les réseaux sociaux.

161. Or, ce comportement illicite est sanctionné par la loi mais son traitement dépend notamment du contenu des informations partagées et de leur obtention. En France, après l'adoption de la loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République, l'article 223-1-1 du Code pénal a été créé et il punit « Le fait de révéler, de diffuser ou de transmettre, par quelque moyen que ce soit, des informations relatives à la vie privée, familiale ou professionnelle d'une personne permettant de l'identifier ou

[406] TGI Paris, 25 sept. 2019, n° 18/00402.
[407] CA Paris, pôle 2 - ch. 7, 31 mars 2021, n° 19/19081. Voir F. ERNOTTE, *Droits des réseaux sociaux*, 1re édition, Larcier, 2021, pp. 227-231.
[408] Cass. 1re civ., 11 mai 2022, n° 21-16.497.
[409] Voir l'enquête de France 24 : https://observers.france24.com/fr/20170915-enquete-chasse-homosexuels-mali-internet-lchm-facebook-youtube-whatsapp
[410] Voir notamment la série d'article de France info : https://www.francetvinfo.fr/faits-divers/terrorisme/enseignant-decapite-dans-les-yvelines/

de la localiser aux fins de l'exposer ou d'exposer les membres de sa famille à un risque direct d'atteinte à la personne ou aux biens que l'auteur ne pouvait ignorer […] »[411]. Aux États-Unis, c'est la loi fédérale sur le harcèlement[412] qui est très souvent utilisée pour punir le doxing. Cette loi punit toute personne qui, par l'utilisation de tout service informatique interactif ou service de communication électronique (entre autres), fait craindre à la victime qu'elle est en danger de mort ou lui cause ou tenterait de causer une détresse émotionnelle importante.[413] Et, comme en France, certaines personnes qui exercent des fonctions officielles ont un niveau de protection plus élevé.[414]

162. Enfin, il s'agira d'analyser ce que sont les deepfakes et leur utilisation à des fins illicites.

3. Les « deepfakes »

163. Le mot de deepfake est la contraction du mot « deep learning » (apprentissage profond) et « fake » (faux). Une étude du Parlement européen définit les deepfakes comme : « des médias audio ou visuels manipulés ou synthétiques qui semblent authentiques et qui mettent en scène des personnes qui semblent dire ou faire quelque chose qu'elles n'ont jamais dit ou fait, produits à l'aide de techniques d'intelligence artificielle, y compris l'apprentissage automatique et l'apprentissage profond »[415]. Le terme « deepfakes » a été utilisé pour la première fois par un utilisateur de Reddit, site web américain, qui l'avait utilisé comme pseudonyme et avait publié de vidéos pornographiques dans lesquels il avait collé les visages des femmes célèbres sur celui d'actrices pornographiques.

164. Cette pratique repose sur l'intelligence artificielle et, en particulier, sur les « generative adversarial networks » (réseaux adversatifs générateurs) inventé par le chercheur américain Ian Goodfellow en 2014. Ces logiciels permettent de générer des fausses images et, grâce aux développements de l'intelligence artificielle, nous avons vu

---

[411] Art. 223-1-1 du Code pénal français.
[412] Voir : 18 U.S.C. §2261A.
[413] Pour plus de détails voir l'article 18 U.S.C. §2261A (2), (A) et (B).
[414] Voir : 18 U.S.C. §119.
[415] European Parliament, tackling Deepfakes in european policy, European Parlimaentary Research Service, July 2021, p. I. Traduction de l'anglais de l'autrice.

apparaître également des faux vidéos et bandes sonores[416]. Les manipulations des vidéos, images ou bandes de son peuvent être multiples : échanges de visage ou de voix, création des vidéos où la personne parle mais n'a jamais tenu ces propos.

165. Depuis des années nous assistons à la diffusion de ce type de vidéos ou images qui touchent des individus ne faisant pas parti de la sphère publique ainsi que des femmes et des hommes politiques, des célébrités ou encore des femmes et hommes d'affaires. Plusieurs exemples peuvent être cités : la vidéo de Barack Obama où il insulte Donald Trump[417] ou encore Elon Musk qui semble apparaître dans une directe Zoom de deux étudiants américains[418].

166. Les deepfakes sont distingués des « Shallowfakes ». Ce terme a été formulé pour la première fois par Sam Gregoy, directeur de programmes de l'ONG « Witness » et se réfère à des contenus manipulés à travers des moyens d'éditions standard qui n'ont pas nécessité l'utilisation de l'intelligence artificielle[419]. Un exemple qui a été très médiatisé c'est celui de la vidéo de Nancy Pelosi, ancienne présidente de la chambre des représentants des États-Unis, qui semble avoir des difficultés à s'exprimer[420] alors qu'en réalité la vidéo avait simplement été ralentie. Selon Britt Paris and Joan Donovan, chercheuses au Data and Society Research Institute la vidéo manipulée de Nancy Pelosi fait partie de ce qu'elles appellent de « Cheapfakes », c'est-à-dire des manipulations audiovisuelles qui sont créées avec des logiciels moins chers et très accessibles. Il s'agit

---

[416] Pour voir les multiples formes que cela peut prendre : P. BRITT and J. DONOVAN, *Deepfakes and Cheap Fakes, The Manipulation of Audio and Visual Evidence*, Data & Society, 2019, p. 10.
[417]Voir : E. BRAUN, *La viralité d'une fausse vidéo d'Obama met en lumière le phénomène du «deep fake»*, Le Figaro, 20 avril 2018. Disponible sur : https://www.lefigaro.fr/secteur/high-tech/2018/04/20/32001-20180420ARTFIG00134-la-viralite-d-une-fausse-video-d8216obama-met-en-lumiere-le-phenomene-du-deep-fake.php
[418] Voir : HT CORRESPONDENT, *You can now deepfake Elon Musk and others in your Zoom meetings*, 18 avril 2020. Disponible sur : https://tech.hindustantimes.com/tech/news/you-can-now-deepfake-elon-musk-and-others-in-your-zoom-meetings-story-ApCAOxBuGHo3tlfpsWbYvI.html
[419] H. AIDER, G. PATRINI, F. CAVALLI et L. CULLEN, *The State of Deepfakes: Landscape, Threats, and Impact*, Deeptrace, September 2019, p. 11.
[420] Voir : H. GRAND, *«Deepfake»: une vidéo trafiquée de Nancy Pelosi relayée par des proches de Trump*, Le Figaro, 24 mai 2019. Disponible sur : https://www.lefigaro.fr/secteur/high-tech/deepfake-une-video-trafiquee-de-nancy-pelosi-relayee-par-des-proches-de-trump-20190524

particulièrement des « techniques comme accélérer, ralentir, couper, relancer, ou décontextualiser les images »[421].

167. Malgré la complexité technique de la manipulation des contenus, l'utilisation est simple. En témoigne l'utilisateur de Reddit cité auparavant qui avait diffusé au sein du réseau le code informatique pour permettre l'accès au plus grand nombre à cette technologie. Ainsi, il existe désormais des applications qui permettent de modifier des contenus audiovisuels comme l'application « FakeApp » ou des sites qui proposent ces services.

168. Les risques qui peuvent entrainer ces contenus manipulés, qu'il s'agisse de deapfakes ou cheapfakes, sont multiples et à plusieurs niveaux. D'une part, ces contenus sont utilisés pour porter préjudice aux individus. Les exemples sont très divers : la création d'une fausse photo ou vidéo qui décrédibilise une personne pour un comportement qu'elle n'aurait jamais tenu, un photomontage la représentant dans un contexte gênant ou encore la reproduction de sa voix avec des mots qu'elle n'aurait jamais prononcés. Ainsi, une grande partie de contenus crées via ces techniques est de nature sexuelle et principalement pornographique[422]. Ces contenus sont hébergés dans des sites pornographiques dédiés aux deepfakes ou dans les sites pornographiques traditionnels. De l'autre part, ces contenus peuvent porter atteinte à l'ensemble de la société. À ce sujet, Danielle K. Citron, professeure de droit et Robert Chesney, professeur et avocat, évoquent huit dangers pour la société : distorsion du discours démocratique, manipulation des élections, érosion de la confiance pour les institutions, exacerbation des divisions sociales, fragilisation/dégradation de la sécurité publique et de la diplomatie, mise en péril de la sécurité nationale et affaiblissement et discrédit du journalisme[423]. Ainsi, une bonne partie de ces contenus est créé afin de diffuser des

---

[421] P. BRITT and J. DONOVAN, *Deepfakes and Cheap Fakes, The Manipulation of Audio and Visual Evidence*, Data & Society, 2019, p. 4. Texte original « cheap fakes » that use conventional techniques like speeding, slowing, cutting, re-staging, or re-contextualizing footage ».

[422] H. AIDER, G. PATRINI, F. CAVALLI et L. CULLEN, *The State of Deepfakes: Landscape, Threats, and Impact*, Deeptrace, September 2019, p. 6.

[423] D. K. CITRON and R. CHESNEY, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 California Law Review 1753 (2019). Disponible sur : https://scholarship.law.bu.edu/faculty_scholarship/640

fausses informations et ces derniers peuvent avoir un impact conséquent sur la vie politique d'un État. Nous pouvons penser aux soupçons de corruption lors de la publication de fausses informations pensant l'élection de Donald Trump ou du vote de la Brexit.

169. Ces contenus voient leur origine grâce aux nouvelles technologies. Avant les avancées de l'intelligence artificielle et des techniques des modifications de contenus de facile accès ce type de manipulations n'existaient pas. Leur diffusion est encore plus amplifiée par les technologies de l'information qui permettent aux contenus de circuler très rapidement et vers toute sorte d'individu qui n'a pas les instruments et les connaissances pour reconnaître la véridicité ou pas de ce qu'il voit.

170. Ces transformations ont porté à une transformation et diversification des infractions auquel le droit est appelé à répondre. Nous allons chercher de comprendre comment les droits nationaux s'adaptent aux infractions causées par ces nouvelles technologies. Certains États comme la France ou le Canada ne disposent pas d'instruments législatifs *ad hoc.* En effet, les droits nationaux répondent aux infractions qui sont causés par ces nouvelles techniques par différents moyens.

En France, selon l'avocat Alain Bensoussan « l'arsenal législatif existant est suffisant pour punir les deepfakes. Il faut désormais le mettre en œuvre »[424]. Concernant les risques pour la démocratie, la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information prévoit des mesures qui peuvent s'adapter à la diffusion de deepfakes susceptibles de porter atteinte à la société à cause de fausses informations qu'ils véhiculent pendant les périodes électorales. La loi prévoit une collaboration des plateformes de partage de contenus et la possibilité de procéder à un référé spécifique qui permet d'arrêter la diffusion de fausses informations.
En outre, concernant les individus, les deepfakes peuvent être de différents natures et peuvent porter atteinte à plusieurs de leurs droits. Si des fausses informations sont partagées sur Internet il pourrait s'agir d'injures ou de diffamation, mais encore si des

[424] A. BENSOUSSAN, L'arsenal législatif existant pour punir les deepfakes, Lexing, 14 août 2019. Disponible sur : https://www.alain-bensoussan.com/avocats/arsenal-legislatif-contre-les-deepfakes/2019/08/14/.

images à caractère sexuel sont partagées il pourrait s'agir d'une atteinte à la vie privée, de harcèlement sexuel mais aussi d'usurpation d'identité[425]. Le même raisonnement s'applique au Canada, où il n'existe pas des lois spécifiques pour les deepfakes toutefois, des dispositions existantes pourraient être utilisées, par exemple, celles qui sont prévues pour réprimer la violation des droits d'auteur, le harcèlement, la diffamation ou l'atteinte à la vie privée[426]. Aux États-Unis les infractions commises par la création et la diffusion des deepfakes peuvent être réprimées sous le fondement des lois fédérales et des États, par exemple les lois criminelles qui concernent le cyberstalking ou l'extorsion[427], ainsi que les lois civiles qui répriment la diffamation[428]. Ces lois ne concernant pas spécifiquement les deepfakes, en effet, sauf quelque exception il n'y a pas de lois *ad hoc.* Aujourd'hui deux lois spécifiques à ce phénomène existent, l'une a été introduite en Virginie et concerne les deepfakes à caractère pornographique et l'autre au Texas qui sanctionne l'utilisation de cette technologie pour interférer sur les élections[429].

B. L'amplification des atteintes à caractère sexuel

171. À travers l'utilisation d'Internet les violences sexuelles ont pu se développer et évoluer. Pour cela, il est intéressant de parler des violences en streaming et plus particulièrement du « viol à distance » (**1**), phénomène peu étudié qui a commencé à prendre une ampleur très importante sur Internet depuis une dizaine d'année. Ensuite, l'analyse se concentrera sur l'amplification du partage de contenus sexuels sans le consentement de la personne (**2**) dont le voyeurisme digital, pratiques qui ont augmenté ces dernières années.

---

[425] Article 226-4-1 du Code pénal.
[426] Voir : Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), Malicious Uses and Abuses of Artificial Intelligence, 2020, p. 64. Disponible sur : http://www.unicri.it/News/Report-Criminals-Leverage-AI-for-Malicious-Use
[427] Voir : 18 U.S.C.A. § 2261A (2018) et 18 U.S.C.A. § 875(d) (2018). Voir : N. I. BROWN, *Deepfakes and the Weaponization of Information*, 23 Va. J. L. & Tech 1, 2020, pp. 37-38.
[428] Voir : N. I. BROWN, *Deepfakes and the Weaponization of Information*, 23 Va. J. L. & Tech 1, 2020, p. 39.
[429] M. F. FERRARO, *Deepfake Legislation: A Nationwide Survey—State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media*, WilmerHale, 2019.

1. Violences sexuelles en streaming

172. La pratique des vidéos en streaming, c'est-à-dire à dire le fait de diffuser des contenus en ligne de manière continue et en temps réel, est de plus en plus répandue. Toutefois, ces contenus peuvent être illégaux. Ces violences en streaming peuvent être divisées en deux catégories : d'un côté, ce qu'on appelle le « happy slapping » c'est-à-dire des violences physiques ou sexuelles exercées par une ou plusieurs personnes et filmées en direct par une tierce personne. De l'autre côté, ce qu'on appelle « viol à distance », c'est-à-dire le fait de contraindre une personne, très souvent un mineur, à se filmer (ou à être filmée) en direct toute seule ou avec un tiers qui exerce sur elle des violences sexuelles.

173. Il sera question ici de se concentrer sur cette deuxième catégorie car elle a fait l'objet de peu d'études malgré ses conséquences internationales et son développement de plus en plus important. Déjà en 2015, selon EUROPOL, il ne s'agissait plus d'une tendance émergente mais d'un crime établi[430]. Cette infraction est généralement appelée « viol à distance » mais également « live streaming child sexuel abuse » (abus sexuel d'enfants en direct) quand les personnes qui regardent le direct sont de « simples » spectateurs et « child sexual abuse to order » (abus sexuel d'enfants sur commande) quand les « spectateurs » ne se limitent pas à regarder les violences mais donnent des consignes sur comment les perpétrer. Ce sont souvent les enfants qui sont contraints de subir ces types de violences sexuelles ou physiques qui s'auto infligent ou infligées par des proches ou des tiers qui « vendent » ces pratiques sur Internet. Parfois, ces infractions sont classifiées sous le terme de « webcam child sex tourism »[431] ce qui est fortement déconseillé car cela semblerait impliquer que la réponse à ce type des crimes serait à trouver dans le secteur du tourisme. Ainsi, au vu de la multiplicité de termes utilisés pour ces types d'infractions il vaudrait mieux se limiter à une terminologie unique qui reflète les violences subies, en particulier par les mineurs, et qui permettrait de trouver une définition universelle pour mieux protéger les victimes.

---

[430] EUROPOL, *The Internet Organised Crime Threat Assessment (IOCTA)*, 2015, p. 29.
[431] Interagency Working Group, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International and ECPAT Luxembourg*, Luxembourg, 28 January 2016, p. 48.

174. Il est important de souligner que ce type d'infraction n'est pas mentionné en tant que tel dans les instruments internationaux et régionaux. Toutefois plusieurs textes peuvent être utilisés pour condamner ces pratiques illicites. Premièrement l'article 34 (c) de la Convention relative aux droits de l'enfant qui engage les États parties à la Convention à prendre des mesures pour « que des enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique ». La notion de « production de spectacles » en anglais « pornographic performances »[432] est importante parce que ce terme, assez large et qui ne met pas de limites sur le contexte, le lieu et le moyen de réalisation, permettrait de condamner des « spectacles » qui ont eu lieu via une webcam et en streaming. Ainsi, l'article 2 (c) du Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants définit la « pornographie mettant en scène des enfants » comme : « toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles ». Le « quelque moyen que ce soit » permet d'inclure les nouvelles technologies (en particulier les technologies de l'information et de la communication) et les modalités qui peuvent surgir dans les années à venir.

L'article 3 (1.a.i) du même protocole permet également de condamner le « le fait d'offrir, de remettre, ou d'accepter un enfant, quel que soit le moyen utilisé », comme pour l'article 2 le « quel que soit le moyen utilisé » permettrait de prendre en compte les infractions commises via les nouvelles technologies. Deuxièmement, en 2007, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels a également ajouté des éléments de clarification et des obligations pour les États signataires concernant les spectacles pornographiques, en effet l'article 21(1) condamne la personne qui recrute l'enfant, qui le contraint à participer à ces types d'activité mais également la personne qui y assiste. Troisièmement, au niveau européen,

[432] Ce terme nous le retrouvons également à l'article 27 (c) de Charte africaine des droits et du bien-être de l'enfant ainsi qu'à l'article 3 (b) de la Convention de l'Organisation International du travail (ILO), *Worst Forms of Child Labour Convention.*

la directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie est venue ajouter le terme « spectacles pornographiques » à la liste des définitions. La directive définit ces pratiques comme : « l'exhibition en direct, pour un public, y compris au moyen des technologies de l'information et de la communication : i) d'un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ; ou ii) des organes sexuels d'un enfant à des fins principalement sexuelles »[433]. La directive prend en compte explicitement les technologies de l'information et de la communication mais ne prend pas en compte les comportements sexuels entre un mineur et un adulte, ce qui peut laisser irrésolu le problème des violences sexuelles en streaming[434].

175. Au niveau national, la grande majorité des États ne dispose pas de mesures spécifiques à ce genre d'infraction. Certains États ont pu condamner ces types d'infractions sous le fondement de mesures *ad hoc* ou d'autres dispositions existantes. À cet égard, le 25 septembre 2018, la 54e chambre du tribunal correctionnel de Bruxelles[435] a reconnu un homme de 25 ans coupable de viol à distance. Pour la première fois, les autorités belges ont statué que, malgré l'absence de contact physique, il s'agissait d'un viol car il n'y avait pas de consentement de la victime et cette dernière a été forcée, par la ruse et la contrainte morale, à se pénétrer digitalement[436]. L'absence de consentement et l'acte de pénétration caractérisent en droit belge le viol437. Avant cette jurisprudence, les atteintes sexuelles à distance étaient poursuivies sur le fondement de l'atteinte à la pudeur[438]. En Suède, le 30 novembre 2017, le tribunal d'Uppsala[439] a reconnu un homme coupable de viol ainsi que d'agression sexuelle à distance sur 27

[433] Article 2 (e) de la Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants.
[434] D. DESARA, *The phenomenon of online live-streaming of child sexuel abuse: challenges and legal responses*, Thèse de doctorat, Alma Mater Studiorum – Università di Bologna, 2019, p. 108.
[435] T. corr. Bruxelles fr. (54eme ch.), 25 septembre 2018, J.L.M.B, 2019/14.
[436] Voir : F. ERNOTTE, *Droits des réseaux sociaux*, 1re édition, Larcier, 2021, pp. 206-207.
[437] Article 375 du Code pénal belge : « Tout acte de pénétration sexuelle, de quelque nature qu'il soit et par quelque moyen que ce soit, commis sur une personne qui n'y consent pas, constitue le crime de viol […] ».
[438] T. VALLAT, *Un tribunal belge reconnait un viol par internet à distance...via une webcam*, Blog de maître Thierry Vallat, 26 septembre 2018. Disponible sur : http://www.thierryvallatavocat.com/2018/09/un-tribunal-belge-reconnait-un-viol-par-internet-a-distance.via-une-webcam.html
[439] Rättelse/komplettering Dom, 2017-11-30, Uppsala Tingsrätt (District Court of Uppsala).

enfants[440]. C'est la première fois qu'une personne est condamnée pour viol, en l'espèce, un individu obligeait des enfants de moins de 15 ans originaires du Canada, des États-Unis et d'Ecosse à commettre des actes sexuels sur leur personne sous menace. Les juges belges et suédois avaient reconnu le viol malgré l'absence de contact physique entre les victimes et l'agresseur. Un parallèle peut être fait avec la jurisprudence italienne, en particulier la décision de la Cour de cassation du 2 juillet 2020[441]. Le cas d'espèce ne concernant pas du live streaming mais un échange contraint de photos à caractère sexuel. La Cour avait rappelé que les violences sexuelles pouvaient être caractérisées même en absence de contact physique avec la victime[442] ; ainsi, la Cour fait référence à une décision du 24 mars 2013[443] dans laquelle la Cour de cassation avait affirmé que la violence sexuelle commise au moyen d'instruments de communication à distance ne pouvait pas constituer une circonstance atténuante. La Cour de cassation italienne avait également précisé dans un arrêt de 2018[444] qu'il n'y avait pas de différence entre le fait d'enregistrer et d'envoyer *a posteriori* des actes sexuels accomplis pendant un appel téléphonique et des mêmes actes accomplis pendant un appel vidéo[445]. En France, les violences sexuelles en livestreaming sont un phénomène qui existe depuis plusieurs années et qui s'amplifie. Selon la capitaine Véronique Bechu, il y aurait au moins 300 personnes en France à avoir commandé un viol ou un acte de torture et barbarie sur un enfant à l'étranger[446]. La jurisprudence française avait montré les limites du Code pénal vis-à-vis de ces questions. En effet, la première personne qui avait été condamnée en 2019 pour avoir commandé des viols à distance l'avait été seulement pour détention et

---

[440] « Suède : un homme condamné pour des viols d'enfants à distance, via internet », Le Parisien ave l'AFP, 1er décembre 2017. Disponible sur : https://www.leparisien.fr/faits-divers/suede-un-homme-condamne-pour-des-viols-d-enfants-a-distance-via-internet-01-12-2017-7426179.php

[441] Corte di cassazione, Sez. 3, del 2 luglio 2020, Rv. 25266-20.

[442] Le texte de la décision italienne établit que : « Il Tribunale del riesame ha ricordato che la violenza sessuale risultava pienamente integrata, pur in assenza di contatto fisico con la vittima, quando gli atti sessuali coinvolgessero la corporeità sessuale della persona offesa e fossero finalizzati e idonei a compromettere il bene primario della libertà individuale nella prospettiva di soddisfare o eccitare il proprio istinto sessuale ».

[443] Corte di cassazione, Sez. 3, n. 19033 del 26/03/2013, L, Rv. 255295 – 01.

[444] Corte di cassazione, Sez. 3, n. 17509 del 30/10/2018, dep. 2019, D., Rv. 275595 – 01.

[445] Le texte de la décision italienne établit que : « Ha ravvisato l'integrazione del reato di cui all'art. 609-quater cod. pen. nella condotta di richiesta ad un minorenne, nel corso di una conversazione telefonica, di compiere atti sessuali, di filmarli e di inviarli immediatamente all'interlocutore, non distinguendosi tale fattispecie da quella del minore che compia atti sessuali durante una video-chiamata o una video-conversazione ».

[446] Colloque de l'association Centre de Victimologie pour Mineurs (CVM), *Les mineurs au cœur des cyberviolences*, Paris, 2020. Disponible sur : https://www.youtube.com/watch?v=qHCcVazQy-g

diffusion de contenus à caractère pédopornographique[447]. La situation a commencé à évoluer en 2020 avec la condamnation d'un autre ressortissant français qui avait été à l'origine de viols à distance sur des mineurs aux Philippines et qui a été condamné à 5 ans d'emprisonnement pour complicité d'agressions sexuelles réalisés[448]. Pour apporter une réponse juridique à ce fléau, en janvier 2020, le député Guillaume Gouffier-Cha a déposé un amendement à la proposition de loi sur la protection des victimes de violences conjugales. Il demandait de pouvoir faire poursuivre toute personne qui solliciterait un viol ou une agression sexuelle en live streaming[449]. Désormais, le Code pénal condamne le fait de faire des offres ou des promesses ou de proposer des dons, présents ou avantages quelconques à une personne afin qu'elle commette des actes de torture ou de barbarie, un viol ou une agression sexuelle même en dehors du territoire national[450].

2. Le partage de contenus sexuels sans le consentement de la personne

176. Il s'agit souvent de contenus réalisés avec le consentement de la personne qui en fait l'objet mais qui sont ensuite partagés sans son consentement. Il peut aussi s'agir de contenus échangés ou obtenus par le piratage de l'ordinateur, des réseaux sociaux ou du téléphone de la victime. Il est fréquent que ce type d'images ou vidéos soient partagés par un partenaire ou un ex-partenaire sans le consentement de la personne qui fait l'objet des contenus afin de l'humilier publiquement ou de lui infliger des dommages matériels, par exemple un licenciement[451]. Ce phénomène est plus communément appelé « porno vengeance » (en anglais « revenge porn »), certains auteurs l'appellent « pornographie

---

[447] Colloque de l'association Centre de Victimologie pour Mineurs (CVM), *Les mineurs au cœur des cyberviolences*, Paris, 2020. Disponible sur : https://www.youtube.com/watch?v=qHCcVazQy-g (min. 33:19)
[448] Tribunal correctionnel de Paris, 13 janv. 2020, n° 14227000004.
[449]Amendement n°CL109, déposé le vendredi 10 janvier 2020, disponible ici : https://www.assemblee-nationale.fr/dyn/15/amendements/2478/CION_LOIS/CL109
[450] Articles 222-6-4, 222-26-1, 222-30-2 du Code pénal français.
[451] En Italie plusieurs cas de licenciement des victimes de partage de contenus à caractère sexuel ont été enregistrés. Voir par exemple : GDB, *Vittima di revenge porn licenziata per «danno di immagine»*, 19 février 2020, disponible sur : https://www.giornaledibrescia.it/brescia-e-hinterland/vittima-di-revenge-porn-licenziata-per-danno-di-immagine-1.3460557 Ainsi que ANSA, *Maestra vittima di revenge porn licenziata. L'audio della preside: "Ogni pretesto per mandarla via"*, 16 décembre 2020. Disponible sur : https://www.huffingtonpost.it/entry/maestra-vittima-di-revenge-porn-licenziata-laudio-della-presideio-prendo-ogni-pretesto-per-mandarla-via-cercate-di-farla-sbagliare_it_5fd9ccd8c5b6218b42ed97ae/

non consensuelle » (an anglais nonconsensual pornography)[452] ou « pornographie involontaire »[453] (en anglais « Involuntary pornography »), d'autres utilisent l'expression « abus sexuel par image » (en anglais « image-based sexual abuse »)[454] ou « exploitation sexuelle par image » (en anglais « image-based sexuel exploitation »)[455]. La référence à la pornographie ne paraît pas convenable. En effet, selon le CNRTL, la « pornographie » est la « représentation (sous forme d'écrits, de dessins, de peintures, de photos, de spectacles, etc.) de choses obscènes, sans préoccupation artistique et avec l'intention délibérée de provoquer l'excitation sexuelle du public auquel elles sont destinées »[456]. Or le fait de considérer ces images comme pornographiques implique que la personne a consenti et légitimé ces photos alors que ce n'est souvent pas le cas. De plus, certains contenus ne sont pas sexuellement explicites. Ainsi, cela « conduit certains décideurs politiques sur la mauvaise voie en pensant que les images doivent franchir le seuil de la « pornographie » ou de l'« obscénité » avant d'être illégales, ou que l'auteur doit agir dans un but de gratification sexuelle pour être criminalisé »[457]. Comme le démontrent les travaux menés par McGlynn et Rackley en 2016[458] et repris par S. DeKeseredy et D. Schwartz[459], le terme « vengeance » ne représente pas l'ensemble des infractions, en effet, ce ne sont pas seulement les partenaires ou ex-partenaires qui publient des contenus en quête de vengeance. Ce sont aussi des personnes, des inconnus, qui le font pour d'autres raisons, par exemple, pour gagner de l'argent ou juste pour s'amuser. En outre, le terme « porno vengeance » mettrait, toujours selon McGlynn et Rackley, trop l'accent sur les

---

[452] M. A. FRANKS, *How to defeat 'revenge porn': First, recognize it's about privacy, not revenge.* Huffington Post, 22 juin 2015. Disponible sur : http://www.huff- ingtonpost.com/mary-anne-franks/how-to-defeat-revenge-porn_b_7624900. html

[453] A. BURNS, In full view: Involuntary porn and the postfeminist rhetoric of choice. In C. Nally & A. Smith (Eds.), *Twenty-first century feminism: Forming and performing femininity* (pp. 93–118). Basingstoke, UK: Palgrave Macmillan, 2015.

[454] C. MCGLYNN, E. RACKLEY, *Not 'revenge porn,' but abuse: Let's call it image-based sexual abuse*, Inherently Human, 15 février 2016. Disponible sur : https://inherentlyhuman.wordpress.com/2016/02/15/not-revenge-porn-but-abuse-lets-call-it-image-based-sexual-abuse/

[455] N. HENRY et A. POWELL, *Sexual violence in the digital age: The scope and limits of criminal law*, Social & Legal Studies, 25(4), 397–418, 2016.

[456] Centre national de ressources textuelles et lexicales, recherche du mot « pornographie ». Disponible sur : https://www.cnrtl.fr/definition/pornographie

[457] C. MCGLYNN, E. RACKLEY, *Not 'revenge porn,' but abuse: Let's call it image-based sexual abuse*, Inherently Human, 15 février 2016. Disponible sur : https://inherentlyhuman.wordpress.com/2016/02/15/not-revenge-porn-but-abuse-lets-call-it-image-based-sexual-abuse/. Traduction libre de l'auteure.

[458] *Ibid.*

[459] W. S. DEKESEREDY and M. D. SCHWARTZ, *Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory*, Sexualization, Media, & Society October-December 2016. Disponible sur : https://journals.sagepub.com/doi/pdf/10.1177/2374623816684692

motivations de l'acte (la vengeance) au dépit des dommages causés à la victime. Pour cela tous les termes qui impliquent le mot « pornographique » ou « pornographie » sont à exclure. C'est le cas aussi du terme « abus », qui n'est pas non plus souhaitable, car ce terme est utilisé souvent pour l'utilisation excessive d'un droit (ex : abus de pouvoir, abus des biens sociaux) et ne semble pas pouvoir caractériser ces infractions. Pour cela seront privilégiés les termes « partage non consenti de contenus à caractère sexuel ».

177. Aux États-Unis, les études démontrent que 90% des victimes de ces infractions sont des femmes et ce phénomène est de plus en plus répandu[460]. Il existe aussi des sites dédiés à l'échange de ces contenus, c'est le cas du site « isanyoneup.com », premier site qui est apparu aux États-Unis où des photos à caractère sexuel étaient partagées avec les informations personnelles des femmes. Le site a atteint les 30 millions de vues par mois. Il y a beaucoup d'autres sites, blogs et forums où ce genre d'images circulent sans oublier les réseaux sociaux où des groupes privés sont créés. Par exemple, sur Snapchat les groupes « Ficha »[461], sur Facebook le groupe « Babylone 2.0 »[462] ou sur Telegram[463]. En janvier 2017 le seul réseau social Facebook a dû analyser 54 000 contenus sexuels soupçonnés d'avoir été partagés sans le consentement des personnes qui y apparaissaient et a clôturé plus de 14 000 comptes. Ainsi, en octobre 2020, une enquête[464] de l'entreprise « Sensity », spécialisée dans les menaces virtuelles, a mis en garde vis-à-vis d'un phénomène très alarmant qui a lieu, pour le moment, seulement sur Telegram. Il s'agit

---

[460] FRANKS, 2016, voir M. HALL, Pornography: Non-Consensual, Vengeful, Online, Originally published in NOTA (National Organisation for the Treatment of Abusers) Newsletter 82 82 (2017): 16–18.

[461] Un groupe « Ficha » de la contraction du verbe « afficher » consiste en un groupe principalement formé par des hommes sur les réseaux sociaux, en particulier Snapchat, où des photos, surtout intimes, de femmes et filles sont partagées sans le consentement des intéressées. Pendant la pandémie de Covid-19 ces groupes ont augmenté fortement en France et ailleurs en Europe. Voir : L. KHOUIEL, *Quand le revenge porn s'adapte au confinement*, VICE, 8 avril 2020. Disponible sur : https://www.vice.com/fr/article/bvg4pz/quand-le-revenge-porn-sadapte-au-confinement. Voir également : S. FONTANA, *Dentro il più grande network italiano di revenge porn, su Telegram*, Wired Italia, 3 avril 2020. Disponible sur : https://www.wired.it/internet/web/2020/04/03/revenge-porn-network-telegram/?refresh_ce=

[462] Le groupe Babylone 2.0 était un groupe Facebook que comme les groupes Ficha était composé principalement par des hommes qui partageaient des photos intimes des femmes et des filles mineurs à leur insu. Ce groupe est désormais fermé mais d'autres ont suivi, comme « Babylone 3.0, la Renaissance ».

[463] S. FONTANA, *Come i gruppi di revenge porn proliferano su Telegram*, Wired Italia, 9 avril 2020. Disponible sur : https://www.wired.it/internet/web/2020/04/09/telegram-gruppi-revenge-porn-funzionamento/?refresh_ce= et L. ZURLONI, *Uscite le minorenni*, Wired Italia, 23 janvier 2019. Disponible sur : https://www.wired.it/internet/web/2019/01/23/telegram-chat-stupro-virtuale-minori-stalking-revenge-porn/?refresh_ce=

[464] H. AJDER, G. PATRINI, F. CAVALLI, *Automating image abuse, deepfake bots on telegram*, Sensity, octobre 2020. *Disponible sur : https://sensity.ai/reports/*

d'un robot alimenté par l'intelligence artificielle qui permet aux utilisateurs de « déshabiller » des images de femmes vêtues. Il y aurait environ 104 852 femmes qui ont vu leurs images personnelles « dénudées » partagées publiquement à la fin du mois de juillet 2020[465]. Ces images peuvent ensuite être utilisées comme des vraies images à contenu intime à des fins d'humiliation publique ou d'extorsion. Suite à la publication de ce rapport le Garante per la protezione dei dati personali, équivalent de la CNIL en Italie, a ouvert une enquête pour vérifier l'activité de Telegram et l'utilisation de cette technologie[466].

2.1 Le voyeurisme digital

178. Les images sexuelles partagées sans le consentement de la victime peuvent être le fruit également du voyeurisme digital. Le voyeurisme a toujours existé, dès ses représentations cinématographiques à la réalité des faits quand un individu en espionnait un autre à travers le trou de la serrure. Cependant aujourd'hui ce phénomène a pris des formes différentes. En effet, les nouvelles technologies ont rendu cela plus facile, non seulement il est plus accessible de regarder mais désormais de capturer une ou plusieurs images et la ou les diffuser. Des appareils de plus en plus petit, discrets et accessibles ont fait leur apparition ainsi que des lieux virtuels où partager ces contenus. Le voyeurisme digital est également appelé « upskirting » de l'anglais « regarder sous les jupes » mais il existe aussi le terme de « downblousing » quand il s'agit de regarder le décolleté. La plus commune des définitions du voyeurisme digital est celle qui définit ce comportement comme le fait de regarder les parties intimes d'une personne sans son consentement, ce qui entrainerait une atteinte à son intimité.

179. Selon le Département politique pour les droits des citoyens et les affaires constitutionnelles du Parlement européen, « le « creepshot », le « upskirting » ou le voyeurisme digital consistent à prendre des photos ou des vidéos des parties intimes des

[465] *Ibid.* p. 2.
[466] Garante per la protezione dei dati personali, *Deep fake: il Garante privacy apre un'istruttoria nei confronti di Telegram per il software che "spoglia" le donne*, 2020. Disponible sur : https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9470722

femmes sans leur consentement et à les partager en ligne »[467]. Au sein de l'Union européenne la résolution du Parlement européen du 12 septembre 2017 est venue rappeler l'importance d'adopter des mesures concrètes contre plusieurs infractions, dont le voyeurisme[468]. Ainsi, dans la jurisprudence de la Cour européenne des droits de l'Homme, le voyeurisme est traité comme une atteinte à la vie privée et, par conséquent, il s'agit d'une atteinte à l'article 8 de la Convention européenne des droits de l'Homme. Un exemple, cité dans le chapitre précédent, est celui de l'affaire *Söderman c. Suède*[469] dans lequel la Cour a condamné la Suède car elle n'avait pas su assurer le droit à la vie privée d'une mineure dont le beau-père avait tenté de la filmer à son insu dans son domicile à des fins sexuelles.

180. La définition juridique n'est pas le même dans tous les États qui prévoient des dispositions, cependant, certaines similitudes existent d'un État à l'autre[470]. L'amplification de ces comportements illicites est caractérisée par une plus importante atteinte à la vie privée car le partage des photos peut faire circuler les contenus sur plusieurs sites Internet ainsi que sur divers réseaux sociaux. Cela peut se passer sans que la victime soit au courant de toutes les plateformes où figure sa photo, ce qui rend leur retrait compliqué.

181. Après avoir souligné l'amplification pour les comportements illicites qui portent atteinte aux droits de la personnalité, il s'agit de montrer l'élargissement des risques liés à l'utilisation d'Internet vis-à-vis du terrorisme et de la traite des êtres humains. En effet, les réseaux criminels se sont emparés d'Internet pour élargir leur action et notamment grâce à la possibilité de recruter des sympathisants ou des victimes.

---

[467] A. VAN DER WILK, *Cyber violence and hate speech online against women*, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, September 2018, p. 18.
[468] Résolution du Parlement européen du 12 septembre 2017 sur la proposition de décision du Conseil portant conclusion, par l'Union européenne, de la convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (COM(2016)0109 – 2016/0062(NLE)), point 3. Le Parlement européen « invite les États membres à adopter des mesures concrètes afin de lutter contre ces nouvelles formes de crimes, y compris l'extorsion sexuelle, la manipulation psychologique, le voyeurisme et la vengeance pornographique, et à protéger les victimes, qui subissent des traumatismes graves les poussant parfois même au suicide ; ».
[469] Cour EDH, GC, 12 novembre 2012, *Söderman c. Suède*, aff. 5786/08.
[470] Pour plus de détails, voir §§ 242-248 de cette thèse.

II. L'amplification du recrutement sur Internet à de fins de terrorisme et de la traite des êtres humains

182. L'amplification se manifeste à travers l'augmentation de la présence de réseaux terroristes d'Internet à des fins de financement, propagande, planification mais également recrutement. Le recrutement au moyen d'Internet est devenu plus facile, plus rapide ainsi que transnational (**A**). Ce phénomène en augmentation montre comment Internet amplifie des comportements illicites déjà existants non seulement à l'égard du terrorisme mais également de la traite des êtres humains surtout lorsqu'il s'agit d'exploitations sexuelles et de travail (**B**).

A. L'action des organisations terroristes facilitées par Internet

183. Les organisations terroristes ont trouvé dans les nouvelles formes de communication et d'information un terreau fertile pour leur expansion. Depuis plusieurs années, les Nations Unies[471] comme d'autres acteurs internationaux ou européens tels que le Conseil de l'Europe[472] ou l'Union européenne[473] alertent sur le danger que représente Internet dans l'expansion des réseaux terroristes et dans la mise en œuvre d'actes terroristes.

184. Avant de développer une analyse à cet égard, il est important de préciser ce que nous définissons comme acte et groupe terroriste. En effet, en l'absence d'une définition de terrorisme acceptée par l'ensemble de la communauté internationale ou européenne[474],

---

[471] Voir, entre autres, Rapport du Secrétaire général, *S'unir contre le terrorisme : recommandations pour une stratégie antiterroriste mondiale*, Soixantième session, 27 avril 2006 ainsi que la Résolution 1963 (2010) Adoptée par le Conseil de sécurité à sa 6459e séance, le 20 décembre 2010, S/RES/1963 (2010).
[472] Voir notamment le point 1 de la Stratégie du Conseil de l'Europe contre le terrorisme (2018-2022), CM (2018)86, 4 juillet 2018.
[473] Voir par exemple le règlement (UE) 2021/784 du Parlement Européen et du Conseil, du 29 avril 2021, relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.
[474] En effet, en droit international et en droit de l'Union européenne il n'existe pas une définition universelle de terrorisme, cela à cause des complexités politiques et idéologiques qui différentes entre les pays. En droit de l'Union européenne certaines infractions ont été harmonisées grâce à la décision-cadre du Conseil européen du 13 juin 2002 relative à la lutte contre le terrorisme (2002/475/JAI) ou encore en droit international il y a la Convention du Conseil de l'Europe pour la prévention du terrorisme du 16 mai 2005 que dans le préambule reprend des éléments de définition donné par la décision cadre ou la résolution 1566(2004) des Nations Unies, adoptée par le Conseil de sécurité à sa 5053e séance le 8 octobre 2004 en soulignant que : les « actes de terrorisme, par leur nature ou leur contexte, visent à intimider gravement une population, ou à contraindre

plusieurs instruments juridiques internationaux et européens donnent des précisions à ce sujet. Pour procéder à cette analyse, la définition d'actes criminels utilisée dans la résolution 1566(2004) sera retenue. Elle prévoit que « les actes criminels » sont « notamment ceux dirigés contre des civils dans l'intention de causer la mort ou des blessures graves ou la prise d'otages dans le but de semer la terreur parmi la population, un groupe de personnes ou chez des particuliers, d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à accomplir un acte ou à s'abstenir de le faire »[475]. Cette définition qui n'est pas présentée dans le texte de la résolution comme une définition de terrorisme est utilisé comme une référence[476]. Ainsi, comme « groupes terroristes » il sera fait référence à tout groupe organisé qui agit pour procéder à des actes tels que décrit par la résolution précitée. Les motivations de ces actes peuvent être idéologiques et fondées sur la religion, comme l'État islamique (ci-après « EI ») ou Al Qaeda (ci-après « AQ »), mais aussi politiques, on peut penser aux mouvements violents d'extrême droite ou extrême gauche.

185. Avant d'analyser les objectifs poursuivis par les groupes terroristes par l'utilisation d'Internet et plus particulièrement les réseaux sociaux, il est intéressant de donner un aperçu de l'évolution de l'usage des moyens de télécommunication par les réseaux terroristes. Pour ce faire, il est intéressant de prendre l'exemple des groupes djihadistes qui ont fait évoluer leur utilisation des nouvelles technologies de l'information et de la communication. En effet, dans les années 90 ils utilisaient de cassettes vidéo envoyées clandestinement aux fins de propagande ou de recrutement. Toutefois, le transport étant assez risqué et Internet ayant commencé à se démocratiser, les premiers sites web vont apparaître[477]. Ensuite entre les années 2000 et 2012-2013, les forums se développent

---

indûment un gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque, ou à gravement déstabiliser ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou d'une organisation internationale ».

[475] Résolution 1566(2004) des Nations Unies, adoptée par le Conseil de sécurité à sa 5053e séance le 8 octobre 2004, point 3.

[476] Voir par exemple le rapport du 28 décembre 2005 du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, dans lequel il souligne que le terme « terrorisme » doit être employé pour des actes qui soient véritablement terroristes et pour préciser son propos il cite le contenu de *la résolution 1566 (2004), voir :* M. SCHEININ, Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'Homme et des libertés fondamentales dans la lutte antiterroriste, Commission des Droits de l'Homme, E/CN.4/2006/98 28 décembre 2005, point 42.

[477] M. HECKER, *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015, p. 12.

mais sont ensuite délaissés à cause des risques d'infiltration des services de renseignement et de l'essor des réseaux sociaux[478] qui vont désormais être leur outil principal pour la propagande et le recrutement. Malgré des débuts méfiants en 2008 vis-à-vis des plateformes numériques américaines tels que Facebook, soupçonnées par les djihadistes d'être en lien avec les services de renseignement, à partir de 2012[479] les réseaux sociaux sont de plus en plus utilisés par les terroristes et notamment Twitter[480]. Selon une analyse de J.M. Berger et J. Morgan à la fin de 2014 il y aurait eu environ 46 000 de comptes Twitter utilisés par des sympathisantes de l'État islamique[481]. Il est à souligner que l'utilisation de réseaux varie selon les groupes terroristes. Par exemple, lorsqu'en novembre 2019[482] les comptes de l'État islamique sur Telegram ont été effacés, cela a eu des conséquences également sur l'utilisation des réseaux par Al Qaeda. L'EI a commencé à utiliser plusieurs plateformes traditionnelles alors qu'AQ a étendu sa présence dans des plateformes alternatives comme GeoNews ou Chirpwire[483]. Même si les moyens de communication ont évolué les objectifs recherchés par les réseaux terroristes sont toujours les mêmes : échanger des informations, faire de la propagande, organiser des attaques terroristes, recruter ou encore chercher des financements[484]. L'action des organisations terroristes est facilitée par la diffusion des contenus de propagande qui circulent sur les réseaux sociaux, cette propagande étant menée, en particulier, aux fins de recrutement et de radicalisation (**1**).

---

[478] *Ibid.* pp. 15-16.
[479] M. Hecker explique que 2012 est une année charnière car c'est la période où le djihadisme attire des volontaires étrangers internationaux dont des occidentaux qui utilisent les réseaux sociaux comme Facebook, Twitter ou encore YouTube. Pour plus d'informations : Marc HECKER, *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015, p. 16.
[480] Pour plus d'informations voir Nico PRUCHA et Ali FISHER, T*weeting for the Caliphate*, CTC Sentinel, vol. 6, n° 62, juin 2013 reporté par Marc HECKER, *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015, p. 16.
[481] J.M. BERGER et J. MORGAN, *The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter*, The Brookings Project on US Relations with the Islamic World, Analysis Paper, n° 20, mars 2015, p. 2.
[482] Voir EUROPOL, *Online Jihadist propagande,* 2020 in review, Europol Public Information, 2021, pp. 17-18. Disponible sur : https://www.europol.europa.eu/publications-documents/online-jihadist-propaganda-2020-in-review
[483] *Ibid,* p. 31.
[484] Voir UNICRI and UNCCT, *Countering terrorism online with artificial intelligence,* An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia, 2021, p. 12 ; voir également UNODC, *Utilisation de l'Internet à des fins terroristes*, mars 2014, p. 1. Voir, entre autres, la Résolution 1963 (2010) Adoptée par le Conseil de sécurité à sa 6459e séance, le 20 décembre 2010, S/RES/1963 ainsi que la Résolution 2178 (2014) Adoptée par le Conseil de sécurité à sa 7272e séance, le 24 septembre 2014, S/RES/2178.

1. Le recrutement aux fins du terrorisme

186. Le recrutement sur Internet représente une aubaine pour les réseaux terroristes, en effet il est possible de toucher un large spectre d'individus, de les cibler en adaptant le contenu et de les recruter plus rapidement. Le terme « recrutement » est employé dans cette analyse avec la signification donnée par la directive 2017/541 du Parlement européen et du Conseil, du 15 mars 2017, qui le définit comme : le fait de solliciter une autre personne à commettre plusieurs types d'actes intentionnels érigés en infraction terroriste comme les atteintes à la vie et à l'intégrité physique d'une personne ou la direction d'un groupe terroriste et la participation aux activités d'un groupe terroriste[485]. Le Ministre des affaires intérieures et du droit de Singapour indiquait en 2017 que, grâce à Internet, le délai de recrutement d'un réseau terroriste comme l'EI a été réduit de 24 à 9 mois seulement[486]. Le bilan est sans appel, en Asie plusieurs exemples le démontrent. Selon l'ancien ministre de l'intérieur de Malaisie les médias sociaux ont été responsables de 17% du recrutement de l'État islamique[487]. En outre, à Singapour, un autre exemple frappant montre que sur 21 ressortissants détenus pour des activités liées au terrorisme en vertu de la loi sur la sécurité intérieure entre 2015 et 2018, 19 se sont radicalisés par la propagande de l'EI en ligne et les deux autres par des contenus en ligne les incitant à participer au conflit syrien[488]. Mais encore, selon une étude française de 2014, menée avec 160 familles dont un proche a été impacté par le discours de l'islam radical, on estime qu'environ dans 91% des cas l'endoctrinement s'est fait par le biais d'Internet[489] et que 98% du discours de l'islam radical utilise internet[490]. En outre, les groupes

[485] Voir article 6 de la directive (UE) 2017/541 du Parlement européen et du Conseil, du 15 mars 2017, relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil.
[486] UNICRI and UNCCT, *Countering terrorism online with artificial intelligence,* An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia, 2021, p. 10.
[487] *Ibid.* p. 12 qui cite A. SIGNPENG and R. TAPSELL, *From Grassroots Activism to disinformation*; Social Media Trends in Southeast Asia, 2020, ISEAS-Yusof Ishak Institute.
[488] *Ibid.* p. 12 qui cite Kimberly T'NG, *Down the Rabbit Hole: ISIS on the Internet and How It Influences Singapore Youth*, April 2019.
[489] D. BOUZAR, C. CAUPENNE et S. VALSAN, *La métamorphose opérée chez le jeune par les nouveaux discours terroristes*, Centre de prévention des dérives sectaires liées à l'islam, novembre 2014, p. 14.
[490] *Ibid*. p. 11.

extrémistes[491] ont su utiliser à leur avantage la pandémie de Covid-19 en surfant sur la manipulation de l'information et sur la désinformation. Ce faisant, ils ont pu profiter du climat de défiance vis-à-vis des acteurs gouvernementaux pour renforcer « les récits extrémistes des acteurs non-étatiques et les stratégies de recrutement »[492]. Ainsi, la capacité de recruter des nouveaux sympathisants est facilitée par les algorithmes des réseaux sociaux. En effet, l'utilisateur, sur la base de contenus qu'il a le plus aimés[493] ou partagés, se voit proposer une sélection ciblée avec des contenus similaires à ceux déjà appréciés ou la proposition d'ajouter en tant qu'amis des personnes aimant les mêmes types de contenu. Cela conduit l'utilisateur à se renfermer sur ses croyances et à les alimenter. Sur Facebook, par exemple, il a été démontré qu'il était très facile d'avoir accès à la propagande de l'EI et à être recruté pour partir en Syrie[494]. Ces propositions facilitent également l'élargissement d'autres communautés comme celle des QAnons[495], des groupes survivalistes persuadés de l'effondrement de notre civilisation ou autres mouvances similaires.

187. Il est indéniable que la facilité du recrutement au moyen de la propagande en ligne mène à une amplification des risques de passage à l'acte terroriste. Une illustration est donnée par l'affaire *R. c. Roshanara Choudhry*[496]. Dans cette affaire, Mme Choudhry, étudiante radicalisée sur Internet, a été condamnée à perpétuité après avoir poignardé un membre du parlement britannique pour « venger » le peuple iraquien[497].

---

[491] Plusieurs groupes d'extrême droite ont eu cette approche, par exemple le Nordic Resistance Movement en Suède, le Kohti Vapautta! en Finlande ou encore Blanche Europe en France. Pour en savoir plus : UNICRI, *Stop the virus of disinformation*, The risk of malicious use of social media during COVID-19 and the technology options to fight it, November 2020.

[492] Voir UNICRI and UNCCT, *Countering terrorism online with artificial intelligence*, An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia, 2021, p. 27.

[493] L'action d'« aimer » un contenu s'exprime à travers un ou des « likes ».

[494] M. HECKER, *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015, p. 24 qui cite notamment G. KRISTANADJAJA, *Comment Facebook m'a mis sur la voie du jihad,* Rue 89, 21 octobre 2014.

[495] R. HARFOUSH définit QAnon comme « un mouvement conspirationniste américain d'extrême droite qui a combiné plusieurs théories du complot populaires (nouvel ordre mondial, État profond, réseaux de trafic d'enfants, etc.) en un récit spécifique centré sur une bataille biblique entre l'ancien président américain Donald Trump et une cabale mondiale de pédophiles sataniques qui dirigeraient le monde en secret », voir : R. HARFOUSH, *QAnon, la culture numérique et les élections françaises*, CNAMM, juin 2021, pp. 2-3.

[496] *Voir R. c. Roshanara Choudhry* [rechercher le n° de l'affaire] *voir également* UNODC, *Utilisation de l'Internet à des fins terroristes*, mars 2014, p.138.

[497] Mme Choudhry avait en effet poignardé le parlementaire Stephen Timms car il avait voté en faveur de la guerre Iraq. Voir : BBC, *Woman jailed for life for attack on MP Stephen Timms*, 3 novembre 2010. Disponible sur : https://www.bbc.com/news/uk-england-london-11682732

188. Face à ces constats il faut tout de même souligner que les nouvelles technologies peuvent être très précieuses pour faire face à l'action des réseaux terroristes. En effet, l'intelligence artificielle peut venir en aide aux enquêteurs ou l'effacement des contenus terroristes peut freiner leur propagande. Ainsi, les contre-discours peuvent être largement diffusés sur les réseaux sociaux.

189. Enfin, il est intéressant d'analyser plus en détail le recrutement à des fins sexuelles et de travail.

B. La traite désinvolte des êtres humains sur Internet

190. Après avoir analysé le recrutement aux fins de terrorisme, il est intéressant de montrer l'amplification sur le recrutement aux fins d'exploitation sexuelles et de travail domestique (**1**) et en particulier à l'égard de mineurs à travers le phénomène du grooming (**2**).

1. Le recrutement aux fins d'exploitation sexuelle et de travail

191. Nous avons analysé précédemment les caractéristiques d'Internet qui facilitent la mise en œuvre des cyberviolences. Or, concernant l'amplification, il est clair que ces mêmes caractéristiques, telles que l'utilisation de pseudonymes, la multiplicité d'utilisateurs ou encore la dimension transnationale aident à amplifier le recrutement. En effet, alors qu'avant, le recrutement se faisait hors ligne oralement, à travers la presse par des offres d'emploi, de mariage ou rencontre, aujourd'hui une différenciation de moyens de recrutement a été constatée[498], en effet, les recruteurs se sont adaptés aux nouvelles technologies et essayent de profiter de ses avantages.

192. Avant de montrer comment les recruteurs utilisent les nouvelles formes de communication à des fins illicites, il est intéressant de définir les termes « traite d'êtres

[498] Direction générale des droits de l'Homme et des affaires juridiques du Conseil de l'Europe, *Traite des êtres humains : recrutement par internet,* L'usage abusif d'Internet pour le recrutement des victimes de la traite des êtres humains, EG-THB-INT (2007) 1, 2007, p. 27.

humains ». Une définition provient du Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, appelé également Protocole de Palerme. Ce dernier définit dans son article 3 l'expression traite des personnes comme « le recrutement, le transport, le transfert, l'hébergement ou l'accueil de personnes, par la menace de recours ou le recours à la force ou à d'autres formes de contrainte, par enlèvement, fraude, tromperie, abus d'autorité ou d'une situation de vulnérabilité, ou par l'offre ou l'acceptation de paiements ou d'avantages pour obtenir le consentement d'une personne ayant autorité sur une autre aux fins d'exploitation » [499]. Ainsi, l'article poursuit en donnant des informations sur ce qui est considéré comme caractérisant l'exploitation, c'est-à-dire « au minimum, l'exploitation de la prostitution d'autrui ou d'autres formes d'exploitation sexuelle, le travail ou les services forcés, l'esclavage ou les pratiques analogues à l'esclavage, la servitude ou le prélèvement d'organes »[500]. La même définition est reprise par l'article 4 de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains. En outre, cet article a fait l'objet d'un éclairage concernant le recrutement sur Internet à travers le rapport explicatif de la Convention qui a spécifié que « la définition de la traite des êtres humains contenue dans la *Convention* trouve aussi à s'appliquer lorsque la traite est pratiquée *via l'utilisation des nouvelles technologies de l'information.* Ainsi, par exemple, lorsque la définition vise le recrutement d'une personne, ce recrutement est visé quelle que soit la manière dont il est effectué (que ce soit oralement, par voie de presse, via Internet, etc.) »[501]. Donc, il s'agit surtout de s'intéresser à l'amplification du recrutement à des fins d'exploitation, en particulier sexuelle et travail forcé.

193. Il revient souvent dans les études menées à ce sujet que l'utilisation d'Internet pour le recrutement aux fins de traite n'est pas à analyser comme une nouvelle forme de traite

[499] Article 3 du Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, 2000.
[500] *Ibid.*
[501] Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains, point 79. Italique de l'autrice.

mais plutôt comme un nouveau moyen utilisé par les recruteurs[502]. Il s'avère que depuis plusieurs années l'utilisation d'Internet à ces fins augmente[503]. Selon un rapport de 2018, aux États-Unis 55% des victimes de traite à de fins d'exploitation sexuelle depuis 2015 avaient rencontré leur trafiquant en ligne et 42% des victimes avaient révélé que les outils en ligne étaient utilisés par les recruteurs pour établir une relation avec elles[504].

194. L'utilisation d'Internet facilite l'identification des potentielles victimes notamment au vu de l'exposition étendue de la vie privée et des données personnelles des usagers. Les recruteurs ont un facile accès à leur géolocalisation, leurs informations personnelles concernant leur éducation, leurs amies ou encore leurs passions[505] ; y compris leurs vulnérabilités, tels que des difficultés économiques, l'abus d'alcool ou de drogue[506]. Mais également des difficultés familiales ou scolaires, en particulier lorsqu'il s'agit de mineurs[507]. Tous ces éléments servent aux recruteurs pour dresser le portrait de la victime et adapter leur discours. Concernant les vulnérabilités de victimes, l'Organisation pour la sécurité et la coopération en Europe (ci-après « OSCE ») signale que les réseaux terroristes utilisent les réseaux sociaux pour recruter des femmes et des filles afin de les marier de force, de les exploiter sexuellement ou les soumettre à des travaux forcés[508]. Ils profitent notamment des situations de vulnérabilité des victimes à travers la méthode du « lover boy », c'est-à-dire la séduction, les recruteurs faisant croire aux victimes qu'ils les aiment afin de les convaincre à faire ce qu'ils demandent[509]. Ainsi, Internet permet aux recruteurs de profiter du pseudonymat et d'utiliser plusieurs fausses identités.

---

[502] Direction générale des droits de l'Homme et des affaires juridiques du Conseil de l'Europe, *Traite des êtres humains : recrutement par internet,* L'usage abusif d'Internet pour le recrutement des victimes de la traite des êtres humains, EG-THB-INT (2007) 1, 2007, p. 26.
[503] Voir, entre autres : EUROPOL, *Intelligence Notification: Trafficking in Human Beings and the Internet,* November 2014, p. 1, UNODC, *Global report on trafficking in persons*, 2020, p. 119
[504] V. BOUCHE, *Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking*, THORN, January 2018, p. 6 cité par : OSCE, Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, mai 2020, p.18.
[505] OSCE, Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools,* mai 2020, p.18.
[506] *Ibid.* p.18.
[507] *Ibid.* p. 18.
[508] *Ibid*, p. 19.
[509] Fondation Scelles, *Système prostitutionnel*, Nouveaux défis, nouvelles réponses, 5e rapport mondial, 2019, p. 104.

À ce sujet, une étude de l'Office des Nations unies contre les drogues et le crime (ci-après « UNODC ») rapporte un exemple frappant de l'utilisation par un recruteur de plusieurs comptes sur les réseaux sociaux qu'il utilisait, d'un côté, pour proférer des injures à une potentielle victime et, de l'autre côté, pour la réconforter dans le but de gagner sa confiance[510]. Ce recrutement a lieu sur plusieurs réseaux sociaux, sur des forums de discussions, sites web mais également les jeux vidéo en ligne. Les formes sont multiples, le plus souvent il s'agit d'offres d'emploi qui concernent l'administration, le nettoyage ou d'autres métiers qui ne nécessitent pas forcément un diplôme. Ces annonces sont publiées sur des sites web classiques de recherche d'emploi mais également sur les sites de rencontres[511]. Un exemple de site web où les annonces d'exploitation et aux fins de recrutement se multipliaient était celui du site américain Backpage. Il s'agit d'un site de petites annonces très populaire qui contenait une section réservée aux adultes. Or, dans cette section, il s'est avéré, après plusieurs plaintes des femmes victimes de la traite et différentes enquêtes du FBI, qu'un grand nombre d'annonces étaient liées à des réseaux de prostitution et de traite d'êtres humains. Cette rubrique du site a depuis été supprimée[512] et les responsables du site poursuivis en justice pour facilitation de la prostitution et blanchiment d'argent[513]. Fait analogue avec le site VivaStreet en France qui a suspendu sa section « rencontres » qui a fait l'objet d'une enquête pour proxénétisme aggravé[514].

---

[510] UNODC, *Global report on trafficking in persons*, 2020, p. 121

[511] A. DI NICOLA, G. BARATTO and E. MARTINI, *Surf and Sound: The role of the Internet in people smuggling and human trafficking*, Department 'Faculty of Law, University of Trento, March 2017. Voir aussi OSCE, Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, mai 2020.

[512] S. N. LYNCH and L. LAMBERT, *Sex ads website Backpage shut down by U.S. authorities*, Reuters, 6 avril 2018. Disponible sur : https://www.reuters.com/article/us-usa-backpage-justice-idUSKCN1HD2QP

[513] Audience le 5 octobre 2021 (donc attendre cette date pour développer). En principe les responsables du site sont protégés par la section 230 du Communication Decency Act qui déresponsabilise les hébergeurs face aux contenus publiés en ligne par leurs utilisateurs. Après ce scandal, les États-Unis ont adopté la loi Stop Enabling Sex Traffickers Act (ci-après « SESTA ») et la loi Allow States and Victims to Fight Online Sex Trafficking Act (ci-après « FOSTA ») qui sont rentrées en vigueur en 2018. Ces deux lois ont renforcé les outils juridiques contre la (pédo)pornographie ainsi que la traite des êtres humains en enlevant l'immunité des hébergeurs protégé jusqu'à ce moment par la section 230 du Communication Decency Act. Ces lois ont suscité des vives critiques face au danger potentiel pour tout site dont le contenu est généré par les utilisateurs et une menace pour le web libre et ouvert.

[514] M-A DAGRY et AFP agence, *Vivastreet : une information judiciaire ouverte pour « proxénétisme aggravé »*, 31 mai 2018. Disponible sur : https://www.lefigaro.fr/actualite-france/2018/05/31/01016-20180531ARTFIG00157-vivastreet-une-information-judiciaire-ouverte-pour-proxenetisme-aggrave.php

195. Outre à la traite d'êtres humains à des fins sexuels, nous assistons également à la diffusion d'annonces proposant « la vente » de personnel domestique, en particulier des femmes vulnérables habitant dans des pays à faible revenu[515]. Cette véritable forme d'esclavage et de profonde violation des droits fondamentaux est partagé librement sur Internet. En effet, si dans le « dark web »[516] ces types d'annonces existent depuis plusieurs années, nous assistons à leur diffusion dans des réseaux sociaux facilement accessibles comme Instagram[517].

196. Un autre facteur d'amplification est celui géographique car avec Internet les recruteurs peuvent désormais chercher des victimes au-delà de leur pays et sans avoir besoin d'intermédiaires ; alors qu'avant ils se concentraient sur des victimes à proximité[518]. Le recrutement acquiert ainsi une dimension internationale et transnationale. Cela mène à la possibilité de rentrer un contact avec un nombre plus important de victimes, par rapport au recrutement hors ligne, et également un nombre supérieur de « clients »[519].

197. Face à la recrudescence de ce phénomène, en décembre 2022 la Commission européenne a proposé la révision de la directive 2011/36/UE du Parlement européen et du Conseil, du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes[520]. Dans la proposition de révision, la Commission explique que pour renforcer la réponse de la justice pénale à la

---

[515] Voir O.PINNELL, J. KELLY, *Slave markets found on Instagram and other apps*, BBC News Arabic, 31 octobre 2019. Disponible sur : https://www.bbc.com/news/technology-50228549
[516] Il s'agit d'une partie d'Internet accessible seulement avec des logiciels spéciaux.
[517] La réponse des reseaux sociaux à ce sujet sera traité dans le chapiter VI de cette thèse.
[518] OSCE, Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, mai 2020, p.19.
[519] Voir notamment UNODC, *Global report on trafficking in persons*, 2020, p. 120, ainsi que V. BOUCHE, *Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking*, THORN, January 2018, p. 7.
[520] Directive 2011/36/UE du Parlement européen et du Conseil, du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes et remplaçant la décision-cadre 2002/629/JAI du Conseil.

traite des êtres humains il est nécessaire dans la directive de prendre en compte de manière explicite la dimension « cyber »[521].

198. Corollaire du recrutement, c'est le contrôle et les menaces exercés par les recruteurs envers les victimes. Ces comportements sont facilités par les nouvelles technologies et à Internet. Par exemple, le contrôle des victimes passe par l'envoi des messages réguliers, des images ou vidéos attestant leur présence dans un lieu donné. Mais cela passe, également, par la menace de diffusion de photos intimes à leurs proches afin de les humilier.

2. Le recrutement des mineurs à des fins sexuelles : le grooming

199. Au sujet du recrutement, il est important d'analyser le phénomène du grooming. Ce terme est utilisé pour décrire le fait de rentrer en contact avec un mineur dans l'objectif ultime d'en abuser sexuellement, de le faire prostituer et/ou de lui demander de produire des contenus pornographiques. Le grooming est sanctionné par l'art. 23 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels qui le définit comme « le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant […] dans le but de commettre à son encontre une infraction [à caractère sexuel] »[522]. Comme pour les autres formes de recrutement, ce phénomène n'est pas nouveau et n'est pas un résultat des nouvelles technologies mais plutôt ces dernières ont doté les agresseurs des nouveaux moyens et des nouvelles techniques. Cette infraction se caractérise le plus souvent par un adulte qui se fait passer par un enfant ou adolescent afin de rentrer en contact avec des mineurs et dans le but de commettre une infraction, le plus souvent sexuelle. Or, il semblerait impossible hors ligne de piéger un enfant en se faisant passer par un mineur alors qu'on est un homme adulte. Cela est au contraire

[521] Voir article 2 bis de la proposition de directive du Parlement européen et du Conseil modifiant la directive 2011/36/UE concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes.
[522] Article 23 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.

possible par l'intermédiaire de l'écran en envoyant de fausses photos et informations personnelles.

200. Pourquoi parlons-nous d'un phénomène d'amplification ? Comme expliqué précédemment, l'accessibilité aux victimes est devenue de plus en plus facile, à travers Internet les agresseurs peuvent aborder plusieurs victimes à la fois et notamment obtenir leur confiance dans un délai plus bref avant d'avoir un contact physique[523]. Ainsi, les nouvelles technologies permettent à travers l'anonymat de masquer l'identité de l'agresseur et, en particulier, ses caractéristiques personnelles, dont l'âge.

201. La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels « a été le premier instrument international à ériger en infraction pénale la sollicitation d'enfants à des fins sexuelles par le biais des technologies de l'information et de la communication »[524]. Elle met en cause la responsabilité pénale du présumé agresseur quand les messages sont suivis par une proposition de rencontre avec l'intention de commettre une infraction (une activité sexuelle ou la production de pornographie enfantine). Cette rédaction limite le champ d'action pour les situations où l'adulte a proposé intentionnellement à un mineur une rencontre afin de commettre une infraction et que cette proposition a été suivie par des actes. Le seul fait de s'être rendu au lieu de rendez-vous suffit pour entrainer la responsabilité pénale. Cependant le seul fait d'échanger des messages à caractère sexuel ou de commettre des infractions sexuelles sur Internet, par exemple le contraindre à envoyer de contenus sexuels, ne rentre pas dans le cadre de l'article 23. L'adulte pourra voir sa responsabilité engagée sur la base d'autres articles de la Convention, par exemple les articles 20 et 21, s'il a fait commettre, par la menace ou par la persuasion, des actes sexuellement explicites à l'enfant (envoi de photos ou actes sexuels devant la webcam) ou encore s'il a réussi à le recruter afin de participer à des spectacles pornographiques.

---

[523] T. OWEN, W. NOBLE, F. C. SPEED, *New Perspectives on Cybercrime*, Springer International Publishing AG, 1ère edition, 2017, p.82.

[524] Sollicitation d'enfants à des fins sexuelles par le biais des technologies de l'information et de la communication (« grooming »), Avis sur l'article 23 de la Convention de Lanzarote et sa note explicative, adopté par le Comité de Lanzarote le 17 juin 2015, p. 9.

202. Dans son avis du 17 juin 2015, le Comité de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels invite les parties à la Convention à élargir le champ d'action de l'article 23 afin d'intégrer également les infractions commises en ligne. En effet, la Convention a été dépassée par les nouvelles technologies et par les infractions de plus en plus commises sur Internet[525]. On voit dans la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels un début de réponse au danger du grooming en ligne mais avec des limites.

203. La Convention sur la cybercriminalité ne prévoit pas des dispositions spécifiques à ce phénomène mais elle encadre certaines de ses conséquences, par exemple la production de contenus pédopornographiques (cf. titre III de la Convention). En droit de l'Union européenne, l'instrument juridique de référence est la directive 2011/92/UE qui définit le grooming par son article 6 1) comme : « le fait pour un adulte de proposer, au moyen des technologies de l'information et de la communication, une rencontre à un enfant qui n'a pas atteint la majorité sexuelle, dans le but de commettre l'une des infractions visées à l'article 3, paragraphe 4, et à l'article 5, paragraphe 6, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre, est passible d'une peine maximale d'au moins un an d'emprisonnement ». Cette définition rappelle celle de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels. Au sein du même article, la directive appelle les États à prendre les mesures nécessaires pour punir également toute tentative de commettre les infractions *supra* citées au moyen des technologies de l'information et de la communication. Certains États au niveau européen et international sanctionnent le grooming en ligne s'il y a une intention de la part de l'agresseur de rencontrer le mineur hors ligne, d'autres le sanctionnent en tant que tel même en l'absence d'intention de voir la victime physiquement[526].

---

[525] *Ibid.* p. 13.
[526] Pour en savoir plus : International Centre for Missing & Exploited Children, *Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review*, First edition, 2017, p. 14. Disponible ici : https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf

204. Les pays de l'Union européenne ont intégré dans leur droit interne les dispositions de la directive européenne pour sanctionner le grooming. En France c'est l'article 227-22-1 du Code pénal qui sanctionne « Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique » avec deux ans d'emprisonnement et de 30 000 euros d'amende. Ce dernier, prévoit également des circonstances aggravantes, en effet, il prévoit que « ces peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende lorsque les propositions ont été suivies d'une rencontre ». En Belgique, c'est l'article 377quater du Code pénal, à la différence de l'approche française, le droit belge a considéré comme relevant du domaine pénal le grooming en ligne mais aussi hors ligne. En effet, le législateur a voulu considérer ce dernier comme circonstance aggravante de certaines infractions qui touchent la sphère sexuelle de l'enfant[527]. Par exemple, l'article 377-ter du Code pénal prévoit une augmentation de la peine lorsqu'une infraction sexuelle serait commise suite à la sollicitation du mineur non seulement virtuelle. En Espagne, le grooming est régi par l'article 183ter du Code pénal et aux Pays-Bas par l'article 248e du Code pénal.

205. Enfin, il faut tout de même souligner que l'utilisation d'Internet, si d'un côté permet une large dissémination de violences et recrutement ; de l'autre côté, elle permet de récolter plus des preuves sur les pédocriminels en comparaison au grooming hors ligne.

[527] I. SALVADORI, *L'adescamento di minori: il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia*, 2018, p. 44.

Conclusion du Chapitre II

206. Les comportements illicites sont facilités et amplifiés par les caractéristiques des réseaux sociaux. Non seulement des outils techniques comme l'utilisation des hashtags ou des bots les amplifient, mais aussi l'absence de maîtrise des contenus permet leur large diffusion et leur caractère indomptable. Ce phénomène d'amplification est illustré par le développement de nouvelles formes de violences sexuelles en ligne, comme le partage non consensuel de contenus à caractère sexuel, le voyeurisme digital ou le viol à distance. D'autres formes d'exploitation comme la traite des êtres humains à des fins sexuels ou le recrutement à des fins de terrorisme se développement et s'amplifient grâce à la facilité et à la rapidité des communications.

CONCLUSION DU TITRE I

207. La nécessaire reconnaissance des spécificités des violences en ligne - Appréhender le phénomène des cyberviolences implique la compréhension de spécificités du cyberespace et, plus particulièrement, des réseaux sociaux où ces violences s'exercent et s'amplifient. En effet, les caractéristiques des violences en ligne sont propres à l'environnement où elles s'exercent. D'abord, l'exécution des comportements illicites est facilitée par les qualités techniques d'Internet qui permettent aux utilisateurs de publier de contenus qui, potentiellement, resteront en ligne pour toujours et ne pourront pas être effacé. Ensuite, le caractère transnational et l'anonymat perçu par les utilisateurs facilitent la publication des contenus illicites et l'atteinte aux droits fondamentaux des individus. En témoigne l'évolution et les risques étendus envers le droit à la vie privée à cause de l'exposition d'informations personnelles des utilisateurs sur Internet. Enfin, ces caractéristiques d'Internet couplées aux outils techniques disponibles sur les réseaux sociaux et grâce à l'intelligence artificielle, comme les hashtags ou les deepfakes alimentent le phénomène d'amplification des cyberviolences. Les violences hors ligne peuvent désormais être exercées plus facilement en ligne et amplifiées grâce à la possibilité offerte par Internet de toucher en un clic un nombre important de personnes. La multiplicité d'acteurs, des victimes et de contenus, ainsi que l'absence de leur maîtrise nous amène à la nécessité de mieux les qualifier pour mieux les encadrer.

TITRE II : LA NECESSITE D'UNE QUALIFICATION UNIVERSELLE DES CYBERVIOLENCES

208. Le phénomène des cyberviolences existe depuis l'apparition d'Internet. Cependant, aujourd'hui, il n'existe pas une définition de cyberviolence en droit qui soit partagée par l'ensemble de la communauté internationale. Les utilisateurs font face à différentes formes de comportements illicites en ligne toujours en évolution grâce aux progrès technologiques.

Face à ces menaces certains États ont répondu à travers l'adoption de dispositions nationales encadrant certains comportements illicites. L'Union européenne et ses institutions, par exemple, ont également adopté des textes contraignants ou simplement étudié le phénomène et émis des recommandations. Cette situation a engendré une diversité de mesures adoptées protégeant les droits des individus sur Internet, mais aussi l'absence d'encadrement pour certains États, entrainant une différence de traitement entre les utilisateurs du cyberespace. De plus, la question de la définition de cyberviolences et de ses manifestations n'a pas été résolue, ce qui pourrait provoquer une réponse inadaptée et inefficace à ces comportements.

Au vu de ces éléments, il s'agira d'identifier la nécessité de mieux qualifier les cyberviolences (**Chapitre III**) pour ensuite déterminer si l'élaboration des règles minimales est nécessaire pour répondre de façon plus adaptée à ce phénomène (**Chapitre IV**).

Chapitre III : L'identification de la nécessité d'une qualification universelle

209. Les termes employés pour définir des comportements illicites sur Internet sont multiples. Des mots comme cyberharcèlement, cyberviolences, cyberhaine, cybersexisme sont utilisés en faisant un amalgame des infractions en ligne. Comme exposé dans l'introduction, cette analyse se concentre sur les cyberviolences de contenu que le rapport Robert[528] détermine comme les « infractions de droit commun commises au moyen de […] nouvelles technologies de l'information et de la communication »[529]. Cela implique l'utilisation de la technologie « pour véhiculer des contenus illicites » et « en tant que moyen permettant de faciliter la commission de toute autre infraction »[530]. En effet, le rapport Robert affirme que la cybercriminalité recouvre, d'une part, une catégorie spécifique d'infractions dirigées contre le système d'information, et, d'autre part, une seconde catégorie qui regroupe l'ensemble des infractions de droit commun commises au moyen de ces nouvelles technologies. La Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) adoptée en 2001, dénombre, quant à elle, cinq catégories d'infractions en ligne. La première concerne les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques (Titre 1 de la Convention), la deuxième, les infractions informatiques (Titre 2 de la Convention), la troisième, les infractions se rapportant au contenu (Titre 3 de la Convention), la quatrième, les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes (Titre 4 de la Convention) et enfin le premier protocole additionnel à la Convention[531] adopté en 2003 ajoute l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Dans les développements qui vont suivre, il s'agira d'étudier les infractions de la troisième catégorie ainsi que les comportements illicites sanctionnés dans le protocole additionnel.

---

[528] M. ROBERT (dir.), *Protéger les internautes, rapport sur la cybercriminalité, rapp. aux ministres de l'intérieur et de l'Economie, à la garde de Sceau et à la secrétaire d'État chargée du numérique,* juin 2014.
[529] *Ibid.* p. 13.
[530] *Ibid.* p. 13.
[531] Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, adopté le 28 janvier 2003.

210. L'Union européenne a adopté des dispositions pour rendre illégaux quatre types de contenus en ligne : les matériaux pédopornographiques, les discours de haine racistes et xénophobes, les contenus terroristes ainsi que les contenus qui portent atteinte à la propriété intellectuelle. Toutefois, au-delà de ces catégories, il n'y a pas d'harmonisation concernant les autres contenus illicites en ligne. En effet, certains peuvent être considérés illégaux par certains États membres de l'Union européenne, d'autres légaux mais nuisibles ou d'autres encore simplement légaux. Cela cause une multiplication des dispositions dans les droits nationaux qui amène à des traitements différents pour des mêmes faits entre citoyens de l'Union européenne.

211. Pour cela, dans le cadre de cette étude, il est apparu nécessaire de proposer des solutions pour améliorer l'encadrement des contenus illicites en ligne et l'harmonisation des droits nationaux afin de garantir une protection plus étendue de droits fondamentaux des utilisateurs sur Internet. La solution est celle de fixer une définition commune et universelle des cyberviolences pour permettre d'assurer une identification harmonieuse des infractions en ligne. Toutefois, il faudrait l'acceptation de cette définition par les États membres de l'Union européenne, du Conseil de l'Europe et des Nations Unies afin d'avoir un cadre juridique plus harmonieux au niveau régional et international. Comme il a été souligné dans les chapitres précédents, le caractère transnational des cyberviolences nécessite une réponse coordonnée au niveau international et non seulement au niveau national. En effet, plusieurs facteurs transnationaux se mêlent en complexifiant l'encadrement et la sanction.

212. Pour proposer une définition universelle des cyberviolences, il est d'abord nécessaire de montrer qu'aucun des instruments européens et internationaux n'en prévoit une. Cependant des définitions « de travail » utilisées par la doctrine ou par les juges européennes, ainsi que des définitions spécifiques pour certains comportements illicites existent au niveau national, européen et international (**Section I**). Ensuite, nous allons analyser les conséquences sur les utilisateurs d'Internet causées par l'absence ou la multiplication des dispositions juridiques nationales sur les cyberviolences. Il semble important d'élaborer une définition de cyberviolences qui permette de rassembler les comportements illicites sur Internet mais qui ne devienne pas rapidement

obsolète compte tenu des développements constants des nouvelles technologies (**Section II**).

Section I : L'absence d'une définition et d'une qualification universelle de cyberviolences

213. On constate l'absence d'une définition universelle de cyberviolences au sein de l'Union européenne ainsi que dans les traités internationaux. Malgré cela, il est intéressant de montrer que certaines études et des rapports élaborés afin de mieux comprendre ces phénomènes présentent des définitions intéressantes. Ces définitions, élaborées par la société civile ou par des organisations régionales comme le Conseil de l'Europe, sont utiles pour apprécier l'état actuel des travaux sur les comportements illicites en ligne.

214. Ainsi, il est nécessaire d'analyser ce qui est prévu dans les droits nationaux des États, qu'ils soient membre de l'Union européenne ou du Conseil de l'Europe. En effet, même si seulement un État européen a adopté une définition de cyberviolences, des définitions éparses de contenus illicites ont vu le jour pour sanctionner ces comportements en ligne (**§I**). Cela cause une diversification des dispositions juridiques qui a des conséquences négatives sur la protection des droits fondamentaux des utilisateurs (**§II**).

I. Des définitions existantes mais fragmentaires

215. Dans les développements qui vont suivre, il s'agira d'analyser les définitions existantes des comportements illicites sur Internet et du terme cyberviolences. D'un côté, il est important de montrer que les acteurs européens et internationaux ont élaboré des définitions principalement en relation aux cyber violences à l'égard des femmes (**A**). De l'autre, que les États participent activement à l'adoption des lois nationales contre les cyberviolences, même si seule la Roumanie s'est dotée d'une définition de cyberviolence, focalisée exclusivement sur les cyberviolences domestiques (**B**).

A. Une amorce cohérente de définition par les acteurs européens et internationaux

216. Dans les travaux sur les violences en ligne, apparaît, en parcourant la doctrine et les rapports des organisations internationales, qu'une grande partie de cette littérature est consacrée aux cyberviolences à l'égard des femmes et des filles. Cela est probablement dû au fait que les femmes et les filles sont très exposées aux comportements illicites. Cela a été souligné à plusieurs reprises dans les enceintes onusiennes et européennes, en témoignent les rapports et les résolutions du Parlement européen et du Conseil[532], des agences européennes[533] ou encore les résolutions des Nations Unies[534]. Plus généralement, on constate que ce sont les personnes les plus vulnérables qui font l'objet des violences en ligne. Selon certaines caractéristiques des victimes, on constate que les violences en ligne peuvent prendre différentes formes. Par exemple, les comportements illicites subis par les jeunes garçons sont distincts de ceux infligés aux jeunes filles, les premiers sont plus sujets à des insultes et à des menaces physiques, alors que les filles sont plus exposées aux violences sexuelles et sexistes[535]. En outre, les femmes ont plus de risques d'être exposées au cyberharcèlement y compris la traque furtive qui peut être une forme de violence conjugale.

---

[532] Voir par exemple N. LOMBA, C. NAVARRA and M. FERNANDES, *Combating gender-based violence: Cyber violence European added value assessment*, European Parliamentary Research Service (EPRS), European Parliament, March 2021. Ainsi que la résolution du Parlement européen du 12 septembre 2017 sur la proposition de décision du Conseil portant conclusion, par l'Union européenne, de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (COM(2016)0109 – 2016/0062(NLE) et la résolution du Parlement européen du 14 décembre 2021 contenant des recommandations à la Commission sur la lutte contre la violence fondée sur le genre : cyberviolence, 2020/2035(INL).

[533] Agence des droits fondamentaux de l'Union européenne, *La violence à l'égard des femmes : une enquête à l'échelle de l'Union européenne,* 5 mars 2014. Disponible sur : *https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance-oct14_fr.pdf* Voir également : EIGE, *Cyberviolence à l'égard des femmes et des filles*, 23 juin 2017. Disponible sur : https://eige.europa.eu/publications/cyber-violence-against-women-and-girls

[534] Voir notamment Assemblée Générale des Nations Unies, Promotion de la Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus : protection des défenseuses des droits de l'homme/défenseurs des droits des femmes, Résolution adoptée par l'Assemblée générale le 18 décembre 2013, Soixante-huitième session, A/RES/68/181. Voir également Comité pour l'élimination de la discrimination à l'égard des femmes, Recommandation générale n° 35 sur la violence à l'égard des femmes fondée sur le genre, portant actualisation de la recommandation générale n° 19, 26 juillet 2017, CEDAW/C/GC/35.

[535] Pew Research Center, *The State of Online Harassment*, Janvier 2021. https://www.pewresearch.org/Internet/2021/01/13/the-state-of-online-harassment/

217. À cet égard, plusieurs études ont été focalisées sur ces violences de genre pour essayer de mieux les appréhender et cela a donné lieu à des réflexions et définitions intéressantes sur les cyberviolences.

1. Les définitions existantes se fondant sur les violences à l'égard des femmes et des filles

218. D'abord, le Comité consultatif de l'égalité des chances entre les femmes et les hommes [536] de la Commission européenne dans son Avis sur la lutte contre la violence en ligne à l'égard des femmes[537], publié le 1er avril 2020, définit les cyberviolences comme suit :

> « Cyberviolence against women is an act of gender-based violence perpetrated directly or indirectly through information and communication technologies that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women and girls, including threats of such acts, whether occurring in public or private life, or hindrances to the use of their fundamental rights and freedoms. Cyberviolence against women is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing without consent, image-based sexual abuse, hacking, identity theft, and direct violence. Cyberviolence is part of the continuum of violence against women: it does not exist in a vacuum; rather, it both stems from and sustains multiple forms of offline violence. »[538].

---

[536] Crée suite à l'adoption de la décision de la Commission européenne du 16 juin 2008 relative à la création d'un comité consultatif de l'égalité des chances entre les femmes et les hommes (2008/590/EC), le Comité consultatif de l'égalité des chances entre les femmes et les hommes a « pour tâche d'assister la Commission dans l'élaboration et dans la mise en œuvre des actions de la Communauté visant à promouvoir l'égalité des chances entre les femmes et les hommes, et de favoriser l'échange permanent des expériences, politiques et pratiques pertinentes, en la matière, entre les États membres et entre les divers acteurs intéressés » (article 2 de la décision 2008/590/EC).

[537] Advisory Committee on Equal Opportunities for Women and Men, *Opinion on combatting online violence against women*, 1st April 2020. Disponible sur : https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/opinion_online_violence_against_women_2020_en.pdf.

[538] *Ibid*. p. 4. Traduction de l'autrice : « La cyberviolence à l'égard des femmes est un acte de violence basé sur le genre perpétré directement ou indirectement par le biais des technologies de l'information et de la communication, qui entraîne ou est susceptible d'entraîner des dommages ou des souffrances physiques,

219. Le Comité justifie sa définition en mettant en avant son étendue qui peut recouvrir plusieurs situations. Ainsi, il considère les cyberviolences à l'égard des femmes « as part of a continuum of violence against women and not as a « virtual » phenomenon separated from violence « in real life » »[539]. Cette notion de « continuum » est soulignée par plusieurs spécialistes des droits des femmes. Cela avait été relevé également par le Groupe d'experts ur la lutte contre la violence à l'égard des femmes et la violence domestique (ci-après « GREVIO »)[540] qui exposait « the importance of viewing cyber violence and offline forms of violence against women and girls as an expression of the same phenomenon, namely gender-based violence. Online violence against women and girls should therefore be seen as a continuum of offline violence and as a means to maintain women in an inferior position in the digital sphere and in real life »[541]. Ce constat est également partagé par la Rapporteuse spéciale sur la violence contre les femmes dans son rapport du 18 juin 2018 où elle affirmait que les violences dont font l'objet les femmes et les filles en ligne « s'inscrivent dans un ensemble continu de formes multiples, récurrentes et interdépendantes de violence fondée sur le genre à l'égard des femmes »[542]. Dans ce même document, la Rapporteuse spéciale donne une définition de

---

sexuels, psychologiques ou économiques pour les femmes et les filles, y compris la menace de tels actes, que ce soit dans la vie publique ou privée, ou des entraves à l'utilisation de leurs droits et libertés fondamentaux. La cyberviolence à l'égard des femmes inclut, entre autres : la violation de la vie privée, la traque, le harcèlement, les discours de haine fondés sur le genre, le partage de contenu personnel sans consentement, les abus sexuels fondés sur l'image, le piratage, l'usurpation d'identité et la violence directe. La cyberviolence s'inscrit dans le continuum des violences à l'égard des femmes : elle n'existe pas en vase clos, mais découle de multiples formes de violence hors ligne qu'elle entretient ».

[539] *Ibid,* p. 4. Traduction de l'autrice : « comme faisant partie d'un continuum de la violence à l'égard des femmes et non comme un phénomène « virtuel » séparé de la violence « dans la vie réelle » ».

[540] Le GREVIO est un organe spécialisé indépendant qui a comme mission de contrôler et de conseiller les États sur la mise en œuvre effective de la Convention d'Istanbul. Celui-ci est composé d'expertes et experts indépendants et qualifiés dans les droits humains, les violences à l'égard des femmes et des hommes ainsi que dans la protection et la prise en charge de victimes des violences. Pour plus d'informations, voir : https://www.coe.int/fr/web/istanbul-convention/grevio

[541] N. LOMBA, C. NAVARRA and M. FERNANDES, *Combating gender-based violence: Cyber violence European added value assessment,* European Parliamentary Research Service (EPRS), European Parliament, March 2021, p. 98. Traduction de l'autrice : « L'importance de considérer la cyber-violence et les formes de violence hors ligne à l'encontre des femmes et des filles comme l'expression d'un même phénomène, à savoir la violence basée sur le genre. La violence en ligne contre les femmes et les filles doit donc être considérée comme un continuum de la violence hors ligne et comme un moyen de maintenir les femmes dans une position d'infériorité dans la sphère numérique et dans la vie réelle ».

[542] Conseil des droits de l'Homme, *Rapport de la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences concernant la violence en ligne à l'égard des femmes et des filles du point de vue des droits de l'homme*, A/HRC/38/47, 18 juin 2018.

la cyberviolence à l'égard de femmes en précisant que : « la définition de la violence en ligne à l'égard des femmes couvre tout acte de violence fondé sur le genre qui est commis, facilité ou aggravé pleinement ou partiellement par l'utilisation des TIC [*ndlr.* Technologies de l'Information et de la communication], par exemple les téléphones portables et les smartphones, Internet, les plateformes des médias sociaux ou les courriers électroniques, et qui vise une femme parce qu'elle est une femme ou touche spécialement la femme »[543]. L'avantage de cette définition est dû, d'abord, à son étendue et, ensuite, à l'appréciation des cyberviolences comme un continuum des violences à l'égard des femmes hors ligne et non comme un phénomène « virtuel » séparé de la violence « dans la vie réelle ».

220. Ainsi, même si la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique ne contient pas de dispositions spécifiques aux cyberviolences, l'article 34 du rapport explicatif de celle-ci spécifie que les comportements illicites qui constituent le harcèlement comprennent également le contexte virtuel. En effet, cet article prévoit que « le comportement menaçant peut consister dans le fait de suivre de manière répétée une personne, d'engager une communication non désirée avec une personne, ou de faire savoir à une personne qu'elle est épiée. Ceci inclut le fait de suivre physiquement une personne, d'apparaître sur son lieu de travail, son centre sportif ou son établissement scolaire, de même que *la suivre dans le monde virtuel* (espaces de discussion, sites de réseaux sociaux, etc.). Une « communication non désirée » désigne la poursuite d'un *contact actif quel qu'il soit avec la victime par n'importe quel moyen de communication disponible, notamment les outils de communication modernes et les TIC* »[544]. Le rapport poursuit ensuite en spécifiant qu'« un « comportement menaçant » peut inclure le fait de […] constituer de fausses identités ou de diffuser de fausses informations en ligne. »[545].

---

[543] Conseil des droits de l'Homme, *Rapport de la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences concernant la violence en ligne à l'égard des femmes et des filles du point de vue des droits de l'homme*, A/HRC/38/47, 18 juin 2018, p. 7.
[544] Conseil de l'Europe, *Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence*, 11 May 2011, Council of Europe Treaty Series - No. 210, point 182. Italique de l'autrice.
[545] *Ibid.* point 183.

221. De plus, l'Institut européen pour l'égalité entre les hommes et les femmes (« EIGE ») qui a mené une étude sur les cyberviolences à l'égard des femmes et des filles[546], ne se prononce pas sur une définition précise mais renvoie vers les différentes formes de comportements illicites qui caractérisent les cyberviolences à l'égard des femmes. En particulier, les insultes, le harcèlement fondé sur le genre et la divulgation non consentie d'images intimes[547]. Dans son étude, l'Institut se concentre surtout sur les cyberviolences entre partenaires intimes et précise que, comme pour les violences hors ligne, elles sont multiformes : sexuelles, psychologiques mais aussi économiques.

222. L'UN Broadband Commission for digital development[548] dans son rapport sur les cyberviolences à l'égard des femmes et des filles donne des indications sur la terminologie et les définitions de cyberviolences. Cependant, ce faisant, la Commission, comme l'Institut européen pour l'égalité entre les hommes et les femmes, ne donne pas une définition unitaire, elle définit plutôt le terme « cyber » et plusieurs comportements illicites pouvant caractériser les cyberviolences. L'UN Broadband Commission estime que :

> « The term « cyber » is used to capture the different ways that the Internet exacerbates, magnifies or broadcasts the abuse. The full spectrum of behaviour ranges from online harassment to the desire to inflict physical harm including sexual assaults, murders and suicides. Cyber violence takes different forms, and the kinds of behaviours it has exhibited since its inception has changed as rapidly — and, unchecked, will continue to evolve — as the digital and virtual platforms and tools have spread »[549].

---

[546] EIGE, *Cyberviolence à l'égard des femmes et des filles*, 23 juin 2017. Disponible sur : https://eige.europa.eu/publications/cyber-violence-against-women-and-girls
[547] *Ibid.* p. 2.
[548] La Commission a été créé en mai 2010 par l'Union Internationale des télécommunications (UIT) ainsi que par l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO). Elle est composée par des dirigeants d'entreprise, de responsables politiques et d'experts des organisations internationales et de la société civile et a comme objectif de « renforcer l'importance du haut débit dans l'agenda politique international, et d'étendre l'accès au haut débit dans chaque pays comme élément clé pour accélérer les progrès vers les objectifs de développement nationaux et internationaux ». Pour plus d'informations sur la Commission voir : https://broadbandcommission.org/about-us/
[549] UN Broadband Commission for digital development working group, *Cyberviolence against women and girls, A world-wide wake-up call*, 2015. Traduction de l'autrice « Le terme « cyber » est utilisé pour décrire les différentes façons dont l'Internet exacerbe, amplifie ou diffuse les abus. Le spectre complet des comportements va du harcèlement en ligne à la volonté d'infliger des dommages physiques, y compris des agressions sexuelles, des meurtres et des suicides. La cyberviolence prend différentes formes, et les types de comportements qu'elle

223. Enfin, un acteur de premier plan sur les sujets des violences en ligne est le Conseil de l'Europe qui s'intéresse depuis des années aux cyberviolences. Au sein du Conseil de l'Europe, le Comité de la Convention sur la cybercriminalité[550] représente les États parties à la Convention du Conseil de l'Europe sur la cybercriminalité. Ce dernier a publié une étude cartographique sur la cyberviolence dans lequel il définit la cyberviolence comme :

> « L'utilisation de systèmes informatiques pour causer, faciliter ou menacer de causer à des personnes de la violence qui entraine ou est susceptible d'entrainer un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques et peut comprendre l'exploitation de leur situation, de leurs caractéristiques ou de leur vulnérabilité »[551].

224. Le Comité de la Convention explique le choix de cette définition en disant avoir adapté au contexte « cyber » deux articles de deux conventions internationales. D'un côté, il se réfère à l'article 3 de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique. Cet article définit la violence à l'égard des femmes comme « une violation des droits de l'homme et une forme de discrimination à l'égard des femmes et désigne tous les actes de violence sexiste qui causent ou sont susceptibles de causer aux femmes un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques, y compris la menace de tels actes, la contrainte ou la privation arbitraire de liberté, que ce soit en public ou dans la vie privée »[552]. De l'autre côté, il fait référence à l'article 1 de la Convention interaméricaine sur la prévention, la sanction et l'élimination de la violence contre les femmes (Convention de Belém do Para) qui définit la violence contre les femmes comme

---

présente depuis son apparition ont évolué aussi rapidement - et, si rien n'est fait, continueront d'évoluer - que les plateformes et outils numériques et virtuels se sont répandus ».

[550] Pour plus d'informations sur son fonctionnement et ses missions voir le règlement intérieur du Comité, disponible ici : https://rm.coe.int/t-cy-rules-of-procedure/1680a00f33

[551] Conseil de l'Europe, Comité de la Convention sur la cybercriminalité, *Étude cartographique sur la cyberviolence*, 2018, p.5.

[552] Article 3 de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique.

« tout acte ou comportement, fondé sur le sexe, qui cause la mort ou un préjudice ou des souffrances physiques, sexuelles ou psychologiques aux femmes, que ce soit dans la sphère publique ou privée »[553]. Comme expliqué par le Comité de la Convention sur la cybercriminalité, ces définitions reflètent le caractère multiforme des violences qui ne se limitent pas aux dommages corporels mais qui concernent également des atteintes sexuelles, phycologiques et/ou économiques.

225. Cette définition a été reprise pour la première et unique fois dans un arrêt par la Cour européenne des droits de l'Homme *Buturuga c. Roumanie*[554]. Ce même arrêt reprend également les rapports précités de l'Institut européen pour l'égalité entre les hommes et les femmes ainsi que de l'UN Broadband Commission for digital development.

226. Pour conclure, au sein de l'Union européenne, une résolution a été adoptée en décembre 2021 par le Parlement européen pour adopter une définition de l'infraction de cyberviolence à caractère sexiste[555], cela afin de reconnaître les spécificités de ces violences qui touchent majoritairement les femmes et les filles[556].

227. L'inspiration donnée par des instruments juridiques encadrant les violences à l'égard des femmes est très intéressante et juste, à la fois car elle reflète la multiplicité des formes de violences mais également la vulnérabilité des victimes. Toutefois, ces entités ne sont pas les seules à avoir formulé des définitions, en effet, au niveau national un mouvement législatif s'est enclenché. Même si la Roumanie est pour l'instant le seul État à avoir adopté une définition des cyberviolences, les autres États membres de l'Union européenne et du Conseil de l'Europe ont pris des mesures et définit certains comportements illicites en ligne.

---

[553] Article 1 de la Convention interaméricaine sur la prévention, la sanction et l'élimination de la violence contre les femmes.
[554] Cour EDH, 11 février 2020, *Buturuga c. Roumanie,* req. n° 56867/15, §40.
[555] Résolution du Parlement européen du 14 décembre 2021 contenant des recommandations à la Commission sur la lutte contre la violence fondée sur le genre : cyberviolence, 2020/2035(INL).
[556] N. LOMBA, C. NAVARRA and M. FERNANDES, *Combating gender-based violence: Cyber violence European added value assessment,* European Parliamentary Research Service (EPRS), European Parliament, March 2021. Concernant les cyberviolences à l'éncontre des femmes journalistes, voir J. POSETTI, N. ABOULEZ, K. BONTCHEVA et autres, *Violence en ligne à l'égard des femmes journalistes : un aperçu mondial des incidences et impacts,* UNESCO et ICFJ, 2021. Disponible sur : https://www.icfj.org/sites/default/files/2021-03/Online%20Violence%20Against%20Women%20Journalists%20Global%20Snapshot%20French.pdf

B. Le cas isolé de la Roumanie, seul État ayant adopté une définition de cyberviolences

228. La Roumanie est le seul État ayant inscrit dans ses textes normatifs le terme « cyberviolence ». Et, à nouveau, comme pour les définitions étudiées dans le paragraphe précédent, cette définition s'inscrit dans le cadre des cyberviolences à l'égard des femmes et des filles et plus particulièrement de violences domestiques. Plus qu'une définition unitaire, il s'agit d'une liste de comportements illicites en ligne commis à l'égard des femmes. En effet, la loi n° 106 du 3 juillet 2020 a introduit les comportements illicites en ligne dans le Code pénal roumain en modifiant la loi n° 217/2003 sur la prévention et la lutte contre la violence domestique adoptée le 22 mai 2003. En particulier, il a été ajouté à l'article 4, paragraphe 1, qui énonce les différentes formes de violence domestiques, un nouveau point (h) qui inclut comme forme de violence domestique la « la cyber-violence - le harcèlement en ligne, les messages en ligne incitant à la haine fondée sur le sexe, la traque en ligne, les menaces en ligne, la publication non consensuelle d'informations et de contenus graphiques intimes, l'accès illégal à l'interception de communications et de données privées, et toute autre forme d'utilisation abusive des technologies de l'information et de la communication par le biais des ordinateurs, les téléphones portables ou autres dispositifs similaires qui utilisent les télécommunications ou peuvent se connecter à Internet, transmettre et utiliser des plateformes sociales ou de messagerie électronique, dans le but de couvrir de honte la victime, de l'humilier, de l'effrayer, de la menacer ou de la réduire au silence »[557]. La loi prévoit également l'intégration d'une perspective d'égalité entre les femmes et les hommes dans toutes les politiques, programmes et recherche sur l'intelligence artificielle pour éviter des risques qui perpétuent le sexisme, les stéréotypes de genre et la cyberviolence[558]. Elle prévoit enfin des mesures à destination du Ministère des

[557] Voir article 4, paragraphe 1 (h), de la loi n°106 portant modification et complément de la loi n° 217/2003 sur la prévention et la lutte contre la violence domestique. Disponible en roumain ici : http://legislatie.just.ro/Public/DetaliiDocument/227611
[558] *Ibid.* article 8, paragraphe 3.

transports, des infrastructures et des communications pour prévenir et répondre aux cyberviolences[559].

229. Toutefois, il est important de souligner que ces dispositions concernent uniquement les violences domestiques, pour cela les victimes ne pourront pas s'en prévaloir pour des faits commis par des inconnus ou des personnes connues mais en dehors de la sphère familiale. Pour cela, au-delà de la cyberviolence conjugale, pour sanctionner les autres comportements illicites il faudra appliquer d'autres dispositions qui ne sont pas spécifiques à la sphère virtuelle. En effet, comme pour la majeure partie des États qui n'ont pas prévu des mesures spécifiques pour prévenir et sanctionner certains comportements illicites il faut utiliser des dispositions déjà existantes. Mais, même si certaines de ces mesures sont destinées aux mêmes comportements, les États n'adoptent pas le même type d'encadrement et ne sanctionnent pas nécessairement les mêmes comportements.

230. Or, il est intéressant d'étudier les différentes appréciations des États à ce sujet. Il faut rappeler que, concernant les contenus pédocriminels ainsi que les contenus de propagande et recrutement terroriste, les États membres de l'Union européenne et du Conseil de l'Europe ont adopté plusieurs mesures après l'adoption de dispositions législatives européennes contraignantes[560] et la ratification des conventions internationales[561]. Ce faisant l'encadrement sur ces sujets est assez homogène[562]. Pour cela, il sera opportun de se concentrer sur d'autres typologies de comportements illicites

---

[559] *Ibid*. article 9, paragraphe 3, de la loi n°106.

[560] Concernant les contenus pédopornographiques et les violences sexuelles à l'encontre des mineurs, voir notamment la directive 2011/92/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil. Voir également la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels ou la Convention du Conseil de l'Europe sur la cybercriminalité. Concernant les contenus terroristes en ligne voir notamment le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

[561] Convention relative aux droits de l'enfant des Nations unies, 20 novembre 1989.

[562] Surtout concernant les mesures contre la pédopornographie et le grooming au vu de la ratification par la plupart des États du Conseil de l'Europe de la Convention du Conseil de l'Europe sur la cybercriminalité dont l'article 9 sur pornographie enfantine. Ainsi que, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels. De plus au sein de l'Union européen, par l'adoption suivie de la transposition dans le droit national de la directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants.

comme les atteintes sexuelles ou encore la haine en ligne dont la définition et le traitement diffère d'un État à l'autre.

II. Les conséquences de l'absence d'une définition universelle : le pluralisme « désordonné »

231. Pour parler de la multiplication des dispositions juridiques nationales sur les cyberviolences, nous pouvons utiliser la notion de « pluralisme juridique » qui renvoie à la dispersion et à la multiplicité des dispositions juridiques. Nous utilisons le terme « désordonné » en faisant un parallèle *a contrario* de la pensée de Mireille Delmas-Marty qui parlait de « pluralisme ordonné »[563] comme moyen de dépasser la contradiction, respecter la diversité tout en permettant une harmonie d'ensemble[564]. En effet, on constate aujourd'hui un pluralisme désordonné avec une diversité d'encadrement juridique sur les cyberviolences, ou bien une absence de dispositions. La solution serait de tendre vers un pluralisme ordonné afin qu'il y ait une harmonisation des dispositions juridiques pour garantir une protection *a minima* des utilisateurs. En droit international, on emploie le concept de fragmentation[565], appréhendé comme « la notion [qui] sert à désigner la multiplication des conflits systémiques et normatifs qui découleraient de la diversification du droit […] »[566]. La doctrine n'a pas une position unanime sur ce phénomène, pour certains auteurs elle a une connotation négative car ils la considèrent

---

[563] M. DELMAS- MARTY, Le pluralisme ordonné, *Les forces imaginantes du droit (II)*, Seuil, 2006.
[564] M. DELMAS- MARTY, *Le pluralisme ordonné et les interactions entre ensembles juridiques*, Texte inspiré d'une conférence présentée le 26 janvier 2006 à l'Université Bordeaux IV sur l'invitation de M. C. Ponthoreau, par renvoi au livre M. DELMAS- MARTY, Le pluralisme ordonné, *Les forces imaginantes du droit (II)*, Seuil, 2006.
[565] B. DURAND-JAMIS, « Propos introductifs : la polarisation de la notion de fragmentation, entre unité et diversité du droit », *La Revue des droits de l'homme*, 15, 2019. Sur la fragmentation du droit international public voir : P. M. DUPUY, *La fragmentation du droit international ou des perceptions qu'on en a ?, EUI Working Paper*, n° 14, 2006 et S. MOUNDOUNGA NTSIGOU, *La fragmentation du droit international public : l'œuvre de codification à la lumière de la fragmentation du droit international*, Thèse, Université de Strasbourg, 2013.
[566] M. KOSKENNIEMI, *Rapport préliminaire sur la fragmentation du droit international : difficultés découlant de la diversification et de l'expansion du droit international*, Groupe d'étude sur la fragmentation, Commission du droit international, ILC(CVI)/SG/FIL/CRD.1, 2004, p. 1, dont la référence m'a été indiquée par A. C MARTINEAU, « La fragmentation du droit international : un renouvellement répété de la pensée ? » (2006), International Law: Do We Need It?, Conférence biennale de la Société Européenne de Droit International, Paris 18-20 mai 2006.

comme « l'érosion du droit international général, [causant] l'apparition de décisions de justice contradictoires, la course au mieux-disant judiciaire et la perte de sécurité juridique »[567]. Pour d'autres, au contraire, il s'agirait d'un simple problème technique qui pourrait être résolu avec la coordination et la rationalisation[568].

232. Dans cette étude, nous analyserons la multiplication de dispositions juridiques, causée, en partie, par l'absence d'une définition universelle de cyberviolences. Ainsi nous étudierons les conséquences de tendre vers plus d'« ordre », d'harmonisation et de coordination. Pour cela, il s'agira d'analyser la multiplication des dispositions juridiques et l'absence d'encadrement dans les droits nationaux (**A**), pour ensuite étudier les risques pour la protection des droits fondamentaux à l'égard des ressortissants des États membres de l'Union européenne et du Conseil de l'Europe (**B**).

A. Les différences d'encadrement dans les droits nationaux

233. Comme on l'a vu précédemment, aucun État membre de l'Union européenne, sauf la Roumanie, n'a défini dans le droit interne les cyberviolences. Toutefois, certains États ont adopté des mesures et des définitions pour certains comportements illicites en ligne.

1. Des définitions éparses des comportements illicites en ligne par les acteurs étatiques

234. L'Union européenne partage avec ses États membres la compétence de légiférer et d'adopter des actes contraignants dans les domaines qui rentrent dans le champs d'application de l'« Espace de liberté, de sécurité et de justice ». Ce dernier poursuit plusieurs objectifs et, en particulier, celui de prévenir et lutter contre la criminalité, le racisme et la xénophobie « par des mesures de coordination et de coopération entre autorités policières et judiciaires et […] si nécessaire, par le rapprochement des

---

[567] M. KOSKENNIEMI, *Rapport préliminaire sur la fragmentation du droit international : difficultés découlant de la diversification et de l'expansion du droit international*, Groupe d'étude sur la fragmentation, Commission du droit international, ILC(CVI)/SG/FIL/CRD.1, 2004, p. 12.
[568] Pour une analyse critique du débat sur la fragmentation, voir : A.C MARTINEAU, *Une analyse critique du débat sur la fragmentation du droit internationa*l, Thèse, Université Panthéon-Sorbonne - Paris I, 2013.

législations pénales »[569]. Pour cela, la protection des droits humains et des libertés fondamentales est une compétence partagée entre l'Union et les États, c'est-à-dire que les États membres peuvent exercer leur compétence seulement si l'Union européenne n'a pas exercé la sienne ou si elle a décidé de ne pas l'exercer[570].

235. Or, lorsque des mesures ne sont pas adoptées au niveau européen, les États peuvent adopter ou non des mesures législatives pour lutter contre certains comportements illicites. Il a été déjà démontré que, aujourd'hui, il n'existe pas de mesures spécifiques qui encadrent la totalité des comportements illicites en ligne et qui pourraient être transposées dans les États membres de l'Union. En l'absence de ces mesures, certains États adoptent des dispositions pour sanctionner les infractions sur Internet. Toutefois, ces mesures peuvent être différentes d'un État à l'autre. Cela alimente le pluralisme juridique et des inégalités de traitement pour les ressortissants de l'Union européenne. On peut l'illustrer cela à travers des exemples des législations nationales. En effet, certains États ont adopté des dispositions *ad hoc* pour sanctionner des comportements illicites en ligne, d'autres utilisent des dispositions déjà existantes en ajoutant la dimension « cyber » comme circonstance aggravante. D'autres encore ne sanctionnent simplement pas certaines infractions.

236. Il ressort que les États membres ne définissent pas de la même manière certains comportements ou les sanctionnent de manière différente. Pour analyser ce pluralisme, plusieurs comportements illicites seront étudiés, en particulier la diffusion des contenus à caractère sexuel non consensuelle (**a**), le voyeurisme digital (**b**) et le cyberharcèlement (**c**).

a) <u>L'encadrement de la diffusion non consensuelle de contenus à caractère sexuel</u>

237. Plusieurs États membres de l'Union européenne ont adopté des dispositions législatives *ad hoc* pour définir et encadrer la diffusion non consensuelle de contenus à

[569] Article 67 du Traité sur le fonctionnement de l'Union européenne.
[570] Article 4 du Traité sur le fonctionnement de l'Union européenne.

caractère sexuel, il s'agit notamment de la France, l'Italie, la Belgique, les Pays-Bas, Malte, l'Espagne, l'Irlande, le Portugal, la Suède et la Pologne[571]. En France, l'article 226-1 du Code pénal punit d'un an d'emprisonnement et de 45 000 euros d'amende le fait de fixer, enregistrer et transmettre sans le consentement l'image d'une personne se trouvant dans un lieu privé. De plus, l'article 226-2 sanctionne également 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 par l'article 226-1 »[572]. Or, l'article 67 de la loi pour une République Numérique du 7 octobre 2016, est venu aggraver les peines prévues à l'article 226-2-1 lorsque le contenu en question est à caractère sexuel. En effet, celui-ci prévoit 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.
>
> 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 »[573].

238. De plus, l'article 226-2-1 al. 2 sanctionne une pratique courante dans les affaires de « revenge porn », c'est-à-dire le fait de donner le consentement à une personne de capturer des contenus à caractère sexuel mais de ne pas lui donner le consentement pour les diffuser à des tiers.

---

[571] Voir : S. DE VIDO and L. SOSA, *Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence*, Directorate-General for Justice and Consumers, European Commission, 2021, pp. 137-138.
[572] Article 226-1 du Code pénal français.
[573] Article 226-2-1 du Code pénal français, introduit grâce à l'adoption de la loi pour une République Numérique du 7 octobre 2016.

239. En Italie, la loi pour la défense des victimes de violence domestique du 19 juillet 2019[574] a introduit l'article 612 ter qui punit quiconque que, après avoir réalisé ou volé des images ou vidéos à caractère sexuel destinés à être privés, les envoie, publie, fournit ou diffuse sans le consentement de la personne qui y est représentée. La sanction prévue par la loi italienne consiste entre un an et six ans d'emprisonnement et une amende de 5 000 à 15 0000 euros[575].

240. En comparant la loi française et la loi italienne, il ressort que le contenu de l'infraction est le même mais la sanction diverge. En effet, alors que la loi française met plus l'accent sur une amende monétaire, la loi italienne prévoit plus d'années de réclusions et une indemnisation moins importante. Les deux États prévoient une aggravation de la peine lorsque les actes sont commis par le conjoint, le partenaire ou ex partenaire de la victime[576].

241. Toutefois, d'autres États membres ne disposent pas des dispositions qui reconnaissent les spécificités de cette infraction, c'est le cas notamment en Roumanie ou Hongrie[577].

b) L'encadrement du voyeurisme digital

242. Il est intéressant d'analyser l'approche de certains États vis-à-vis du voyeurisme digital. La définition juridique n'est pas universelle, toutefois certaines similitudes ont été identifié dans les droits nationaux.

243. En France, la loi du 3 août 2018 a introduit à travers l'article 226-3-1 du Code pénal l'infraction de voyeurisme digital qui est définit comme « le fait d'user de tout moyen afin d'apercevoir les parties intimes d'une personne que celle-ci, du fait de son habillement ou de sa présence dans un lieu clos, a caché à la vue des tiers, lorsqu'il est commis à l'insu ou sans le consentement de la personne »[578]. L'article prévoit également

[574] Legge n.69, *Tutela delle vittime di violenza domestica e di genere*, 19 luglio 2019 (GU 25.07.2019).
[575] Article 612 ter du Code pénal italien.
[576] Article 226-2-1 du Code pénal français et article 612 ter du Code pénal italien.
[577] Pour plus d'informations, voir § 261 de cette thèse.
[578] Article 226-3-1 al. 6 du Code pénal français.

une circonstance aggravante lorsque les images ont été « fixées, enregistrées ou transmises »[579] ou lorsque les faits sont commis dans un « véhicule affecté au transport collectif de voyageurs », ce qui montre la dimension publique de l'infraction. Cette infraction est punie d'un an d'emprisonnement et de 15 000 euros d'amende et les peines sont doublées lorsqu'il y a des circonstances aggravantes[580]. Le droit français présente également une autre disposition assez similaire dans le Code pénal notamment l'article 226-1 qui concerne non pas le seul fait d'« apercevoir » mais le fait de fixer, enregistrer et transmettre l'image d'une personne se trouvant dans un lieu privé en portant atteinte ainsi à l'intimité de sa vie privée. Le premier article analysé se concentrait sur les parties intimes de la personne alors que dans cet article il s'agit d'une atteinte plus large.

244. Le droit belge, punit quiconque « aura observé ou fait observer une personne ou en aura réalisé ou fait réaliser un enregistrement visuel ou audio, directement ou par un moyen technique ou autre, sans l'autorisation de cette personne ou à son insu, alors que celle-ci était dénudée ou se livrait à une activité sexuelle explicite, et alors qu'elle se trouvait dans des circonstances où elle pouvait raisonnablement considérer qu'il ne serait pas porté atteinte à sa vie privée »[581]. Cet article semble faire référence, plus que celui du Code pénal français, à la sphère intime.

245. Le législateur belge à travers la consécration du délit de voyeurisme a voulu mettre l'accent sur l'atteinte à la vie privée et particulièrement à l'intimité, plutôt que considérer le voyeurisme comme une agression sexuelle[582]. Au niveau des sanctions, le législateur fixe uniquement une peine d'emprisonnement allant de six mois à cinq ans. Cette peine est aggravée avec une réclusion de dix à quinze ans si les faits sont commis sur un mineur de moins de seize ans.

---

[579] Article 226-3-1 al. 6 du Code pénal français.
[580] Outre à la fixation, enregistrement et transmission des images et à l'atteinte dans un véhicule affecté au transport collectif de voyageurs, il y a circonstance aggravante lorsque l'atteinte est commise par une personne qui abuse de l'autorité que lui confèrent ses fonctions, lorsque c'est commis sur un mineur ou sur une personne vulnérable. Ainsi que lorsque l'infraction est commise par plusieurs personnes agissant en qualité d'auteur ou de complice.
[581] Article 371/1 du Code pénal belge.
[582] Voir : M. TöLLER, « Revenge porn ou vengeance pornographique », *RDTI*, 2018/71, pp. 87-105 et N. BASECQZ, *La protection pénale des personnes vulnérables dans l'environnement numérique*, 2018 in H. JACQUEMIN et M. NIHOUL (eds), *Vulnérabilités et droits dans l'environnement numérique*, Collection de la Faculté de droit de l'UNamur, Larcier, Bruxelles, p. 133 – 177.

246. Ces deux définitions, celle retenue par le droit français et celle par le droit belge, montrent qu'il n'y a pas une unanimité quant à la définition de cette infraction. En effet, d'un côté, elle peut avoir une dimension publique, où une personne est observée et son image est capturée par un inconnu dans la sphère publique. De l'autre côté, une sphère plus intime dans laquelle la personne est reprise par une personne qu'elle connaît et dans des moments d'intimité.

247. Au Royaume-Uni[583], le voyeurisme (appelé « upskirting ») est défini et sanctionné par le Sexual Offences Act adopté en 2003 à la section 67/A qui a été ajoutée en 2019 grâce au Voyeurism (Offences) (No. 2) Bill. La section 67/A (1) érige en infraction le fait d'utiliser un équipement sous les vêtements d'une autre personne dans le but de lui permettre ou de permettre à un tiers d'observer les parties intimes de la personne (qu'elles soient exposées ou recouvertes de sous-vêtements). Cela sans son contentement ou sans croire raisonnablement que la personne y consent[584]. De plus, la section 67/A (2) complète l'infraction en ajoutant que l'infraction de voyeurisme est commise lorsque la personne enregistre une image sous les vêtements d'une autre personne représentant ses parties intimes (qu'elles soient exposées ou recouvertes de sous-vêtements). Comme pour la section précédente, ces actes sont illicites car exercés sans le consentement de la personne ou sans croire raisonnablement que la personne y consent[585]. Selon la loi, ces actions, celle d'observer et celle d'enregistrer, doivent être commises dans le but d'obtenir une gratification sexuelle ou d'humilier la victime[586]. On considère que l'application de ces limites est regrettable car les agresseurs ne cherchent pas toujours la gratification sexuelle ou l'humiliation. Enfin, la loi prévoit une peine pouvant aller jusqu'à deux ans d'emprisonnement.

---

[583] Même si le Royaume-Uni ne fait désormais plus partie de l'Union européenne, il est intéressant d'analyser sa législation qui est le fruit des travaux menés suite à un fait d'actualité. Gina Martins, jeune fille victime de voyeurisme digital, a en effet lancé une pétition pour faire adopter une loi contre le voyeurisme et sa demande a été entendue par des parlementaires britanniques qui ont présenté le Voyeurism (Offences) Act 2019 qui est entré en vigueur le 12 avril 2019.
[584] Section 67/A (1) Sexual Offences Act.
[585] *Ibid.* section 67/A (2).
[586] *Ibid*. section 67/A (3). Le texte expose précisément « obtaining sexual gratification » « humiliating, alarming or ditressing ».

248. En Allemagne cette infraction est réprimée depuis 2020[587], cependant, cela n'est pas le cas en Italie ou en Espagne, où ce type de comportement illicite est réprimé à travers les dispositions d'atteinte à la vie privée.

c) L'encadrement du cyberharcèlement ou mieux « des cyberharcèlements »

249. Il est intéressant de commencer cette analyse par les dispositions adoptées par l'État italien. En effet, il existe plusieurs dispositions législatives qui concernent des actes de harcèlement, entendu comme un comportement indésirable répété qui a « pour objet ou pour effet de porter atteinte à la dignité d'une personne et de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant »[588].

250. En Italie, la loi 71/2017[589], entrée en vigueur le 18 juin 2017, prévoit des dispositions pour prévenir et sanctionner le « cyberbullismo »[590] c'est-à-dire le cyberharcèlement entre mineurs[591]. En effet, la loi italienne définit le « cyberbullismo » comme « toute forme de pression, d'agression, de harcèlement, de chantage, d'insulte, de dénigrement, de diffamation, d'usurpation d'identité, d'altération, d'acquisition illicite, de manipulation, de traitement illicite de données à caractère personnel au détriment des mineurs, effectuée par voie électronique, ainsi que la diffusion de contenus en ligne concernant également un ou plusieurs membres de la famille du mineur, dont le but intentionnel et prédominant est d'isoler un mineur ou un groupe de mineurs au moyen d'un abus grave, d'une attaque nuisible ou d'un acte de dérision »[592].

---

[587] Voir amendement du 14 octobre 2020 entrée en vigueur le 1er janvier 2021. Disponible en allemande ici : https://perma.cc/9RTY-ZMJK

[588] Art. 2 §3, directive 2000/43/CE du Conseil, du 29 juin 2000, relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique.

[589] Legge n° 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, del 29 maggio 2017(17G00085), GU Serie Generale n.127 del 03-06-2017.

[590] Ce terme est très présent dans la doctrine anglo-saxonne avec le terme de « cyberbullying ».

[591] Pour aller plus loin sur le cyberharcèlement entre mineurs, voir F. Gottschalk, Cyberbullying: an overview of research and policy in OECD contries, OECD Education Working Papers N° 270, EDU/WKP(2022)8, 24 March 2022, pp. 32-41.

[592] Voir article 1 (2) de la loi n° 71 précitée. Texte original en italien, traduction de l'autrice : « per «cyberbullismo» si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identita', alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonche' la diffusione di contenuti on line aventi ad oggetto anche uno o piu' componenti della famiglia del minore il cui scopo

251. Ainsi, outre à la protection des mineurs, le législateur a également complété l'article 612 bis du Code pénal italien sur le stalking avec la dimension « cyber ». Le stalking est une forme de harcèlement et le Code pénal prévoit une peine d'emprisonnement allant de six mois à cinq ans pour quiconque menace ou importune, de façon répétée, une personne de manière à lui provoquer un état d'anxiété ou de peur grave et persistant qui peut susciter une crainte fondée pour sa propre sécurité ou celle d'un proche qui l'oblige à modifier son mode de vie[593]. Après la définition, l'article 612 bis spécifie que ces comportements sont réprimés plus sévèrement lorsqu'ils sont commis par des (ex) conjoints ou partenaires intimes par voie informatique ou télématique. L'ajout des moyens informatiques a été fait *a posteriori* à travers la loi n° 119, du 15 octobre 2013. Toutefois, cette circonstance aggravante semble se limiter à la sphère familiale de la victime, ce qui exclurait le cyberstalking par des inconnus. Selon la jurisprudence italienne, en particulier la décision de la Cour de cassation du 28 décembre 2017 n° 57764, l'attitude néfaste du cyberstalking n'est pas tant celle qui consiste à forcer la victime à être offensée ou menacée par voie électronique, que celle qui consiste à diffuser aux utilisateurs du réseau des données vraies ou fausses, hautement préjudiciables et source d'inquiétude pour la partie offensée.

252. En France, le législateur définit le harcèlement moral comme « 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 »[594]. Ainsi, il définit le harcèlement sexuel, d'une part comme « 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 raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante,

intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo ».

[593] Article 612 bis du Code pénal italien. Traduction de l'autrice, texte original : « […] chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita ».

[594] Article 222-3-2-2 du Code pénal français.

hostile ou offensante »[595] . D'autre part, comme « le fait, même non répété, d'user de toute forme de pression grave dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers »[596]. Il n'existe pas de disposition spécifique de cyberharcèlement mais, pour encadrer les comportements qui peuvent caractériser le harcèlement en ligne, le législateur a ajouté à ces infractions « traditionnelles » une circonstance aggravante lorsque les faits de harcèlement sont commis par « l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique »[597]. La peine maximale encourue pour des actes de harcèlement moral en ligne est de deux ans d'emprisonnement et 30 000 euros d'amende et lorsqu'il s'agit de harcèlement sexuel de trois ans d'emprisonnement et 45 000 euros d'amende.

Aux termes de la loi du 7 juillet 2023 le législateur a prévu une obligation pour les plateformes de réseaux sociaux de rendre visibles à leurs utilisateurs des messages de prévention contre le harcèlement et d'indiquer aux personnes autrices de signalements les structures d'accompagnement[598].

253. Le législateur français a également prévu des sanctions pour le cyberharcèlement en meute ou « raid numérique ». Ce dernier, grâce à l'adoption de la loi du 3 aout 2018[599], est défini et sanctionné par l'article 222-3-2-2 du Code pénal qui prévoit que :

> « L'infraction [de harcèlement] est également constituée :
>
> a) Lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée ;
>
> b) Lorsque ces propos ou comportements sont imposés à une même victime, successivement,

[595] Article 222-3 (III) du Code pénal français.
[596] Article 222-3 (III) du Code pénal français.
[597] Article 222-3-2-2 al 4 du Code pénal français et article 222-3 (III) al. 6 du Code pénal français.
[598] Article 3 de la loi n°2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, publiée au Journal Officiel du 8 juillet 2023.
[599] Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes.

par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition »[600].

La particularité de cette disposition est qu'une personne peut être condamnée pour la publication d'un seul message si celui-ci s'inscrit dans une « meute », c'est-à-dire un ensemble de messages et publications haineuses, même en l'absence de concertation avec les autres auteurs. En France, plusieurs exemples de raid numériques peuvent être cités comme ceux organisés par la « Ligue du LOL » contre des journalistes[601], ceux perpétrés contre des militantes féministes comme Alice Coffin[602] ou encore celui de la jeune Mila[603].

254. En Autriche, l'article 107 (c) du Code pénal[604] prévoit une infraction autonome de harcèlement persistant impliquant les télécommunications ou les systèmes de communication. Cet article punit le fait de diffamer une personne et de publier des faits ou des images personnelles d'une manière qui peut être perçue par un large nombre de personnes. Cette disposition inclue également une sanction plus lourde lorsque les faits précédemment cités amènent au suicide ou à la tentative de suicide de la personne harcelée. Comparés aux articles du Code pénal français, ces derniers recouvrent des faits et propos bien plus larges.

255. En droit belge, il n'existe pas d'infraction spécifique de cyberharcèlement. Toutefois deux dispositions de la loi peuvent être utilisés : l'article 442 du Code pénal et l'article 145 §3 bis, de la loi du 13 juin 2005, relative aux communications électroniques. D'une part, l'article 442 du Code pénal sanctionne le harcèlement et punit d'une peine d'emprisonnement de quinze jours à deux ans et/ou d'une amende de cinquante euros à

[600] Article 222-3-2-2 du Code pénal français.
[601] Un groupe de journalistes français que, à travers un groupe Facebook, organisaient de raid numérique sur Twitter à l'encontre de collègues journalistes femmes ou hommes homosexuels.
[602] Alice Coffin, militante féministe a été et continue d'être l'objet de raid numériques sur Twitter pour ses positions radicales sur le féminisme. La haine des internautes l'a plus d'une fois obligée à quitter les réseaux sociaux au vu de l'ampleur que ces actes de cyberharcèlement prenaient.
[603] Voir § 119 de cette thèse.
[604] Voir Bundesrecht konsolidiert, Strafgesetzbuch § 107c, disponible sur : https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296&Paragraf=107c

trois cents euros « quiconque aura harcelé une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée »[605]. Cet article ne contient pas, comme les articles 222-3 et 222-3-2-2 du Code pénal français, une circonstance aggravante concernant l'utilisation d'un support numérique pour causer des actes de harcèlement. Toutefois il est utilisé par les juges pour condamner des comportements de harcèlement en ligne[606]. Il convient de soulever une exception à la répétition des faits qui caractérise le harcèlement, en effet par un arrêt de la Cour de cassation du 29 octobre 2013, « un acte unique pouvait être considéré comme harcèlement au motif que les effets se répètent dans le temps »[607]. En l'espèce il s'agissait de la publication d'une vidéo sur YouTube qui, comme le précise Ch.-E Clesse est par nature « répétitive, car consultable de manière illimitée »[608]. D'autre part, l'article 145 §3 bis de la loi du 13 juin 2005 prévoit qu' « est punie d'une amende de 50 euros à 300 euros et [ou] d'un emprisonnement de quinze jours à deux ans […] la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci »[609]. Cette infraction est souvent désignée de façon inappropriée sous le terme de « harcèlement téléphonique »[610]. Les mots « harcèlement » et « téléphonique » ne sont toutefois pas appropriés. En effet, pour rentrer dans le domaine de l'article 145 la répétition n'est pas nécessaire[611], au contraire de l'article 442 bis. Ainsi, ces infractions ne se limitent pas au téléphone mais peuvent viser n'importe quel moyen de communication électronique.

256. Après avoir analysé comment certains comportements illicites sont appréhendés par les droits nationaux, il est intéressant de surligner que cette multiplicité des mesures entraîne une différence de traitement entre les ressortissants des États membres, en

---

[605] Article 442 bis du Code pénal belge.
[606] Voir notamment Corr. Leuven, 8 novembre 2010, *A.M.*, 2011.
[607] F. ERNOTTE, *Droits des réseaux sociaux*, 1re édition, Larcier, 2021, p. 199.
[608] *Ibid.* p. 199.
[609] Article 145 § 3bis, de la loi du 13 juin 2005 relative aux communications électroniques.
[610] Voir par exemple N. BANNEUX et L. KERZMANN, « Le mal nommé « harcèlement téléphonique » : chronique des tribulations législatives d'une infraction moderne », *RDTI*, 2009/1, n° 34, p. 29-45.
[611] Voir notamment CA, 71/2006 cité par N. BANNEUX et L. KERZMANN, « Le mal nommé « harcèlement téléphonique »: chronique des tribulations législatives d'une infraction moderne », *RDTI*, 2009/1, n° 34, p. 36.

particulier au sein de l'Union européenne, et cela amène à plusieurs conséquences négatives.

B. Les conséquences du pluralisme, vecteur de fragilisation de la protection des droits fondamentaux

257. On constate que la multiplication de définitions et, par conséquent, d'encadrements amène à plusieurs conséquences négatives pour la protection des droits fondamentaux des utilisateurs. En particulier, on souligne une absence de données fiables sur les cyberviolences (**1**) et un risque étendu pour la protection des droits fondamentaux dans certains États de l'Union européenne (**2**).

1. L'absence de données fiables sur les cyberviolences

258. La multiplicité des définitions utilisées et l'absence de définitions dans certains États ont pour conséquence un manque de données fiables récoltées dans ce domaine. Aujourd'hui si des données nationales sont disponibles, il n'est pas facile de les interpréter et les comparer. Un rapport commandé par la « Commission des droits de la femme et de l'égalité des genres » (FEMM) du Parlement européen sur les cyberviolences et le discours de haine en ligne à l'encontre des femmes[612] a constaté l'absence de données sur le phénomène des violences en ligne, en particulier dans une perspective de genre. Ce dernier a également souligné la difficulté de récolter et comparer les données. En effet, plusieurs obstacles ont été enregistrés, notamment ceux de savoir s'il s'agit d'un crime ou d'un délit ainsi que la catégorisation des infractions qui permet rarement de retracer les différentes formes de cyberviolence, à cause de la différence des définitions d'un État à l'autre. Sans compter la sensibilisation et la formation des victimes et du personnel de police et justice qui ne permet pas de placer les États sur le même niveau de protection des individus, car dans certains cas les violences en ligne sont encore très peu comprises et dénoncées.

[612] A. VAN DER WILK, *Cyber violence and hate speech online against women*, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament September 2018.

259. Le même rapport recommande aux États membres de faire des efforts sur la collecte des données et la production des statistiques accessibles, transparentes et claires. Il ajoute également une liste de caractéristiques qui devraient être prises en compte dans la collecte et notamment : « le profil des auteurs, leur relation avec la victime, les moyens de perpétration, le nombre de cas signalés, le nombre de cas poursuivis et le nombre de condamnations, ventilés selon le sexe/le genre identifié et l'âge de la victime »[613]. De plus, une résolution du Parlement européen contenant des recommandations à la Commission européenne sur la lutte contre les cyberviolences fondées sur le genre a été adoptée le 14 décembre 2021[614]. Elle avait été proposée par la « Commission des droits de la femme et de l'égalité des genres » et la « Commission des libertés civiles, de la justice et des affaires intérieures » avec l'objectif de fixer des règles minimales relatives à la définition de l'infraction de cyberviolence à caractère sexiste et des sanctions. Et, de « créer un système fiable pour la collecte régulière de données statistiques ventilées et comparables sur la violence à caractère sexiste, y compris la cyberviolence »[615]. Enfin, le Groupe d'experts du Conseil de l'Europe sur la lutte contre la violence à l'égard des femmes et la violence domestique[616] a également exprimé ce souhait dans sa première recommandation sur la dimension numérique des violences à l'égard des femmes en recommandant aux États de mettre en place un système de collecte et d'analyse systématique des données sur la violence à l'encontre des femmes ayant une composante numérique[617].

---

[613] *Ibid.* p. 64.
[614] Résolution du Parlement européen du 14 décembre 2021 contenant des recommandations à la Commission sur la lutte contre la violence fondée sur le genre : cyberviolence, 2020/2035(INL).
[615] *Ibid.* point 27.
[616] Groupes d'experts indépendants qui contrôlent la mise en œuvre par les États membres de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique.
[617] GREVIO, *Recommandation générale n° 1 sur la dimension numérique des violences à l'encontre des femmes*, 20 octobre 2021. Disponible sur : https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

2. Un risque étendu pour la protection des droits fondamentaux des utilisateurs

260. Certains États ont adopté des dispositions et encadrés certains comportements illicites, d'autres, ne disposent simplement pas de dispositions juridiques pour encadrer et sanctionner certaines violences en ligne. L'affaire *KU c. Finlande*[618], entre autres[619], avait montré le risque d'atteinte aux droits fondamentaux lorsqu'un État ne prévoit pas des dispositions adéquates contre les violences en ligne. L'espèce, qui date de 1999, concernait la mise en ligne par un inconnu d'une annonce à caractère sexuel indiquant que la victime âgée de 12 ans recherchait une relation intime. Cette annonce précisait le nom, l'âge et les caractéristiques du mineur et renvoyait également à une page web avec la photo et son numéro de téléphone. Or, le fournisseur d'accès avait refusé de transmettre l'identité de la personne ayant publié l'annonce et le tribunal saisi avait rejeté la demande introduite par la police afin d'obliger le fournisseur d'accès à divulguer l'identité de ce dernier. La Cour européenne des droits de l'Homme a alors conclu à la violation de l'article 8 de la Convention européenne des droits de l'Homme sur le droit au respect de la vie privée car l'État finlandais n'avait pas protégé le droit d'un enfant à la protection de sa vie privée. Selon la Cour le législateur aurait dû prévoit un cadre permettant de concilier la confidentialité des services Internet, la prévention des infractions pénales et la protection des droits et libertés d'autrui. Ce cadre a ensuite été prévu par la loi finlandaise sur l'exercice de la liberté d'expression dans les médias, qui n'était pas encore en vigueur au moment des faits[620].

261. Concernant les infractions en ligne et l'absence de mesures prises par les États, on peut prendre l'exemple de la diffusion non consensuelle de contenus à caractère sexuel. Comme mentionné précédemment des États comme l'Italie et la France ont inscrit cette infraction dans leur Code pénal. Aux États-Unis il y a plus de trente États qui ont adopté des dispositions pour sanctionner cette infraction[621]. Toutefois, d'autres États, y compris

---

[618] Cour EDH, 2 décembre 2008, *K.U c. Finlande*, req. n° 2872/02.
[619] Voir par exemple Cour EDH, GC, 12 novembre 2012, *Söderman c. Suède*, req n° 5786/08.
[620] Cour EDH, 2 décembre 2008, *K.U c. Finlande*, req. n° 2872/02 §49.
[621] Voir le tableau du Cyberbullying research center dans la catégorie « Revenge porn law », disponible ici : https://cyberbullying.org/sexting-laws

des membres de l'Union européenne, ne l'ont pas encore fait. C'est le cas notamment de la Roumanie et de la Hongrie. En Roumanie, un projet de loi avait été adopté en 2019 à l'unanimité par le sénat roumain pour créer une infraction autonome de « revenge porn ». Cependant, la loi n'a toujours pas été adoptée. Cette infraction est actuellement sanctionnée dans le cadre des violences conjugales, mais elle ne l'est pas lorsque la personne qui partage les photos ne fait pas partie du cercle familial. Pour cela, les victimes de ces actes ne disposent pas d'une protection *ad hoc*. En Hongrie par exemple, elles peuvent seulement recourir à d'autres dispositions du Code pénal comme le harcèlement ou la diffamation. Il est évident que le traitement réservé aux ressortissants de ces deux États n'est pas le même que celui des ressortissants d'autres États qui prévoient des dispositions spécifiques[622]. En effet, les dispositions juridiques dont les victimes peuvent se prévaloir ne permettent pas de prendre en compte tous les aspects de cette infraction à caractère sexuel. Par exemple, lorsque la victime se prévaut d'une disposition sur la diffamation, cette dernière ne permet pas de prendre en compte les atteintes à l'intimité et à la vie privée. Mais encore, si le droit national permet aux victimes de « revenge porn » de se prévaloir des dispositions relatives à l'atteinte à la vie privée, cette dernière doit être perçue comme une atteinte plus générale à l'intégrité de la personne. En effet, comme l'explique Alisdair Gillespie « it has been postulated that in western society one of the fundamental aspect of privacy is the right to control the exposure of one's body. […] The person is not putting a photograph of the other on the website, they are putting a photograph or movie on the website that accentuates the sexual identity of the victim. They are therefore stripping away the right of the victim to control her body and indeed control her sexuality and instead it is placed on the Internet for all to see. This is the degrading of an individual and must be considered to be not merely the imposition of distress but of harm. It is a harm against the integrity of the individual »[623].

---

[622] Par exemple en Italie, France, Allemagne ou République Tchèque où des dispositions *ad hoc* ont été adoptées.

[623] GILLESPIE, 2016, p. 221 cité par G. M CALETTI, « « Revenge porn » e tutela penale, Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane », *Diritto penale contemporaneo*, Rivista trimestrale, 3/2018, p. 82. Traduction par l'autrice : « il a été postulé que dans la société occidentale, l'un des aspects fondamentaux de la vie privée est le droit de contrôler l'exposition de son corps. (...) La personne ne met pas une photo de l'autre sur le site web, elles y mettent une photo ou un film qui accentue l'identité sexuelle de la victime. Elles retirent donc à la victime le droit de contrôler son corps et sa sexualité et, au lieu de cela, ils le placent sur Internet à la vue de tous. Il s'agit

262. Une autre infraction comme celle du viol à distance, qui a été examinée dans le chapitre précèdent, peut faire l'objet de traitements différents par les législations nationales avec des conséquences sur les sanctions et la réparation des victimes. En France, par exemple, cette infraction avait pu être sanctionnée comme une complicité d'agression sexuelle alors que dans d'autres États comme la Belgique ou la Suède les juridictions avaient reconnu le viol malgré l'absence de contact physique[624]. Or, il faudrait un cadre harmonieux pour permettre de reconnaître au même titre ce type d'infractions.

263. Les conséquences du pluralisme des droits nationaux peuvent représenter un risque pour la protection des droits fondamentaux et garantir à certains citoyens européens une protection étendue et à d'autres une protection plus restreinte. Cela expose les États membres de l'Union européenne à des manquements à leurs obligations positives de protéger les individus des atteintes aux droits fondamentaux.

Section II : La solution aux risques du pluralisme : l'harmonisation des droits nationaux en matière de cyberviolence

264. Le constat que nous avons relevé nous amène à rechercher une solution pour parvenir à une protection étendue des droits fondamentaux sur Internet. On propose alors d'harmoniser les dispositions juridiques sur les violences en ligne à travers l'adoption d'une définition universelle des cyberviolences ainsi que l'adoption des règles minimales pour encadrer les infractions qui prolifèrent aujourd'hui et prolifèreront dans le futur dans le cyberespace. En effet, cela pourrait éviter la multiplication de dispositions juridiques distinctes au niveau national, régional et international. Ainsi, et surtout, entraver les conséquences négatives du pluralisme qui affaiblit la protection des droits fondamentaux pour les utilisateurs d'Internet.

---

de l'avilissement d'un individu et il faut considérer qu'il ne s'agit pas seulement de l'imposition d'une détresse mais d'un préjudice. Il s'agit d'une atteinte à l'intégrité de l'individu ».

[624] Voir §175 de cette thèse.

S'il est vrai que l'adoption du « Digital Services Act »[625] en 2022 a fait avancer la régulation des plateformes pour améliorer la réponse à la diffusion des contenus illicites, il n'apporte pas de réponses sur les définitions et les différentes formes de comportements illicites sur Internet.

265. Il s'agit ainsi, après avoir analysé les définitions existantes en matière de cyberviolences et les conséquences du pluralisme juridique, de proposer une définition universelle qui soit reconnue au niveau régional, voir international pour encadrer de manière plus uniforme les atteintes aux droits fondamentaux (**§I**). Cette définition devra ensuite être accompagnée par l'adoption des règles minimales (**§II**).

I. Une définition universelle encadrant les atteintes aux droits fondamentaux

266. Cette définition se veut générale et respectueuse des particularités juridiques des États membres de l'Union européenne, du Conseil de l'Europe ainsi que des États membres des Nations unies. Comme dirait Marie-Laure Izorche « il faut de la logique pour la cohérence, mais du flou pour la cohésion, la souplesse, le respect de la diversité »[626]. Cette définition, n'a pas vocation à restreindre l'encadrement à un certain nombre de violences, au contraire, elle doit laisser la porte ouverte aux évolutions technologiques et à l'essor d'autres comportements illicites qui pourraient surgir après son adoption. Il est clair désormais que le droit est en constant retard par rapport aux infractions en ligne et qu'une définition plus large permettrait de pouvoir encadrer les futures infractions.

[625] Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[626] M-L IZORCHE, « La marge nationale d'appréciation, enjeu de savoir et de pouvoir, ou jeu de construction ? », *Revue de science criminelle et de droit pénal comparé*, nº 1, 2006, p. 25.

267. Cette définition est la suivante :

I. Constituent des cyberviolences l'utilisation intentionnelle des systèmes informatiques pour causer, faciliter ou menacer de causer à une personne ou à un groupe des personnes une atteinte à un droit ou plusieurs droits et/ou à sa dignité.

Les cyberviolences seront constituées lorsque l'atteinte :

1° Entraine ou est susceptible d'entrainer un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques, ou

2° Crée une situation dégradante au sein ou en dehors des systèmes informatiques.

II. Ces atteintes peuvent comprendre l'exploitation de la situation, des caractéristiques ou de la vulnérabilité de la personne ou du groupe des personnes.

III. Ces atteintes peuvent être imposées à une même victime par un ou plusieurs individus de manière concertée ou à l'instigation de l'une d'elles.

268. Il faut surligner que certaines caractéristiques de la définition du Comité de la Convention sur la cybercriminalité ont été reprises car elles recouvrent justement et suffisamment un large éventail de comportements illicites en ligne. Toutefois, certains ajouts ont été nécessaires pour parvenir à une définition exhaustive mais, en même temps, assez large pour ne pas la rendre obsolète avec les évolutions de la technologie. Il sera utile de motiver cette proposition à travers une analyse des termes choisis.

269. *I. Constituent des cyberviolences l'utilisation intentionnelle des systèmes informatiques pour causer, faciliter ou menacer de causer à une personne ou à un groupe des personnes une atteinte à un droit ou plusieurs droits et/ou à sa dignité.*

Ce premier paragraphe permet d'appréhender l'utilisation des systèmes d'informations.

D'abord, l'expression « systèmes informatiques » désigne, conformément à la Convention du Conseil de l'Europe sur la cybercriminalité, « tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données »[627]. On y associe également les médias et réseaux sociaux.

Ensuite, par « utilisation intentionnelle » on prend en compte l'intentionnalité qui est laissé à l'interprétation des autorités nationales. Cela est conforme à la Convention sur la cybercriminalité du Conseil de l'Europe[628].

De plus, ce paragraphe permet, non seulement, de sanctionner des atteintes aux droits fondamentaux des individus, mais également, le fait de les « faciliter ». En effet, comme il a été souligné dans les chapitres précédents, Internet facilite plusieurs infractions et les amplifie.

Ainsi, il est également important de sanctionner le fait de « menacer de causer » comme cela est déjà le cas dans certains droits nationaux pour des infractions sur Internet comme le partage de contenus à caractère sexuel sans le consentement de la personne ou le fait de menacer de diffuser des informations personnelles ou de commettre un crime (homicide, viol)[629]. Cette menace pourrait, en effet, même si elle n'est pas suivi d'acte, causer à la victime une détresse psychologique.

Cette disposition prend en compte le fait de causer, faciliter ou menacer un dommage à un individu mais aussi à un groupe d'individus. En effet, il est nécessaire de montrer également cette particularité d'Internet qui permet de porter atteinte aux droits de plusieurs personnes à la fois. Il peut s'agir de personnes qui n'ont pas de liens entre eux ou bien qui ont comme point commun le fait d'appartenir à une religion, au même genre (par exemple les femmes ou les personnes transgenre) ou encore de croire à la même religion.

---

[627] Article 1 Convention du Conseil de l'Europe sur la cybercriminalité.
[628] Voir Conseil de l'Europe, *Rapport explicative de la Convention sur la cybercriminalité,* 23 novembre 2001, point 39.
[629] Pour la menace de commettre un crime voir l'article 222-17 du Code pénal français, pour le chantage voir l'article 312-10 du Code pénal français.

Enfin, les atteintes prises en compte dans cette définition concernent les droits fondamentaux, une violence en ligne est toute infraction qui porte atteinte aux droits humains fondamentaux des individus y compris leur dignité en tant qu'êtres humains et qui cause un préjudice et/ou une souffrance.

270. La suite de la définition, prévoit deux éléments alternatifs. En effet il est prévu que :

Les cyberviolences seront constituées lorsque l'atteinte :

> *1° Entraine ou est susceptible d'entrainer un préjudice ou des souffrances physiques, sexuelles, psychologiques, économiques ou administratives ;*

Ce paragraphe permet d'appréhender la multiplicité des formes et natures des cyberviolences. Cette multiplicité avait été prise en compte dans la définition du Comité de la Convention sur la cybercriminalité qui s'était inspiré de la définition de la violence à l'encontre des femmes et des filles, retenue dans la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique et dans la Convention interaméricaine sur la prévention, la sanction et l'élimination de la violence contre les femmes. En effet, ces dernières considèrent que les violences de genre se matérialisent sous différentes formes : physiques, sexuelles, psychologiques et économiques.

Ce choix terminologique dénote l'urgence de reconnaître toutes les formes de comportements illicites sur Internet qui peuvent être de nature sexuelle comme le partage de contenus à caractère sexuel sans le consentement de la personne ; ou encore psychologique lorsque la personne est victime de cyberharcèlement ou de l'installation des logiciels espions. De plus, cette violence peut être économique voir administrative lorsque les nouvelles technologies sont utilisées pour détourner des aides financières perçues par la victime à travers l'usurpation d'identité ou par le vol d'informations personnelles. Enfin physiques, notamment à travers les viols à distance ou le « happy slapping », actes de violences perpétrés sur des personnes, enregistrées et diffusées en direct.

271. *2° Crée une situation dégradante au sein ou en dehors des systèmes informatiques.*

Ce paragraphe concerne en particulier les violences telles que le cyberharcèlement que, comme pour les faits de harcèlement hors ligne, créent une situation qui dégrade les conditions de vie de la victime. Sur Internet, cela peut se matérialiser par des atteintes aux droits des victimes tels que la liberté d'expression ou l'atteinte à la vie privée. Cependant, ces violences peuvent également avoir des conséquences en dehors des systèmes d'information sous la forme des violences physiques ou verbales dans l'espace public. Cela a été le cas dans des affaires de cyberharcèlement scolaire ou entre mineurs[630].

272. *II. Ces atteintes peuvent comprendre l'exploitation de la situation, des caractéristiques ou de la vulnérabilité de la personne ou du groupe des personnes.*

Ce paragraphe permet, à travers des termes généraux, de prendre en compte la situation ainsi que les caractéristiques d'une ou plusieurs victimes. L'article 3 (9), de la directive 2008/115/CE du Parlement européen et du Conseil, du 16 décembre 2008, relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier définit ainsi les « personnes vulnérables » : « les mineurs, les mineurs non accompagnés, les personnes handicapées, les personnes âgées, les femmes enceintes, les parents isolés accompagnés d'enfants mineurs et les personnes qui ont été victimes de torture, de viol ou d'une autre forme grave de violence psychologique, physique ou sexuelle »[631]. La Cour européenne des droits de l'Homme donne également des indications sur les sujets vulnérables. Elle cite notamment les femmes[632], les enfants[633], les personnes âgées dépendantes et les personnes transgenre[634]. Elle ajoute

[630] Plusieurs évènements tragiques ont eu lieu en France par exemple où des cas de cyberharcèlement ou de partage non consensuel de contenus sexuels ont causés des homicides (voir par exemple : LCI, *Mort d'Alisha à Argenteuil : le récit glaçant d'un macabre engrenage*, 11 mars 2021) ou des suicides (voir notamment LCI, *Décès de la youtubeuse Mava Chou : une plainte pour provocation au suicide déposée le jour de sa mort*, 26 décembre 2021).
[631] Directive 2008/115/CE du Parlement européen et du Conseil, du 16 décembre 2008, relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier.
[632] Cour EDH, 24 juillet 2012, *B.S c. Espagne*, req n° 47159/08.
[633] Cour EDH, 22 octobre 1996, *Stubbing et autres c. Royaume-Uni*, req. n° 22083/93 et 22095/93.
[634] Cour EDH, 11 juillet 2002, *Goodwin c. Royaume-Uni*, req. n° 28957/95.

également les « groupes vulnérables » comme les Roms, les demandeurs d'asile, les personnes en situation de handicap mental et les personnes porteuses du VIH[635]. Or, il serait possible de transposer ces catégories aux atteintes sur Internet notamment les femmes, les enfants mais également certains groupes de personnes en raison de leur orientation sexuelle, ethnie, religion comme il l'a été souligné par le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Les conséquences d'une telle vulnérabilité et de l'absence de protection de certaines catégories de personne a pu amener à des violences à grande échelle comme celles perpétrées à l'encontre des Rohingyas[636].

La vulnérabilité existe également vis-à-vis des mineurs notamment à cause de leur jeune âge mais également de leur situation socio-économique. Les femmes et les filles sont les plus exposées à la pauvreté, 330 millions de femmes et de filles vivant avec moins de 1,90 dollar par jour, soit 4,4 millions de plus que les hommes[637]. 15 millions de filles ne pourront pas aller à école et apprendre à lire et à écrire[638], ce qui augmente la vulnérabilité des filles et leur exposition à la traite des êtres humains et à l'exploitation sexuelle en ligne et hors ligne. Les garçons sont également victimes d'exploitation sexuelle en ligne. En effet, dans une étude menée par ECPAT et INTERPOL sur des images d'exploitation sexuelle d'enfants sur Internet, il s'est avéré que 64,8 % des victimes étaient des filles et 31,1% étaient des garçons et 4,1% montrait des garçons et des filles ensemble[639]. En outre, une étude de ECPAT sur l'exploitation sexuelle des garçons en Thaïlande a identifié l'extrême pauvreté comme le facteur plus important de vulnérabilité[640].

---

[635] Pour approfondir voir L. BURGORGUE LARSEN, *La vulnérabilité saisie par les juges en Europe*, Cahiers européens, Pedone, 2014, voir en particulier le chapitre de S. BESSON.

[636] Les Rohingyas, groupe ethnique indo-aryen apatride qui réside principalement à l'ouest de la Birmanie et qui subit régulièrement des persécutions. Facebook a reconnu que son réseau avait été utilisé pour attiser la violence en Birmanie et avait permis « à des groupes organisés de mettre en œuvre des attentats sectaires contre les Rohingyas, minorité musulmane du pays ». Voir Courrier international, *Génocide des Rohingyas : le mea culpa de Facebook*, 7 novembre 2018. Disponible sur : https://www.courrierinternational.com/dessin/genocide-des-rohingyas-le-mea-culpa-de-facebook

[637] UN Women, T*urning Promises Into Action: Gender Equality in the 2030 Agenda for Sustainable Developmen*t. Global Factsheet, 2018, p. 2. Disponible sur : https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2018/SDG-report-Fact-sheet-Global-fr.pdf

[638] *Ibid*. p. 2.

[639] ECPAT et INTERPOL, *Towards a global indicator on unidentified victims in child sexual exploitation material*, 2018, p. 3.

[640] ECPAT and THAILAND INSTITUTE OF JUSTICE, *Global initiative to explore the sexual exploitation of boys*, Thailand report, 2021, pp. 6,22, 23.

273. *III. Ces atteintes peuvent être imposées à une même victime par un ou plusieurs individus de manière concertée ou à l'instigation de l'une d'elles.*

Ce paragraphe inclut la possibilité de sanctionner les comportements illicites perpétrés par une ou plusieurs personnes à l'encontre d'un individu ou un groupe d'individus. Lorsqu'une même personne fait l'objet d'atteintes de la part de plusieurs personnes, elle est victime d'un « raid numérique ». L'infraction est caractérisée lorsque les comportements illicites sont menés de manière concertée, mais également lorsqu'il n'y a pas de concertation.

II. L'adoption des règles minimales sur les cyberviolences

274. La définition exposée précédemment comporterait une clarification et une identification cohérente des cyberviolences au sein des États. Elle pourrait être adoptée à travers une directive européenne ou un protocole additionnel à la Convention de Budapest sur la cybercriminalité mais également une convention internationale. Toutefois, sans approfondir ce point sur les fondements juridique de l'adoption qui sera traité dans le chapitre suivant, il convient de souligner que l'adoption d'une définition universelle, pour être efficace, devrait s'accompagner des règles minimales qui définissent et encadrent les comportements illicites sur Internet. En effet, si l'objectif de cette définition est celui d'harmoniser les droits nationaux pour rendre la prévention et la sanction des cyberviolences plus efficace, il conviendrait d'adopter des règles minimales qui énumèrent et définissent les comportements illicites en ligne. Cela, afin de garantir que chaque État prévoit *a minima* des dispositions sur les multiples formes de cyberviolences. En effet, cela permettrait de mieux appréhender ce phénomène et garantir une protection minimale aux utilisateurs en rapprochant, dans un premier temps, les droits nationaux des États membres de l'Union européenne et, ensuite, du Conseil de l'Europe et des Nations unies. Un exemple qui pourrait inspirer l'adoption de ces règles minimales est celui de la directive 2013/40/UE du Parlement européen et le Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information dans laquelle des règles minimales avaient été fixées pour rapprocher le droit pénal des États membres dans le domaine des attaques contre les systèmes d'information.

275. Pour que cette harmonisation soit possible, les États disposeraient d'une marge d'appréciation. En effet, comme expliqué par Mireille Delmas-Marty, « pour que l'harmonisation soit admise dans des pays de tradition juridique différente, il faut sans doute éviter d'imposer un modèle d'ordre trop directement inspiré par l'ordre étatique, donc admettre, de façon explicite ou implicite, une « marge nationale d'appréciation », autrement dit une certaine souplesse qui facilite les ajustements et réajustements caractérisant le processus d'harmonisation »[641]. Cette harmonisation s'inscrit dans la pensée de Delmas-Marty du « pluralisme ordonné », « « pluralisme » car les différences sont admises, « ordonné » si le droit mondial réussissait ainsi à dépasser la contradiction entre l'un et le multiple »[642]. La marge d'appréciation des États est, selon elle, « la principale clef du pluralisme ordonné. D'une part, elle exprime la dynamique centrifuge, la résistance nationale à l'intégration ; mais, d'autre part, la marge n'étant pas illimitée mais bornée par des principes communs, elle impose une limite, un seuil de compatibilité qui ramène au centre […]. Les oscillations, qui traduisent tantôt les résistances des droits internes tantôt les avancées du processus d'harmonisation, permettent, en ajustant l'ampleur de la marge acceptable, de déterminer un seuil de compatibilité »[643].

[641] M. DELMAS- MARTY, Le pluralisme ordonné, *Les forces imaginantes du droit (II)*, Seuil, 2006, pp. 77-78.
[642] *Ibid*. p. 26.
[643] *Ibid*. p. 78.

Conclusion du Chapitre III

276. Malgré l'existence de définitions et d'encadrements juridiques de certaines formes de cyberviolences dans les droits nationaux et en droit de l'Union européenne, il n'existe pas aujourd'hui une définition de cyberviolence reconnue par la communauté internationale.

Les décisions nationales ayant mené à l'adoption de dispositions pour définir et sanctionner des formes de cyberviolences ont participé à la création d'un système de régulation qui varie d'un État à l'autre. Cela mène à une protection fragile des droits fondamentaux des utilisateurs surtout dans les États qui n'ont pas prévu des mesures particulières. Après l'adoption du Digital Services Act[644] qui a pour vocation de fixer des obligations pour les plateformes vis-à-vis du partage des contenus illicites, il serait nécessaire de clarifier ce que sont les cyberviolences et sur quelles formes elles peuvent se manifester à travers la création d'une définition générale et des règles minimales.

[644] Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

Chapitre IV : L'élaboration nécessaire de règles minimales contre les cyberviolences

S'il est évident que l'autorégulation ne suffit pas, il n'en apparait pas moins que les droits nationaux eux-mêmes sont débordés. Il serait nécessaire de définir, au-delà des procédures, des véritables règles de fond communes[645].

277. Dans les développements précédents, nous avons constaté l'absence d'une définition universelle des cyberviolences et d'encadrement commun au niveau national, régional et international. Ce pluralisme juridique assure une faible protection des droits fondamentaux, en particulier aux ressortissants de certains États mais également l'impossibilité de bien mesurer ce phénomène. À plusieurs reprises nous avons souligné la nécessité d'adopter une définition universelle et des règles minimales encadrant les cyberviolences de contenu. Des dispositions et des mesures qui pourraient être prises comme exemple sont celles adoptées contre les contenus pédopornographiques dans la Convention sur la cybercriminalité du Conseil de l'Europe ou contre les infractions informatiques dans la directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information.

278. Après avoir proposé une définition universelle des violences en ligne il s'agira, dans les développements qui vont suivre, d'étudier l'élaboration des règles minimales encadrant les comportements illicites en ligne. En premier lieu, nous allons analyser la nature juridique et le contenu des textes qui pourraient être adoptés pour prévoir des règles minimales (**Section I**). Ainsi, en second lieu, nous allons étudier les avantages que ces règles minimales pourraient entrainer dans le traitement des cyberviolences au niveau national, régional et international (**Section II**).

[645] M. DELMAS-MARTY, *Les forces imaginantes du droit. Le relatif et l'universel*, Paris, Seuil, 2004, p. 334.

Section I : Le processus d'élaboration des règles minimales contre les comportements illicites en ligne

279. Le fait d'adopter des règles minimales permettrait de constituer un socle de notions minimales pour identifier et qualifier de façon commune les différentes formes de violences en ligne. Cette définition permettrait également d'accorder de peines minimales et ainsi de leur donner l'attention adéquate et de reconnaitre leur spécificité.

280. Dans cette première section, il s'agira, d'un côté, de s'intéresser aux instruments juridiques au niveau régional et international que les États membres de l'Union européenne, du Conseil de l'Europe et des Nations Unies pourraient adopter afin d'intégrer ces règles minimales (**§I**). Puis, de l'autre côté, il s'agira d'étudier le contenu de ces règles minimales à travers une analyse des contenus illicites sur Internet (**§II**).

I. L'adoption par les États des règles minimales contre les cyberviolences

281. Pour analyser l'adoption des règles minimales par les États, il a été nécessaire de diviser cette première section en trois parties. Premièrement, au niveau régional, nous étudierons le fondement pour l'adoption d'une directive européenne par les États membres de l'Union européenne en matière des comportements illicites en ligne (**A**). Deuxièmement, nous analyserons la possibilité d'adopter un protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (**B**). Enfin, au niveau international, nous étudierons la faisabilité de l'adoption d'une convention internationale (**C**).

A. L'adoption d'une directive européenne par les États membre de l'Union européenne

282. L'adoption des règles minimales pourrait se faire à travers l'adoption d'une directive. Nous avons privilégié cet instrument juridique parce que, à la différence d'un règlement, la directive donne aux États membres une plus grande flexibilité. En effet, le règlement

est un acte juridique contraignant qui doit être adopté par les États membres en intégralité. La directive, au contraire, est un instrument juridique qui fixe des objectifs et chaque État membre est libre de les atteindre à travers l'adoption de mesures qu'il considère adéquates.

283. Les comportements illicites sur Internet relèvent majoritairement du droit pénal. Pour cela, afin d'adopter une directive encadrant les contenus illicites en ligne, il faudrait se fonder sur l'article 83 du traité sur le fonctionnement de l'Union européenne (**1**). Il conviendra d'analyser également l'article 81 du traité sur le fonctionnement de l'Union européenne qui encadre la matière civile (**2**).

1. Le fondement en matière pénale : l'article 83 du traité sur le fonctionnement de l'Union européenne

284. La compétence pénale de l'Union européenne a été considérablement étendue grâce à l'adoption du traité de Lisbonne en 2007. La coopération judiciaire en matière pénale figure dans les articles 82 à 86 du traité sur le fonctionnement de l'Union européenne. À cet égard, il est intéressant d'analyser plus spécifiquement l'article 83 qui prévoit un rapprochement des dispositions législatives dans des domaines de criminalité particulièrement grave (§1) et dans des domaines où le rapprochement est nécessaire à l'effectivité des politiques de l'Union européenne (§2)[646].

285. D'abord, l'article 83, paragraphe 1, prévoit la possibilité d'adopter des directives établissant des règles minimales relatives à la définition des infractions pénales et des sanctions dans des domaines de criminalité particulièrement graves et qui ont une dimension transnationale[647]. Or, le même paragraphe spécifie ces domaines de criminalité pour justifier l'intervention du législateur européen. Ces domaines sont : le

[646] Voir notamment D. FLORE, « Contours, limites et perspectives du rapprochement des droits pénaux matériels au sein de l'Union européenne », *Rev. UE*, 2014/582.
[647] Voir : L. ARROYO ZAPATERO et M. MUÑIOZ DE MORALES ROMERO, « Droit pénal européen et Traité de Lisbonne : le cas de l'harmonisation autonome (article 83.1 TFUE) », in G. GIUDICELLI-DELAGE et C. LAZEGES (dir.), *Le droit pénal de l'Union européenne au lendemain du traité de Lisbonne*, Société de législation comparée, 2012, p. 113, qui parlent d'harmonisation autonome.

terrorisme, la traite des êtres humains et l'exploitation des femmes et des enfants, le trafic illicites de drogues et d'armes, le blanchiment d'argent, la corruption, la contrefaçon de moyens de paiement ainsi que la criminalité informatique et organisée. Ces derniers sont des domaines qui ont déjà fait l'objet d'instruments de rapprochement[648]. Ensuite, le paragraphe 2 vient nuancer ces catégories. En effet, il prévoit que l'Union européenne peut être compétente pour établir des règles minimales relatives à la définition des infractions pénales et des sanctions « lorsque le rapprochement des dispositions législatives et réglementaires des États membres en matière pénale s'avère indispensable pour assurer la mise en œuvre efficace d'une politique de l'Union dans un domaine ayant fait l'objet de mesures d'harmonisation »[649]. Enfin, le paragraphe 3, prévoit un mécanisme dit de « frein d'urgence »[650] qui ouvre la possibilité à un État membre de demander la saisine du Conseil européen s'il estime qu'un projet de directive tendant au rapprochement des droits nationaux porte atteinte « aux aspects fondamentaux de son système de justice pénale […] »[651].

286. Les comportements illicites de nature pénale concernant les cyberviolences pourraient entrer dans le champ d'application de l'article 83, paragraphe 1, en particulier dans la notion de criminalité informatique. C'est également la position défendue par la « Commission des libertés civiles, de la justice et des affaires intérieures » et la « Commission des droits des femmes et de l'égalité des genres » dans la résolution sur les cyberviolences basées sur le genre adoptée le 14 décembre 2021[652]. Les commissions demandent, en effet, l'adoption d'une définition générale ainsi que des mesures spécifiques pour lutter contre ces types de violences sur le fondement de l'article 83, paragraphe 1. Les commissions justifient ce fondement en estimant que « le terme « criminalité informatique » mentionné à l'article 83, paragraphe 1, du traité FUE, peut

---

[648] D. FLORE, « Contours, limites et perspectives du rapprochement des droits pénaux matériels au sein de l'Union européenne », *Rev. UE*, 2014/582.
[649]Article 83, paragraphe 2, traité sur le fonctionnement de l'Union européenne. Voir A. BERNARDI, *L'harmonisation pénale accessoire*, in in G. GIUDICELLI-DELAGE et C. LAZEGES (dir.), *Le droit pénal de l'Union européenne au lendemain du traité de Lisbonne*, Société de législation comparée, 2012, p. 153.
[650] Voir V. C. HAGUENAU-MOIZARD, F. GAZIN, et J. LEBLOIS-HAPPE, *Les fondements du droit pénal de l'Union européenne*, 1e édition, Bruxelles, Larcier, 2015, p. 103.
[651] Article 83, paragraphe 3, du traité sur le fonctionnement de l'Union européenne.
[652] Résolution du Parlement européen du 14 décembre 2021 contenant des recommandations à la Commission sur la lutte contre la violence fondée sur le genre : cyberviolence, 2020/2035(INL), point 56.

concerner aussi bien des infractions commises contre des réseaux de communication électronique ou des systèmes d'information que des *infractions commises au moyen de ceux-ci* »[653].

287. Cependant, il faudrait spécifier ce que la « dimension transfrontière » implique. Dans la communication de la Commission européenne sur la politique de l'Union européenne en matière pénale, il est établi que l'adoption de dispositions pénales au niveau de l'Union européenne permettrait « d'empêcher les auteurs d'infraction de se cacher derrière les frontières ou d'exploiter les différences entre les systèmes juridiques nationaux à des fins criminelles »[654]. Or, si la dimension transfrontière concerne seulement ces aspects, il pourrait être difficile de prévoir des règles minimales pour des comportements qui n'ont pas forcement cette dimension, lorsqu'ils sont commis entre personnes dans un même État et lorsque le système juridique est le même. Cependant, l'article 83, paragraphe 1, du traité sur le fonctionnement de l'Union européenne spécifie que cette dimension résulte « du caractère ou des incidences de ces infractions ou d'un besoin particulier de les combattre sur des bases communes »[655]. Or, « le besoin particulier de les combattre sur des bases communes » pourrait justifier la nécessité d'adopter des règles minimales, en particulier, compte tenu de la difficulté des États membres de prévenir et sanctionner les cyberviolences. Il semblerait que cet article vise également les infractions « pour lesquelles une volonté politique d'agir en commun existe, indépendamment même de tout élément transfrontalier intrinsèque »[656].

288. Pour l'adoption des règles minimales en matière de cyberviolences, on pourrait prendre comme exemple la directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information. Cette dernière,

---

[653] Annexe à la résolution du Parlement européen du 14 décembre 2021 contenant des recommandations à la Commission sur la lutte contre la violence fondée sur le genre : cyberviolence, 2020/2035(INL). Italique par l'autrice.
[654] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions vers une politique de l'Union européenne en matière pénale : assurer une mise en œuvre efficace des politiques de l'Union européenne au moyen du droit pénal, COM/2011/0573.
[655] Article 83, paragraphe 1, du traité sur le fonctionnement de l'Union européenne.
[656] D. FLORE, « Contours, limites et perspectives du rapprochement des droits pénaux matériels au sein de l'Union européenne », *Rev. UE*, 2014/582.

adoptée sur le fondement de l'article 83 représente un exemple clair de ce qu'une directive sur les infractions de contenu sur Internet pourrait contenir.

1.1 L'exemple de la directive 2013/40/UE

289. La directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information, a été adoptée avec l'objectif de « […] rapprocher le droit pénal des États membres dans le domaine des attaques contre les systèmes d'information en fixant des règles minimales concernant la définition des infractions pénales et les sanctions applicables, et de renforcer la coopération entre les autorités compétentes […] »[657]. Cette directive est l'une des réponses apportées par l'Union européenne pour faire face au développement constant et inquiétant des atteintes aux systèmes informatiques au sein des États membres de l'Union européenne. Elle s'inscrit dans une politique de « cyber-dissuasion européenne efficace »[658], c'est-à-dire une meilleure coordination européenne en matière de cyberdéfense et cybersécurité.

290. La directive pose le constat qui est très proche de celui que nous faisons en matière de partage de contenus illicites en ligne. En effet, elle énonce qu' « il est nécessaire d'adopter une approche commune en ce qui concerne les éléments constitutifs des infractions pénales »[659]. Ainsi, elle souligne qu'il existe des lacunes et des différences importantes dans les législations et les procédures pénales des États membres en matière d'attaques contre les systèmes d'information qui risquent d'entraver la lutte contre la criminalité organisée et le terrorisme, et de compliquer la coopération policière et judiciaire dans ce domaine[660]. Un parallèle peut être fait avec les cyberviolences de contenu car, comme mentionné dans le chapitre précèdent, l'absence d'un cadre commun peut entraver la poursuite des agresseurs et la réparation des victimes. En outre, la

[657] Voir la directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, point 1.
[658] A. CAMMILLERI, « Intelligence artificielle et droit de la cybersécurité dans l'Union européenne », *RDUE*, 2017/4, p. 134.
[659] Voir la directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, point 8.
[660] *Ibid.* point 27.

directive souligne « la nécessité de prendre d'urgence des mesures complémentaires pour rapprocher le droit pénal »[661] au vu du caractère transnational des systèmes d'information. Cette nécessité peut être, à nouveau, transposée aux cyberviolences.

291. La directive pose des définitions précises des infractions aux systèmes d'information. En effet, elle fixe des règles minimales concernant les définitions pénales en matière d'attaques contre les systèmes d'information[662]. En particulier, de l'article 2 à 7, elle définit entre autres, l'accès illégal à des systèmes d'information, l'atteinte illégale à l'intégrité d'un système et à l'intégrité des données, ainsi que l'interception illégale. Cela permet de créer un cadre commun au sein de l'Union européenne. En effet, les États membres ont été obligés de se conformer à la directive au plus tard le 4 septembre 2015.

292. Dans cet élan, on pourrait assister à l'adoption, au moins au sein de l'Union européenne, d'une directive pour élaborer et harmoniser les définitions des comportements illicites en ligne, fixant ainsi un cadre minimum commun qui permettrait d'évaluer, prévenir et sanctionner les comportements illicites dans l'ensemble des États membres.

293. Si certains États ont déjà des dispositions dans leurs droits nationaux qui sanctionnent les comportements illicites en ligne, la directive permettrait aux États qui n'en disposent pas de se doter de ces mesures. Ainsi, elle pourrait avoir une fonction essentiellement didactique et sensibilisatrice comme c'est le cas pour d'autres directives adoptées par le Parlement européen et le Conseil, par exemple la directive 2011/93/UE, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie[663]. Cette dernière avait été adoptée pour harmoniser les incriminations de certaines infractions relatives aux abus et à l'exploitation sexuelle des enfants. La directive avait été adoptée nonobstant la plupart des infractions étaient déjà inscrites dans les dispositions nationales des États membres.

---

[661] *Ibid.* point 27.
[662] *Ibid.* Art. 1.
[663] Directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil.

2. Le fondement en matière civile : l'article 81 du traité sur le fonctionnement de l'Union européenne

294. En matière civile, c'est l'article 81 du traité sur le fonctionnement de l'Union européenne qui réglemente la coopération judiciaire ayant une incidence transfrontalière.

295. L'article 81, paragraphe 1, prévoit la possibilité d'adopter des mesures de rapprochement des dispositions législatives et réglementaires des États membres, et, comme pour l'article 83, il prévoit cette possibilité lorsqu'il s'agit d'une problématique transfrontière. L'article 81, paragraphe 2, complète le paragraphe précédent en énumérant les catégories dans lesquelles des mesures peuvent être adoptées. En effet, le Parlement et le Conseil peuvent adopter des mesures visant à assurer, entre autres : la reconnaissance mutuelle entre les États membres des décisions judiciaires et extrajudiciaires, et leur exécution, la signification et la notification transfrontières des actes judiciaires et extrajudiciaires. Ainsi que, la compatibilité des règles applicables dans les États membres en matière de conflit de lois et de compétence, la coopération en matière d'obtention des preuves un accès effectif à la justice, l'élimination des obstacles au bon déroulement des procédures civiles, au besoin en favorisant la compatibilité des règles de procédure civile applicables dans les États membres. Et, des mesures assurant le développement de méthodes alternatives de résolution des litiges ainsi qu'un soutien à la formation des magistrats et des personnels de justice.

296. Or, parmi ces critères aucun ne semble pouvoir permettre d'adopter des règles minimales concernant des comportements illicites en ligne relevant du droit civil. Les comportements illicites identifiés sont d'ordre pénal, la seule atteinte de droit civil qui pourrait faire l'objet de l'institution des règles minimales est l'atteinte à la vie privée et il serait souhaitable de prévoir une protection spécifique pour la vie privée en ligne. Il serait possible d'ajouter aux dispositions nationales « traditionnelles » qui concernent la vie privée une dimension « cyber », en prévoyant clairement dans les textes le même degré de protection de la vie privée hors ligne pour les atteintes en ligne.

297. Les règles minimales concerneraient ainsi seulement des dispositions de droit pénal, comme pour la directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information. Cela permettrait la fixation des règles minimales et plusieurs garanties, notamment l'assurance d'une égalité de traitement entre les citoyens européens mais également un plus grand repérage et suivi de ces comportements[664]. Fixer ces règles minimales permettrait d'établir un cadre commun minimum au sein des États membres de l'Union européenne et influencer les autres États non membres notamment ceux du Conseil de l'Europe. Cependant, les États du Conseil de l'Europe pourraient se doter d'un instrument encadrant les cyberviolences de contenu. Il s'agirait d'ajouter un protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité.

B. L'adoption d'un protocole additionnel à la Convention sur la cybercriminalité pour les États membres du Conseil de l'Europe

298. Après avoir analysé le fondement d'une directive qui serait adoptée par les États membres de l'Union européenne, il s'agira d'étudier la possibilité pour les États membres du Conseil de l'Europe d'adopter un protocole additionnel à la Convention sur la cybecriminalité (**1**). Ensuite, on analysera comment ce texte serait accueilli par les États membres de la Convention (**2**).

1. La création d'un troisième protocole additionnel sur les infractions de contenu

299. Le Conseil de l'Europe demeure la seule et unique organisation régionale et internationale à avoir adopté une convention internationale sur la cybercriminalité. Cette convention a trois objectifs : d'abord, harmoniser le droit matériel pénal interne dans le domaine de la cybercriminalité. Ensuite, prévoir les pouvoirs de procédure pénale

[664] Ce point sera étudié dans la section II.

internes nécessaires pour les enquêtes et les poursuites concernant les infractions commises au moyen d'un système informatique. Enfin, mettre en place un régime rapide et efficace de coopération internationale[665].

300. La Convention ne concerne pas les infractions de contenu sauf celles relatives à la pornographie infantile. En effet, le Comité chargé de la rédaction de la Convention avait voulu insérer des dispositions concernant les comportements illicites de contenu, en particulier sur la diffusion de la propagande raciste, mais les États membres du Conseil de l'Europe n'ont pas trouvé un consensus. Même si certaines délégations étaient favorables à l'inclusion de cette infraction pénale, d'autres ne l'étaient pas à cause de l'atteinte potentielle à la liberté d'expression[666]. Pour cela, les atteintes racistes et xénophobes ont été traités dans un protocole additionnel à la Convention élaboré par le Comité européen pour les problèmes criminels. Ce premier protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques a un double objectif : harmoniser le droit pénal matériel en matière de racisme et xénophobie sur Internet et améliorer la coopération internationale à cet égard. Le protocole énumère les infractions que chaque État partie doit s'engager à sanctionner dans sa législation nationale, par exemple la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques, les menaces et insultes avec une motivation raciste et xénophobe ainsi que la négation, la minimisation grossière, l'approbation ou la justification du génocide ou des crimes contre l'humanité sur Internet.

301. Dans le même sens, un protocole additionnel sur plusieurs infractions de contenu pourrait être adopté. Il s'agirait donc du troisième protocole additionnel[667]. Celui-ci permettrait d'harmoniser les sanctions et renforcer la coopération des États vis-à-vis des violences sexistes et sexuelles. Ce protocole pourrait faciliter, comme celui sur le racisme et la xénophobie, la lutte contre les crimes sur Internet au niveau national et international. En effet, l'adoption des mesures contre les infractions de contenu qui

---

[665] Voir Conseil de l'Europe, *Rapport explicatif de la Convention sur la cybercriminalité*, 23 novembre 2001, point 16.
[666] *Ibid.* point 35.
[667] En effet un deuxième rapport additionnel a été adopté le 17 novembre 2021 et concerne le renforcement de la coopération et de la divulgation de preuves électroniques.

seraient prévues dans un nouveau protocole pourraient empêcher l'utilisation abusive des systèmes informatiques par des États qui sont dotés de lois peu protectrices des droits fondamentaux.

302. Ce protocole pourrait ainsi contenir des mesures générales et mentionner plusieurs infractions de contenu, y compris certaines qui ont déjà été adoptées par certains États membres. En effet, il serait nécessaire de prévoir des dispositions explicites de ces infractions de contenus sur Internet au vu de l'urgence et de l'expansion des cyberviolences dans la dernière décennie. Cela avait d'ailleurs été souligné également par le rapport explicatif de la Convention sur la cybercriminalité à propos de l'article 9 sur les infractions se rapportant à la pornographie infantile. En effet, le rapport explicatif avait clarifié que : « cette disposition [l'article 9] incrimine différents aspects de la production, de la possession et de la diffusion de pornographie enfantine. La plupart des États incriminent déjà la production traditionnelle et la diffusion physique de pédopornographie, *mais étant donné que l'Internet est de plus en plus utilisé comme instrument principal pour l'échange de ce matériel, il a été considéré que des dispositions spécifiques dans un instrument juridique international pour lutter contre cette nouvelle forme d'exploitation sexuelle enfantine et de mise en danger des enfants étaient tout à fait essentielles* »[668].

303. Comme cela a été le cas pour le protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe, la rédaction d'un nouveau protocole sur plusieurs infractions de contenu pourrait être confiée au Comité européen pour les problèmes criminels. En effet, ce Comité supervise et coordonne les activités du Conseil de l'Europe dans le domaine de la prévention et de la lutte contre la criminalité.

[668] Conseil de l'Europe, *Rapport explicatif de la Convention sur la cybercriminalité,* 23 novembre 2001, point 93. Italique de l'autrice.

2. L'efficacité d'un protocole additionnel dépendante de la volonté des États

304. L'adoption d'un protocole additionnel à la Convention sur la cybercriminalité sur les infractions de contenu sur Internet pourrait ne pas faire l'unanimité parmi les États membres du Conseil de l'Europe. Il y a l'exemple du premier protocole additionnel qui a été ratifié par un faible nombre d'États ayant ratifié la Convention sur la cybercriminalité. En effet, alors que tous les États membres du Conseil de l'Europe, sauf la Russie et l'Irlande, ont ratifié la Convention, ils sont dix-sept à ne pas encore avoir signé ou ratifié le protocole. Cela montre une certaine méfiance vis-à-vis de ce texte. Cette méfiance est due à une possible atteinte excessive à la liberté d'expression des utilisateurs et probablement à la volonté des États de ne pas ajouter des obligations contraignantes dans leur droit national en matière de droits fondamentaux.

305. De plus, nous retrouvons cette méfiance envers d'autres conventions protectrices des droits fondamentaux, par exemple, la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique. Cette dernière, alors qu'elle pourrait servir de fondement pour définir et encadrer certaines cyber infractions sexuelles et sexiste de contenu, n'a pas encore été ratifiée par douze des quarante-sept États membres du Conseil de l'Europe. En outre, la Turquie, l'un des États à l'origine du texte, a dénoncé la Convention en 2021, devenant ainsi le premier État à l'avoir ratifiée et le premier à l'avoir quittée[669].

306. Or, pour que le protocole soit efficace, notamment afin d'atteindre l'harmonisation des législations, il faudrait que tous les États membres du Conseil de l'Europe, ou au moins ceux parties à la Convention sur la cybercriminalité, le ratifient. Toutefois, il se peut que cette analyse soit erronée. En effet, vingt ans sont passés depuis l'adoption de la Convention sur la cybercriminalité et du protocole sur le racisme et la xénophobie. Il

[669] V. BELLAMI, W. CARAZO-MÉNDEZ, C. GRADIN, « Dénonciation de la Convention d'Istanbul par la Turquie : L'insoluble équilibre entre volonté étatique et garantie des droits des femmes et des filles », *Revue Droits Fondamentaux*, n°19, 2021. Disponible sur : *https://www.crdh.fr/revue/n-19-2021/denonciation-de-la-convention-distanbul-par-la-turquie-linsoluble-equilibre-entre-volonte-etatique-et-garantie-des-droits-des-femmes-et-des-filles/*

se peut que, face à une pression montante de l'opinion publique vis-à-vis de la réglementation d'Internet et des ravages causés par les dérives des réseaux sociaux, les États soient plus ouverts aux négociations et à l'acceptation de certaines dispositions pouvant mieux protéger les droits fondamentaux des individus sur Internet.

307. Après avoir analysé le cadre régional et la possibilité d'adopter un protocole additionnel à la convention sur la cybercriminalité, il est intéressant de proposer une voie multilatérale avec l'adoption d'une convention internationale par les Nations Unies.

C. L'adoption d'une convention internationale par les Nations unies

308. C'est par la résolution du Conseil des droits de l'Homme, du 29 juin 2012, sur la promotion, la protection et l'exercice des droits de l'Homme sur l'Internet, que, pour la première fois dans l'enceinte des Nations unies, a été reconnue la protection des droits humains sur Internet[670]. Avant cette date, nous pouvons mentionner des engagements plus généraux sur la société de l'information pris à Genève en 2004 et à Tunis en 2005 par les États membres des Nations unies réunis par l'Union internationale des télécommunications (UIT). À cette occasion, les États ont exprimé, à travers une Déclaration de principes, que les nouvelles technologies offraient des possibilités en faveur des objectifs du millénaires, ancêtres des Objectifs de Développement Durable (ODD), c'est-à-dire l'égalité entre les femmes et les hommes, la lutte contre l'extrême pauvreté et la faim ou encore l'autonomie des femmes[671]. Toutefois, aucune référence avait été faite aux violences en ligne.

309. Sous proposition d'un État comme la France, qui met en avant plusieurs dispositions sur les cyberviolences en droit interne ou d'un autre État comme l'Allemagne qui a

---

[670] Conseil des droits de l'Homme, *La promotion, la protection et l'exercice des droits de l'homme sur l'Internet*, 29 juillet 2012, A/HRC/20/L.13.
[671] Voir : Sommet mondial sur la société de l'information, Déclaration de principes, *Construire la société de l'information : un défi mondial pour le nouveau millénaire*, WSIS-03/GENEVA/DOC/4-F, 12 mai 2004, disponible sur : https://www.itu.int/net/wsis/docs/geneva/official/dop-fr.html

adopté une loi *ad hoc*[672], un projet de texte pourrait être proposé au Conseil des droits de l'Homme des Nations unies. Le Conseil des droits de l'Homme pourrait constituer un groupe de travail pour l'élaboration de la convention avec des États, des experts internationaux, des membres de la société civile, des plateformes ainsi que des victimes de cyberviolence. Cette nouvelle convention pourrait contenir, comme pour les précédentes propositions, une définition générale des cyberviolences ainsi que des règles minimales couvrant la variété d'infractions présentes en ligne (qui seront développées dans le paragraphe suivant).

310. Une fois adoptée, la convention pourra être dotée, comme pour les autres conventions onusiennes, d'un comité d'experts pour suivre l'effective application du traité. Cette mission pourrait être confiée au Comité des droits de l'Homme ou un comité nouveau qui suivrait les violations des droits humains sur internet et l'application de cette nouvelle convention. Toutefois, à l'instar des réflexions sur les obstacles de l'adoption d'un troisième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, on serait confronté aux mêmes problématiques. En particulier, au vu des différentes appréciations vis-à-vis de la liberté d'expression.

311. Avant de connaître les avantages des règles minimales, il serait utile de comprendre quels comportements pourraient être prévus dans ces projets de texte.

II. Les comportements illicites encadrés par les règles minimales

312. La directive proposée pourrait prendre en compte plusieurs typologies de comportements illicites et, en particulier, ceux qui ne sont pas inscrits dans des Conventions internationales ou dans d'autres directives européennes afin de garantir des règles minimales de protection.

[672] La loi Netzwerkdurchsetzungsgesetz (NetzDG) du 30 juin 2017.

313. La liste qui sera présentée dans les développements qui suivront n'a pas la prétention d'être un catalogue exhaustif des comportements illicites[673]. De plus, dans un contexte particulier et changeant comme celui des nouvelles technologies, l'adoption d'une définition générale de cyberviolences[674] permettrait d'encadrer des comportements illicites qui n'ont pas encore été détectés mais qui pourraient l'être dans les mois et les années à venir. Cela, afin de ne pas rendre ces nouveaux textes caducs très rapidement.

314. Certains comportements illicites analysés sont déjà prévus dans les législations nationales en tant qu'infractions « traditionnelles ». Toutefois il serait utile de spécifier le contexte numérique. Par exemple, à travers des circonstances aggravantes ou bien des nouvelles dispositions, pour garantir que ces atteintes soient sanctionnées aussi bien hors ligne qu'en ligne. En effet, mêmes si certains comportements sont déjà prévus dans les droits nationaux, il est nécessaire de les inscrire dans ces nouveaux textes afin que tous les États membres adoptent des mesures contre les cyberviolences, surtout ceux qui ont des législations peu protectrices des droits fondamentaux.

315. Après avoir analysé les différents types de comportements illicites traités par la doctrine et par la jurisprudence, trois catégories prioritaires ont été identifiées : les atteintes à la personne, à son intégrité et ses libertés (**A**), les atteintes sexistes et sexuelles (**B**) et les atteintes de tout genre répétées et groupées (**C**).

A. Les atteintes à la personne, à son intégrité et à ses libertés

316. Concernant les atteintes à la personne, à son intégrité et à ses libertés, plusieurs comportement illicites sont identifiés.

317. **La violation du secret de correspondance -** Premièrement, il faudrait protéger toute personne contre les atteintes à son droit à la vie privée et prendre en compte l'atteinte au secret de correspondances qui peut être violé de façon visible mais également invisible par le biais de logiciels espions. Très souvent la traque furtive en ligne touche particulièrement les femmes et

[673] Nous ne traitons pas les atteintes aux biens, comme il a été expliqué en introduction. Ainsi que, les atteintes aux droits de la propriété intellectuelle et artistique.
[674] Voir le chapitre qui précède.

rentre dans le cadre des violences domestiques de la part d'un partenaire intime[675]. À cet égard, la Cour européenne des droits de l'Homme a estimé pour la première fois dans son arrêt *Buturuga c. Roumanie* que « les violations informatiques de la vie privée, l'intrusion dans l'ordinateur de la victime et la prise, le partage et la manipulation des données et des images, y compris des données intimes »[676] pouvaient constituer un aspect des violences à l'encontre des femmes. Ces atteintes constituent ce qu'on appelle le « cybercontrôle » ou la « cybersurveillance », qui concerne plusieurs formes de violences exercées pour contrôler tous les aspects de la vie de la victime, notamment les déplacements ou les relations sociales[677]. L'affaire *Buturuga* est très instructive vis-à-vis de la méconnaissance par les autorités nationales des atteintes qui peuvent survenir à travers les réseaux sociaux. En effet, la requérante alléguait avoir été victime de violence domestique et lors de son dépôt de plainte elle avait demandé comme élément de preuve une perquisition électronique de l'ordinateur de la famille au motif que le défendeur avait abusivement consulté son compte Facebook et, en particulier, avait fait des copies des conversations privées, de ses documents et photos. Les autorités de police roumaines avaient refusé d'examiner sa demande au motif que cela ne présentait pas de liens avec les violences dont elle disait être victime. De plus, le tribunal de première instance avait ensuite considéré qu'il n'y avait pas eu atteinte au secret de correspondance. En effet, selon le tribunal, les données publiées sur les réseaux sociaux étaient publiques. Nous pouvons également citer l'arrêt *Volodina c. Russie* dans lequel la Cour européenne des droits de l'Homme avait été saisi car les autorités russes avaient, entre autres, refusé d'ouvrir une enquête pénale pour les menaces de mort reçues par la victime sur Internet au motif qu'elles n'étaient pas « réelles »[678]. Cela démontre, non seulement un manque de connaissance des violences à l'égard des femmes[679], mais également des comportements illicites en ligne et, en particulier, des aspects techniques des réseaux sociaux, notamment la distinction entre ce qui est public et privé.

318. La haine en ligne - Il faudrait prévoir des dispositions concernant le discours de haine en ligne qui se manifeste par plusieurs comportements illicites comme les

---

[675] EIGE, *Cyberviolence à l'égard des femmes et des filles*, 23 juin 2017, pp. 1 et 2. Disponible sur : https://eige.europa.eu/publications/cyber-violence-against-women-and-girls.
[676] Cour EDH, *Buturuga c. Roumanie* du 11 février 2020, req. n° 56867/15, §74.
[677] Centre Hubertine Auclert, *Cyberviolences conjugales, recherche-action menée auprès de femmes victimes de violences conjugales et des professionnel-le-s les accompagnant*, 2018, p. 60. Disponible sur : https://www.centre-hubertine-auclert.fr/outil/rapport-cyberviolences-conjugales-2018
[678] Cour EDH, *Volodina c. Russie* du 14 décembre 2021, req. n° 40419/19, §11.
[679] En effet, comme prévu dans la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, les violences conjugales ne sont pas seulement physiques mais peuvent comporter des aspects psychologiques. Ainsi, la violation des correspondances peut être l'une des causes de violences psychologiques.

messages et commentaires malveillants, insultants et humiliants[680] qui peuvent inciter, entre autres, à la haine ou à la violence. Cela a été défini par le Conseil de l'Europe comme : « tout type d'expression qui incite à, promeut, diffuse ou justifie la violence, la haine ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes, ou qui les dénigre, en raison de leurs caractéristiques personnelles ou de leur statut réels ou attribués telles que [une prétendue] «race», la couleur, la langue, la religion, la nationalité, l'origine nationale ou ethnique, l'âge, le handicap, le sexe, l'identité de genre et l'orientation sexuelle »[681]. Or, ces types de comportements sont déjà sanctionnés par plusieurs textes nationaux et internationaux comme le protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Ce dernier, définit tout « matériel raciste et xénophobe » comme « tout écrit, image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes »[682]. Selon certains auteurs[683], le discours de haine « se trouve dans un lien complexe avec la liberté d'expression, les droits des groupes, ainsi que les concepts de dignité, de liberté et d'égalité […] le discours de haine [est

[680] En anglais, ce type de comportements sont identifiés comme étant parti du « hate speech online ». Voir notamment : T.E SYNODINOU, *EU Internet law - regulation and enforcement*, Springer, 1st ed. 2017 édition, 9 novembre 2017, p, 370 et s.

[681] Voir la recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine adoptée par le Comité des Ministres le 20 mai 2022, lors de la 132e Session du Comité des Ministres.

[682] Article 2 du protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Concernant l'Union européenne à ce sujet, voir la décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008F0913&from=en*. Voir également l'action commune du 15 juillet 1996 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, concernant l'action contre le racisme et la xénophobie, disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31996F0443&from=EN. Ainsi que, la résolution législative du Parlement européen sur la proposition de décision-cadre du Conseil concernant la lutte contre le racisme et la xénophobie, COM(2001) 664 — C5-0689/2001 — 2001/ 0270(CNS), disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52002AP0363&from=FR.

[683] L. SILVA, M. MONDAL, D. CORREA et al., *Analyzing the Targets of Hate in Online Social Media*, Tenth International AAAI Conference on Web and Social Media, Vol. 10 No. 1, 2016, p.688. Disponible sur : https://arxiv.org/pdf/1603.07709.pdf

défini] comme toute infraction motivée, en tout ou en partie, par le parti pris de l'auteur contre un aspect d'un groupe de personnes. Selon cette définition, le discours haineux en ligne n'est pas nécessairement un crime, mais il peut quand même nuire aux gens »[684].

319. La Cour européenne des droits de l'Homme a été plusieurs fois amenée à juger des affaires concernant les discours de haine. Dans son arrêt *Lilliendahl c. Islande*[685] elle a souscrit à la conclusion de la Cour suprême islandaise, en définissant « graves, fortement blessants et préjudiciables » des commentaires homophobes d'un ressortissant islandais. Ce dernier avait employé en ligne, en référence aux personnes homosexuelles, les termes « kynvilla » (déviation sexuelle) et « kynvillingar » (déviants sexuels).

320. Les plateformes en ligne donnent également leur définition de discours de haine et l'inscrivent dans les « standards de la communauté »[686]. Facebook, par exemple, n'autorise pas les discours incitant à la haine « parce que ces discours créent une atmosphère d'intimidation et d'exclusion, et peuvent aboutir à des violences dans le monde réel »[687]. La plateforme définit les discours haineux « comme une attaque directe sur des personnes fondée sur ce que nous appelons des caractéristiques protégées : l'origine ethnique, l'origine nationale, la religion, l'orientation sexuelle, la caste, le sexe, le genre, l'identité sexuelle, et les maladies graves ou les handicaps »[688]. Elle définit « une attaque » comme « un discours violent ou déshumanisant, une affirmation d'infériorité, ou un appel à l'exclusion ou à la ségrégation »[689]. Des dispositions sont prévues également par le réseau Twitter qui parle d'« imagerie

---

[684] *Ibid.* p.688. Traduction libre de l'auteure. Texte original : « hate speech lies in a complex nexus with freedom of expression, group rights, as well as concepts of dignity, liberty, and equality […]. We define hate speech as any offense motivated, in whole or in a part, by the offender's bias against an aspect of a group of people. Under this definition, online hate speech may not necessarily be a crime, but still harm people ».
[685] Cour EDH, 12 mai 2020, *Lilliendahl c.Islande*, req. n° 29297/18.
[686] On fait référence ici aux « standards » ou « standards de communauté », c'est-à-dire des règles que les plateformes intègrent dans leurs Conditions Générales d'Utilisation (CGU). Ces règles définissent les catégories de contenus dont la plateforme autorise la publication sur les pages de son site. Pour en savoir plus sur les standards de Facebook, V. https://www.facebook.com/communitystandards/. Le réseau social Twitter les appelle quant à lui « Règles et politiques de Twitter ». V. pour plus d'informations : https://help.twitter.com/fr/rules-and-policies#twitter-rules.
[687] Facebook, Standard de la communauté Facebook, Discours haineux, disponible sur : https://www.facebook.com/communitystandards/hate_speech
[688] *Ibid.*
[689] *Ibid.*

haineuse »[690] c'est-à-dire « les logos, symboles ou images dont le but est d'encourager l'hostilité et la méchanceté à l'encontre d'autres personnes sur la base de leur race, religion, handicap, orientation sexuelle, identité sexuelle ou origine ethnique/nationalité sont considérés comme de l'imagerie haineuse »[691]. Sur l'onglet « règles et politiques », Twitter dénombre de façon non exhaustive les exemples d'imagerie haineuse, par exemple : les croix gammées, les images manipulées incluant des étoiles jaunes ou des images modifiées pour intégrer des caractéristiques animales.

321. Les discours haineux sont aussi à la base du code de conduite signé par plusieurs plateformes avec la Commission européenne[692]. En le signant, les plateformes[693] s'engagent, d'abord, à mettre en place des mesures efficaces d'examen des signalements de discours haineux illégaux. Ensuite, à fournir les informations afin d'améliorer le blocage de ces discours. Et, enfin, à établir des règles et lignes directrices internes qui précisent l'interdiction de la promotion de la violence et des comportements haineux. Les dénominateurs communs de ces définitions sont les attaques aux caractéristiques de la personne ou à ses croyances, à son orientation sexuelle ou identité de genre. En septembre 2020, après un boycott mondial[694], plusieurs plateformes, dont Facebook, YouTube et Twitter, ont conclu un accord avec la Fédération mondiale des annonceurs (« World Federation of Advertisers » - WFA) afin de mieux lutter contre les contenus qui incitent à la haine. L'accord contient plusieurs définitions concernant les critères pour détecter les discours de haine afin d'éviter la multiplication et la différenciation des critères entre une plateforme et l'autre[695]. En octobre 2020, Facebook a également

---

[690] Twitter, Sécurité et cybercriminalité, Conduite haineuse, disponible sur : https://help.twitter.com/fr/rules-and-policies/hateful-conduct-policy
[691] *Ibid.*
[692] Commission européenne, *Countering illegal hate speech online*, disponible sur : https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300
[693] Les signataires originaires sont : Facebook, Twitter, YouTube et Microsoft. Depuis 2018 trois autres plateformes se sont ajoutées : Jeuxvideo.com, Snapchat et Dailymotion.
[694] Plusieurs annonceurs ont décidé de suspendre leur publicité sur Facebook notamment pour lutter contre la haine en ligne à travers la campagne #StopHateForProfit. Des célébrités mondiales ont également cessé d'utiliser Facebook et Instagram pendant 24h pour protester contre le laxisme des plateformes vis-à-vis des discours haineux.
[695] Pour plus de détails, voir : World Federation of Advertisers, *WFA and platforms make major progress to address harmful content*, 23 September 2020. Disponible sur : https://wfanet.org/knowledge/item/2020/09/23/WFA-and-platforms-make-major-progress-to-address-harmful-content

annoncé le retrait au niveau mondial de tout contenu négationniste. Avant cette décision, ce retrait était prévu seulement pour les États qui condamnaient juridiquement ces propos, comme la France ou l'Allemagne.

322. La diffamation et l'injure - Il faudrait également rappeler les atteintes à l'honneur et à la considération de la personne. Pour cela, il s'agit surtout d'analyser la diffamation et l'injure en ligne.

En premier lieu, pour définir la diffamation, en ligne comme hors ligne, une référence peut être faite au droit français qui la décrit comme « toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé […] »[696]. La diffamation peut être homophobe, raciste ou sexiste. Les droits des États membres de l'Union européenne sont assez similaires en la matière. Par exemple, le droit italien l'inscrit à l'article 595 du Code pénal et la définit comme en droit français. Le droit belge y ajoute l'exposition au mépris public : « l'imputation méchante, à une personne, d'un fait précis qui est de nature à porter atteinte à l'honneur de cette personne ou à l'exposer au mépris public et pour lequel la loi n'admet pas la preuve du fait imputé »[697]. Il n'existe pas de véritable réglementation européenne en la matière, la diffamation est appréhendée « sous l'angle d'un « phénomène » que la matière européenne et constitutionnelle va appréhender par deux biais potentiellement propres celui d'une justice supranationale européenne et celui d'une justice nationale suprême »[698]. En droit international, on peut citer l'article 10 de la Convention pour la sauvegarde de droits de l'Homme car il protège la « réputation ou les droits d'autrui », ainsi que, l'article 19, point 3 a), du Pacte international relatif aux droits civils et politiques des Nations Unies qui prévoit la protection du « respect des droits ou de la réputation d'autrui ».

En second lieu, l'injure se distingue de la diffamation car elle ne se réfère pas à l'imputation d'un fait. Il s'agit d'une parole, un écrit ou tout autre expression de la

---

[696] Article 29 de la loi du 29 juillet 1881 sur la liberté de la presse.
[697] Article 443 du Code pénal belge.
[698] J. S. BERGÉ, « La justice saisie par la Cour de Justice : recherche d'une spécificité du droit de l'Union européenne en matière de libre circulation de l'information diffamatoire », in L. BURGORGUE-LARSEN et G. CALVÈS, *La diffamation saisie par les juges en Europe sous la direction*, Cahiers européens, Pedone, 2019.

pensée, adressé à une personne dans le but de la blesser ou offenser. Elle peut être publique et/ou privée qu'elle soit en ligne ou hors ligne. En effet, comme hors ligne, sur Internet il existe des lieux accessibles au public ou, au contraire, privés. Tout dépend des paramètres du compte. L'injure publique peut être répandue sur les réseaux sociaux lorsqu'une publication est faite en mode public, par exemple lorsqu'une personne publie un commentaire sur son mur Facebook ou sur son fil Twitter lorsque le compte est public[699]. Ou bien, privé quand un individu l'écrit à travers sa messagerie privée (ex : Messenger) à un autre utilisateur.

323. Le « swatting » ou canular téléphonique - Un autre phénomène répréhensible est celui du « swatting », terme qui a comme racine « SWAT » les forces spéciales américaines. Ce terme désigne un canular téléphonique où une personne qui souhaite rester anonyme envoie d'urgence et inutilement les services de police chez quelqu'un, le plus souvent un particulier, afin de nuire à sa personne, l'humilier et le mettre dans une situation dégradante. Avant de passer à l'acte, la personne étudie la victime pour avoir le maximum d'informations pour ensuite appeler les agents de police et leur annoncer qu'elle est en grave danger ou qu'elle représente elle-même un danger. Ce terme est aussi employé lors de fausses alertes à la bombe ou attentat. Ce phénomène s'est amplifié avec Internet qui permet facilement à un individu de connaître les informations personnelles de sa victime. En outre, l'auteur peut, grâce à la technologie, modifier le numéro d'appel de l'émetteur et faire croire au récepteur que l'appel vient du téléphone de la victime.

---

[699] Le mur Facebook n'est pas toujours considéré comme un lieu public. Par exemple, la jurisprudence française n'est pas concordante, en effet pour la Cour d'appel de Reims - CA Reims, 9 juin 2010, n°009-03209 - le mur Facebook est présumé public puisque « *nul ne peut ignorer que Facebook, qui est un réseau accessible par connexion Internet, ne garantit pas toujours la confidentialité nécessaire* ». Cette thèse a été confirmée par la Cour d'appel de Besançon le 15 novembre 2011, n°10-02642. Cependant, les Cours d'appel de Rouen - CA Rouen 15 novembre 201, n°11-0187 - et de Bordeaux - CA Bordeaux 1 avril 2014, n°13-01992 - ont pu considérer que le « mur Facebook » était présumé privé. Pour la Cour d'appel de Rouen en effet « *il ne peut être affirmé de manière absolue que la jurisprudence actuelle nie à Facebook le caractère d'espace privé, alors que ce réseau peut constituer soit un espace privé, soit un espace public en fonction des paramétrages effectués par son utilisateur* ». Ainsi, dans un arrêt de 2015, la Cour d'appel de Paris a également considéré que le mur Facebook avait un caractère privé, en l'espèce ce dernier n'était accessible qu'à 14 personnes (Cour d'appel de Paris, 3 décembre 2015, n°13-01746).
Les juridictions françaises ont à plusieurs reprises étudiés le nombre d'amis ou followers des comptes incriminés. Par exemple elle a pu estimer que si le nombre d'amis sur Facebook dépassait un certain nombre alors les messages litigieux devaient être considérés comme publics (Civ. 1re, 10 avril 2013, n° 11–19.530). Concernant Twitter, la Cour de cassation a estimé que lorsque le compte est public les publications sont présumées publiques (Cour de cassation, Chambre criminelle, 11 décembre 2018, 17-85.159).

324. Aux États-Unis cette infraction s'est surtout développée parmi les joueurs de jeux en ligne, comme en France, ainsi que contre des célébrités ou personnalités politiques[700]. Cette infraction peut avoir des conséquences très graves et caractériser d'autres types d'infractions, par exemple l'homicide involontaire. C'est le cas de l'américain Tyler Barriss condamné à 20 ans de réclusion pour avoir appelé les secours pour une soi-disant prise d'otage. En effet, lorsque les policiers se sont rendus sur place ils ont tué un jeune homme en pensant erronément qu'il était en train de prendre son arme[701]. Mais encore, l'affaire de l'hacker franco-israélien Ulcan renvoyé par un juge d'instruction en 2019 aux assises en France car accusé d'avoir fait intervenir les forces de l'ordre chez les parents d'un journaliste qu'il harcelait. Suite à cette intervention le père est décédé d'infarctus[702]. On peut également ajouter que cette infraction a des conséquences sur les forces de l'ordre qui ressentent un sentiment de manipulation et de mise en danger de la vie d'autrui[703].

325. **La divulgation d'informations personnelles -** Un autre comportement illicite en ligne est celui du « dox(x)ing » qui est une pratique qui consiste à rechercher et à divulguer les informations d'une personne sans son consentement. Ces informations peuvent être multiples : le nom, le numéro de téléphone, de sécurité sociale ou de compte bancaire, l'adresse personnelle ou des informations concernant des activités auxquelles la personne prend part. Un exemple de doxing peut être illustré par les actions menées par le collectif « Anonymous »[704] qui a dévoilé, entre autres, plusieurs informations personnelles sur des membres du Ku Klux Klan[705]. Plusieurs infractions peuvent être commises pour mener cette infraction, par exemple si les informations partagées ont été

---

[700] Voir : M. JAMES ENZWEILER, « Swatting Political Discourse: A Domestic Terrorism Threat », *Notre Dame Law Review*, Vol. 90, 2015.
[701] Le Monde, *« Swatting » : vingt ans de prison pour un canular téléphonique ayant mené à la mort d'un homme*, 1er avril 2019. Disponible sur : https://www.lemonde.fr/pixels/article/2019/04/01/swatting-vingt-ans-de-prison-pour-un-canular-telephonique-ayant-mene-a-la-mort-d-un-homme_5444226_4408996.html
[702] C. FÉRAL-SCHUHL, *Cyberdroit - Le droit à l'épreuve de l'Internet 2020-2021*, 02/2020, 8è édition.
[703] N. ESTANO, « Nouvelles technologies et cyberharcèlement : l'exemple du swatting », *Criminologie*, Volume 52, Numéro 2, Automne 2019, p. 13–32. Disponible sur : https://www.erudit.org/fr/revues/crimino/2019-v52-n2-crimino04971/1065854ar/
[704] Le collectif Anonymous est composé par des personnes qui utilisent leur compétence en informatique et piratage pour mener des actions qui ont pour objectif de favoriser des changements politiques et sociaux.
[705]L. FRANCESCHI-BICCHIERAI, *Anonymous Hackers Officially Dox Hundreds of Alleged KKK Members*, VICE, 6 novembre 2015. Disponible sur : https://www.vice.com/en_us/article/kb7eyv/anonymous-hackers-officially-dox-hundreds-of-alleged-kkk-members

obtenues par des méthodes illégales comme le piratage ou le « spear phishing »[706]. Ainsi, la divulgation d'informations personnelles peut être considérée comme une atteinte à la vie privée, un acte d'intimidation ou de diffamation et également du cyberharcèlement. Plus graves sont les cas de doxing qui ont de répercussions hors ligne et qui peuvent mener au licenciement de la victime, à du harcèlement et à des atteintes à l'intégrité physique. On peut également constater l'existence de cas de « doxing » couplés avec du « swatting », par exemple quand on fait livrer des marchandises non payées à des personnes dont on s'est procuré l'adresse.

326. **La provocation au suicide, au meurtre et au viol -** Il est important de rappeler les provocations au suicide, au meurtre ou au viol. Le plus souvent il s'agit de commentaires ou messages sur les blogs, forums ou réseaux sociaux. Concernant les appels au suicide, ces dernières années il y a eu l'apparition de défis en ligne, notamment le « Momo challenge » (ou Défi de Momo) et le « Blue Whale Challenge » (ou Défi de la Baleine Bleue). D'une part, le Momo Challenge est une légende qui s'est propagée sur les réseaux sociaux dans laquelle un personnage fantastique nommé Momo contacte des jeunes pour leur faire accomplir des défis dangereux dont le suicide par défenestration. D'autre part, le Blue Whale Challenge apparu en 2015 et soupçonné d'être à l'origine d'accidents et des suicides chez les adolescents, se base sur le même principe du Momo Challenge. Un jeune entre en contact avec un « tuteur » sur les réseaux sociaux qui lui ordonne d'accomplir de défis dangereux qui comportent de blessures corporelles. Ce dernier défi avait été notamment cité par le Parlement européen dans sa résolution du 3 octobre 2017 pour alerter sur la dangerosité de ces pratiques auprès de plus jeunes[707].

327. **Le « happy slapping » ou vidéo-agression -** Concernant l'atteinte à l'intégrité de la personne, il y a également le phénomène du « happy slapping » (vidéo-agression en français), c'est-à-dire des violences perpétrées sur des personnes, enregistrées et diffusées en direct. Il peut y avoir plusieurs exemples : des violences physiques, sexuelles, acte des barbaries ou de torture. Ce phénomène combine les violences en ligne

[706] Le « spear phishing » est une variante de l'hameçonnage. L'hameçonnage consiste à envoyer un message à un grand nombre d'utilisateurs afin d'obtenir des informations confidentielles et personnelles. Le « spear phishing » consiste au contraire à l'envoi ciblé à un groupe restreint d'utilisateurs, voir un seul, cependant l'objectif reste le même.
[707] Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité (2017/2068(INI))

avec les violences hors ligne. En France, comme l'explique l'avocate Christiane Féral-Schuhl[708], l'article 222-33-3 du Code pénal depuis la loi du 5 mars 2007 établit une distinction entre : l'auteur de l'atteinte volontaire à l'intégrité d'autrui, le complice de l'auteur de violence qui filme l'agression et qui s'expose, pour cela, aux mêmes peines que ce dernier ainsi que la personne qui diffuse la vidéo.[709] Les mêmes principes sont appliqués par le juge italien[710].

328. L'usurpation d'identité - Une autre infraction très répandue est l'usurpation d'identité. Selon Fanny Georges, il existe trois types d'identités numériques. D'abord, l'identité déclarative ou représentation de soi qui se « compose de données saisies directement par l'utilisateur »[711], ensuite l'identité agissante qui est « constituée des messages répertoriés par le Système concernant les activités de l'utilisateur »[712] et, enfin, l'identité calculée qui se compose « de chiffres, produits du calcul du Système, qui sont dispersés sur le profil de l'utilisateur »[713]. L'usurpation d'identité consiste à s'emparer de l'identité (n'importe laquelle des identités citées précédemment) de quelqu'un sans son consentement. Elle peut se traduire par plusieurs modes d'action : le vol d'un mot de passe, d'un nom de compte informatique, d'un pseudonyme ou d'un adresse email[714]. Ce vol d'informations permet ensuite de pouvoir effectuer des transactions financières, recevoir des allocations ou encore créer des contenus diffamatoires contre la personne dont on s'est emparé de l'identité ou des tiers.

---

[708] C. FÉRAL-SCHUHL, *Cyberdroit - Le droit à l'épreuve de l'Internet 2020-2021*, 02/2020, 8è édition, p. 1545.
[709] La diffusion de la vidéo constitue une infraction autonome. Une exception est faire pour les personnes dont la profession est d'informer le public ou lorsque la vidéo est utilisée comme élément de preuve auprès de la justice.
[710] M. ACQUAVIVA, *Se riprendo un reato commetto reato?*, 28 juin 2018. Disponible sur : https://www.laleggepertutti.it/216485_se-riprendo-un-reato-commetto-reato
[711] F. GEORGES, « Identités virtuelles : Les profils utilisateur du web 2.0 », *Questions théoriques*, 2010, pp.208. Disponible sur : https://halshs.archives-ouvertes.fr/halshs-00948281/document
[712] *Ibid.*
[713] *Ibid.* Pour approfondir le sujet de l'identité numérique, voir également : J. EYNARD (dir), *L'identité numérique*, 1e édition, Bruxelles, Larcier, 2020.
[714] Par exemple l'hameçonnage (en anglais « phishing ») qui se concrétise par l'envoi d'un courrier électronique qui permet de saisir les données de la victime par le renvoi à un site Internet fictif ou à la demande, en apparence licite, de données personnelles.

B. Les atteintes sexistes et sexuelles

329. Concernant les atteintes sexistes et sexuelles, plusieurs comportement illicites ont été identifiés. D'abord, il faut rappeler que les messages malveillants et les commentaires haineux peuvent avoir comme fondement une discrimination basée sur le sexe ou l'identité de genre de la victime. De plus, des infractions très répandues sont celles du partage non consenti de contenus à caractère sexuel (photos ou vidéos) et du voyeurisme digital, qu'on a analysé dans les développements précédents[715]. Ensuite, d'autres infractions sexuelles et sexistes ont pu se développer en ligne.

330. **Le « slut shaming » -** Le « slut shaming » désigne le fait de considérer une femme ou une fille comme une « salope ». Cela se concrétise par des images dégradantes, des vidéos ou des commentaires dégradants sur les réseaux sociaux, forums et blogs.

331. **Le « sextage » abusif** - Le « sextage » est l'échange consensuel d'écrits, images, vidéos ou d'autres contenus à caractère sexuel. Il devient abusif quand ces contenus sont partagés sans le consentement de l'une des personnes. Par exemple, lors du « cyber-flashing » (« cyber exhibitionnisme » en français) qui consiste à envoyer des photos à caractère sexuel sans le consentement de la victime, notamment de photos de parties intimes. Ces images sont envoyées à travers Airdrop[716] ou Bluetooth, mais peuvent également être transmises par les messageries téléphoniques classiques ou les réseaux sociaux.

332. **Le partage non consensuel d'images à caractère sexuel** - Il s'agit de contenus à caractère sexuel réalisés avec (ou sans) le consentement de la personne qui en fait l'objet mais qui sont ensuite partagés sans son consentement[717].

333. **Le voyeurisme digital -** Le voyeurisme digital peut être une forme de partage de contenus à caractère sexuel sans le consentement. Il s'agit du fait de regarder les parties

[715] Voir chapitre III de cette thèse.
[716] Fonctionnalité sur les appareils Apple qui permet de transmettre des fichiers (photographies, vidéos, articles, notes) à travers le Bluetooth ou le Wi-Fi d'un dispositif Apple (téléphone, ordinateur, tablette) à un autre.
[717] Pour plus d'information, voir le Chapitre III de cette thèse, §§ 180-181.

intimes d'une personne sans son consentement, de les prendre en photo ou en vidéo et de les partager en ligne[718].

334. Le recrutement à des fins d'exploitation sexuelle - Il faut également mentionner le recrutement d'individus à des fins d'exploitation sexuelle qui touche majoritairement des femmes et des filles (96 %[719]). Comme analysé dans les développements précédents, le recrutement à des fins d'exploitation sexuelle est puni par le droit européen ainsi que par le droit international. Les instruments qui encadrent ces types de comportements illicites ne prévoient pas expressément la dimension « cyber ». Toutefois, grâce à leur interprétation par les cours européennes ces types de comportements sont sanctionnés lorsqu'ils ont lieu en ligne. Par exemple, la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains[720] prévoit des modes de recrutement mais pas les moyens d'actions. C'est le rapport explicatif de la Convention qui indique que la « définition de la traite des êtres humains contenue dans la Convention trouve aussi à s'appliquer lorsque la traite est pratiquée via l'utilisation des nouvelles technologies de l'information »[721].

Concernant les mineurs, l'article 19 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels distingue plusieurs formes de recrutement : le fait de recruter un enfant[722] pour qu'il se livre à la prostitution ou de favoriser la participation d'un enfant à la prostitution, le fait de contraindre un enfant à se livrer à la prostitution ou d'en tirer profit. Ainsi que, le fait d'exploiter un enfant de toute autre manière à de telles fins et d'avoir recours à la prostitution d'un enfant. L'exploitation peut aussi être caractérisée par la pornographie, enfantine[723] ou pas. Par

---

[718] Pour plus d'information, voir le Chapitre III de cette thèse, §§ 182-185.
[719] Commission européenne (Migration and home affairs), *Study on the gender dimension of trafficking in human beings*, Final report, 2016. Disponible sur : https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf, p.163
[720] Conseil de l'Europe, *Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains,* 16 mai 2005.
[721] Conseil de l'Europe, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, 16 mai 2005, point 79. Disponible sur : https://rm.coe.int/16800d388d
[722] Qui n'a pas atteint l'âge légal pour entretenir des activités sexuelles selon la législation nationale en vigueur.
[723] Article 20 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.

la production, l'offre, la mise à disposition et la diffusion et transmission de la pornographie.

La traite d'êtres humains à des fins sexuelles a pu se développer sur Internet, les réseaux sociaux et d'autres sites en apparence inoffensifs. La Commission européenne constate, dans un rapport de 2016[724], que le trafic est un crime commis pour la plupart du temps hors ligne mais la portée et l'ampleur sont facilitées et étendues par Internet. L'acte même d'exploitation (violence sexuelle mais aussi torture ou barbarie), non seulement celui de recrutement, a également lieu de plus en plus en ligne. En effet, comme on l'a expliqué précédemment, il s'agit désormais d'avoir accès à de véritables viols à distance perpétrés sur des victimes qui se trouvent, le plus souvent, à de milliers de kilomètres de mandataires qui paient une dizaine d'euros. Ces derniers n'ont pas de contact physique avec la victime, ils ne sont pas à l'origine de la pénétration sexuelle, mais ils donnent ordre à une personne de le faire, très souvent avec des instructions sur les modalités de l'agression, ou ils ordonnent à la victime de s'auto pénétrer.

Il est intéressant de parler plus spécifiquement du recrutement de mineurs et, en particulier, de la sollicitation à des fins sexuelles ou « grooming »[725]. Pour rappel, le grooming est défini par la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels comme « le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant […] dans le but de commettre à son encontre une infraction [à caractère sexuel] »[726]. Il s'agit très souvent d'adultes qui se font passer par des jeunes sur les réseaux sociaux ou plateformes de jeux en ligne[727] et rentrent en contact avec des mineurs. Cela, afin d'obtenir des photos à caractère sexuel, des

[724] Commission européenne (Migration and home affairs), *Study on the gender dimension of trafficking in human beings*, Final report, 2016. Disponible sur : https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf
[725] Voir §§199-209 de cette thèse.
[726] Article 23 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.
[727] C. D'ANASTASIO, *Children Stream on Twitch—Where Potential Predators Find Them*, WIRED, 2020. Disponible sur : https://www.wired.com/story/children-stream-twitch-potential-predators-exploitation/?fbclid=IwAR3pMIBkkEe9GZbS5p4cBR7r1rQBt-t_mWUfs5PYkCrmU98CRY12EWbkR2o

échanges par webcam ou encore des rencontres physiques pour avoir des rapports sexuels.

Concernant les mineurs, il y a également d'autres comportements illicites, outre l'exploitation sexuelle et le recrutement, qui entrent dans la définition des cyberviolences comme la production de la pornographie enfantine sur Internet ainsi que sa mise à disposition, diffusion et possession. Ces infractions sont listées clairement dans l'article 9 de la Convention du Conseil de l'Europe sur la cybercriminalité :

> « 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit :
>
> a) la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique ;
> b) l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique ;
> c) la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;
> d) le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;
> e) la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. »[728].

Ainsi, la Convention clarifie au même article le terme de « pornographie enfantine » qui « comprend toute matière pornographique représentant de manière visuelle :

> a) un mineur se livrant à un comportement sexuellement explicite ;
> b) une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;

[728] Article 9 Convention du Conseil de l'Europe sur la cybercriminalité.

c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite. »[729].

Enfin, la crise sanitaire liée à l'épidémie de Covid-19 a également fait apparaître de nouvelles formes d'atteintes en ligne, c'est le cas du « Zoom Bombing » du nom de la plateforme d'appel en vidéoconférence Zoom. En effet, INTERPOL, dans un rapport publié le 7 septembre 2020[730], a indiqué que certains États ont fait état de cas isolés de « Zoom bombing », c'est-à-dire d'intrusions par des inconnus dans des cours virtuels d'enfants pour diffuser des contenus pédosexuels.

C. Les comportements illicites à caractère répété et en meute

335. Il est nécessaire de différencier les comportements illicites à caractère répété et en meute. Il s'agit, d'un côté, du cyberharcèlement caractérisé par la répétition de toute sorte d'infraction. Certains chercheurs utilisent également le terme « cyberagression »[731]. Par exemple, l'envoi répété de messages malveillants ou dégradants, les commentaires répétés incitant au viol, au meurtre ou au suicide. On peut également parler du « cyberstalking » (cybertraque), c'est-à-dire des actes qui caractérisent traditionnellement la traque[732] mais qui s'exercent par les nouvelles technologies : par mail, Internet ou d'autres outils de communication[733]. Pour certains auteurs[734], il s'agit d'une simple transposition en ligne du stalking traditionnel. Pour d'autres, les nouvelles technologies conduisent à des nouvelles formes de comportements déviants[735]. À cet égard, douze États européens ont une législation spécifique sur le stalking[736]. L'Union

---

[729] *Ibid.*
[730] INTERPOL, *Covid19 - les menaces et les tendances en matière d'exploitation sexuelle des enfants et d'abus pédosexuels*, 7 septembre 2020, p. 12. Disponible sur : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Un-rapport-d-INTERPOL-met-en-evidence-l-incidence-du-COVID-19-sur-les-abus-pedosexuels?fbclid=IwAR3lSK5Kx-WQ9P5yD6nNijhtLUzu-0armVTRFTKQQjQ9v3jI7InFhLT6xZ8
[731] C. BLAYA, « Le cyberharcèlement chez les jeunes », *Enfance*, 2018/3, n° 3, p. 423.
[732] EIGE, *Cyberviolence à l'égard des femmes et des filles*, 23 juin 2017, pp. 1 et 2. Disponible sur : https://eige.europa.eu/publications/cyber-violence-against-women-and-girls.
[733] S. SUMMERS, C. SCHWARZENEGGER, G. EGE, F. YOUNG, *The Emergence of EU Criminal Law. Cyber Crime and the Regulation of the Information Society*, Oxford: Hart Publishing, 2014, p. 207.
[734] Voir par exemple : A. W., BURGESS, T. BAKER, *Cyberstalking*, J.C.W. Boon & L, 2002.
[735] Voir par exemple : THOMAS and LOADER (2002) cités par P. BOCIJ, « Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet », *First monday*, 2003, p. 3.
[736] Notamment l'Autriche, la Belgique, l'Allemagne, l'Irlande, les Pays Bas, l'Italie, le Luxembourg, la Hongrie et la République Tchèque.

européenne ne prévoit pas de mesures spécifiques, toutefois d'autres réglementations plus génériques sur le droit à la vie privée peuvent être utilisés pour le réprimer.

336. Enfin, de l'autre côté, des infractions sont perpétrées au même moment par plusieurs personnes. Il s'agit du « raid numérique » ou harcèlement en meute. Cela se manifeste, par exemple, par l'envoi en groupe des messages malveillants à une même cible[737].

Section II : Les avantages de l'adoption des règles minimales

337. Précédemment nous avons analysé les conséquences du pluralisme juridique menant à une protection plus faible des droits fondamentaux des utilisateurs[738]. Dans les développements qui vont suivre, il s'agira de confronter aux conséquences négatives précédemment exposées, les avantages que l'adoption des règles minimales pourrait entrainer pour les ressortissants des États membres qui ratifieront les dispositions proposées.

338. En premier lieu, il s'agira d'analyser les effets de l'harmonisation des législations nationales sur l'identification et la qualification des contenus illicites en ligne (**§I**). En second lieu, nous étudierons les conséquences que cette harmonisation pourrait entrainer sur la protection des droits fondamentaux en ligne (**§II**).

I. L'assurance d'une identification et qualification adaptée et harmonieuse

339. Le pluralisme a amené à une absence des données fiables sur les cyberviolences. Or, l'adoption des règles minimales et, par conséquent, l'harmonisation des définitions et de l'encadrement des violences en ligne permettrait une meilleure récolte et exploitation des données (**A**). Les règles minimales permettraient une meilleure protection de tous les

[737] Le droit français, la loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes punit une personne qui a envoyé un seul message en participant, même sans le savoir, à un raid numérique. En effet l'article 222-33-2-2 du Code pénal dispose que « lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée ».
[738] Voir §§257-263 de cette thèse.

ressortissants des États les ayant adoptées, en particulier, ceux qui résident dans des États qui ne prévoient pas des mesures *ad hoc* pour les infractions en ligne (**B**).

A. Une meilleure récolte et exploitation des données sur les cyberviolences

340. Comme pour les violences hors ligne - physiques, sexuelles, psychologiques, économiques - la récolte des données est essentielle pour mesurer leur ampleur ainsi qu'évaluer l'efficacité des mesures mises en œuvre pour les contrer.

341. Aujourd'hui, il n'y a pas officiellement une obligation de récolter de données au niveau européen et international sur les cyberviolences. Cela est prévu, au contraire, dans la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique [739] et dans la directive 2012/29/UE du Parlement européen et du Conseil, du 25 octobre 2012, établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité[740]. Ces textes prévoient de collecter des données statistiques désagrégées par genre. De plus, l'article 14 de la directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information, prévoit la mise en place d'un système d'enregistrement, de production et de communication des infractions définies par la directive[741]. Et, en particulier, la mise en place de statistiques sur les données existantes sur les infractions informatiques et le nombre des personnes condamnées pour ces types d'infraction. Dans le préambule de la directive, il est souligné que ce recueil de données est utile « afin d'avoir une vision plus complète du problème de la cybercriminalité et du niveau de sécurité des réseaux et de l'information au niveau de l'Union et de permettre ainsi de formuler une réponse plus efficace »[742]. Ce constat

[739] Voir article 11 de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique.
[740] Voir l'article 28 de la directive 2012/29/UE du Parlement européen et du Conseil, du 25 octobre 2012, établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil.
[741] Voir les articles de 3 à 7 de la directive 2013/40/UE du Parlement Européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.
[742] Voir la directive 2013/40/UE du Parlement Européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, point 24.

peut être transposé aux violences en ligne de contenu. En effet, à travers la récolte de données le phénomène pourrait être mieux appréhendé.

342. Pour cela, une nouvelle directive, un nouveau protocole additionnel ou une convention devraient prévoir une obligation de récolte des données basées sur les définitions des cyberviolences énoncées précédemment. Il sera certainement plus facile de récolter les données fiables si les définitions des États membres ne diffèrent pas.

343. Toutefois, la récolte des données ne serait pas le seul avantage à tirer de l'adoption des règles minimales. Cela permettrait également d'aller vers un pluralisme ordonné du droit et vers une protection accrue des droits des individus. En effet, les règles minimales pourraient permettre un traitement équitable des victimes et des agresseurs au sein de l'Union européenne.

B. Une meilleure protection des droits fondamentaux pour tous les ressortissants

344. La fixation des règles minimales permettrait d'éviter une différence des définitions et d'encadrement. Dans les développements précédents nous avons analysé la différence de définitions et de sanctions au niveau national de certains comportements illicites sur Internet comme le voyeurisme, le cyberharcèlement ou encore le partage non consensuel de contenus à caractère sexuel sur Internet. Ainsi, nous avons analysé comment le pluralisme pouvait entrainer des conséquences négatives pour la protection des utilisateurs. En particulier, sur le traitement des victimes, lorsqu'aucune disposition nationale prévoit une sanction pour les atteintes subies sur Internet.

345. Avoir des règles minimales permettrait, comme cela a été le cas pour les atteintes sexuelles à l'encontre des mineurs qui ont été, à plusieurs reprises, encadrées par les directives européennes et les Conventions du Conseil de l'Europe[743], de créer un standard

[743] Voir notamment la directive 2011/92/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels ou la Convention du Conseil de l'Europe sur la cybercriminalité.

minimum en droit interne pour mieux protéger les victimes et sanctionner les agresseurs. Ces règles minimales pourraient donc assurer l'égalité de traitement entre les demandeurs de l'Union européenne qui s'estiment victimes d'atteintes sur Internet. En effet, cet encadrement permettrait de protéger les ressortissants des États membres dont les législations ne contiennent pas de dispositions protectrices contre les violences en ligne. À titre d'exemple, ces règles permettraient de pallier le manque de disposition existant en Hongrie et la Roumanie qui ne détiennent pas des dispositions qui protègent les individus de la diffusion non consensuelle des contenus à caractère sexuel sur Internet.

346. Ainsi, avoir des règles minimales permettrait de garantir une certaine sécurité juridique en tant que principe général du droit de l'Union européenne. Ce dernier « exige qu'une réglementation de l'Union permette aux intéressés de connaître avec exactitude l'étendue des obligations qu'elle leur impose et que ces derniers puissent connaître sans ambiguïté leurs droits et leurs obligations et prendre leurs dispositions en conséquence »[744]. Or, fixer des règles minimales au niveau de l'Union européenne garantirait une meilleure lisibilité des droits et des obligations en ligne des utilisateurs, en particulier au vu de la diversité d'encadrement des comportements illicites dans les États membres.

347. Enfin, il pourrait aussi être évoqué que l'adoption de ces règles minimales et, par conséquent, des sanctions pourraient avoir une fonction « expressive ou dénonciatrice »[745]. Ainsi, des dispositions définissant et sanctionnant plus précisément les cyberviolences pourraient souligner la gravité de la commission de ces actes illicites et des conséquences provoquées. Mais également, cela permettrait de stimuler un changement culturel et social parmi les utilisateurs d'Internet et la population en général. Ces nouvelles dispositions pourraient affecter les normes sociales et les faire évoluer

[744] Voir CJUE, 29 mars 2011, *Arcelor Mittal Luxembourg c. Commission* et *Commission c. Arcelor Mittal Luxembourg e.a.*, C-201/09 P et C-216/09, point 68, voir aussi CJUE, 10 mars 2009, *Heinrich*, C-345/06, point 44.
[745] Voir dans ce sens, concernant l'adoption des mesures contre le revenge porn, G. M CALETTI, « « Revenge porn » e tutela penale, Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane », *Diritto penale contemporaneo*, Rivista trimestrale, 3/2018, p. 87.

dans la bonne direction[746]. En effet, comme le souligne G. M. Caletti, et au vu de l'apparition récente de nouveaux moyens de communication, les auteurs de contenus illicites ne se rendent pas toujours compte que leurs actes sont réprimés par la loi. Les autorités elles-mêmes, comme les agents de police, ne sont pas tous formés aux infractions en ligne et, certains d'entre eux, sont encore peu réceptifs au dépôt de plainte pour certaines violences en ligne[747].

II. L'amélioration de l'action des États dans la protection des droits fondamentaux

348. Après avoir analysé les avantages de l'adoption des règles minimales vis-à-vis des individus, il s'agira de se concentrer sur les conséquences positives pour les États membres qui adopteraient ces nouveaux textes.

349. D'un côté, les États pourraient assurer un meilleur respect des obligations internationales qu'ils ont ratifié en matière de droits fondamentaux. En effet, si ces obligations concernent des infractions traditionnelles, il serait nécessaire de prévoir le même niveau de protection pour les atteintes en ligne (**A**). De l'autre côté, l'adoption de ces nouveaux instruments juridiques, pourrait faciliter la coopération interétatique, comme cela a été le cas après l'adoption de la Convention du Conseil de l'Europe sur la cybercriminalité (**B**).

---

[746] Voir la position de C. R. SUNSTEIN sur la fonction expressive de la loi, C. R. SUNSTEIN, « Social Norms and Social Roles », *Columbia Law Review*, vol. 96, no. 4, Columbia Law Review Association, Inc., 1996, pp. 965.

[747] Voir G. M CALETTI, « « Revenge porn » e tutela penale, Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane », *Diritto penale contemporaneo*, Rivista trimestrale, 3/2018, p. 87. CALETTI expose l'exemple de policiers australiens et anglais (voir la note 145 dans son article). Cependant, cette mauvaise connaissance des violences en ligne et surtout de la possibilité de les sanctionner est présente également parmi les policiers français. Certaines victimes ont témoigné du refus par les forces de l'ordre d'accepter une plainte pour cyberviolence. À cet égard, voir la série de documentaires *Revenge* sur France TV. Disponible sur : bit.ly/RvengeTV. La jurisprudence de la Cour européenne des droits de l'Homme a pu également donner un exemple de cette méconnaissance à travers l'affaire *Buturuga c. Roumanie* précédemment citée. Pour rappel, les agents de police avaient refusé d'analyser la demande de la plaignante concernant l'atteinte au secret de correspondances et plus particulièrement aux informations et échanges personnels sur Facebook.

A. Un meilleur respect par les États des leurs obligations positives contre les atteintes aux droits fondamentaux

350. En s'engagent pour l'harmonisation des législations sanctionnant les comportements illicites en ligne, les États réaffirment leur engagement vis-à-vis des leurs obligations internationales en matière de droits humains, c'est-à-dire la nécessité de respecter, protéger et mettre en œuvre (**1**). Ensuite, ils s'engageraient à respecter ce qu'on pourrait appeler une « due diligence du cyberespace » qui les oblige à protéger les droits fondamentaux en ligne et, en particulier, à prendre des mesures contre les contenus illicites outre que la pédopornographie ou le terrorisme (**2**).

1. Les obligations internationales des États : respecter, protéger et mettre en œuvre

351. En ratifiant des traités internationaux les États s'engagent à respecter certains devoirs et obligations. Le droit international des droits humains prévoit que les États ont une obligation de respecter, protéger et mettre en œuvre (« *respect, protect and fullfil* »)[748] les droits humains. Ces obligations valent également pour le cyberespace[749].

352. En premier lieu, les États ont l'obligation de *respecter* les droits humains des utilisateurs d'Internet. David Kaye, *rapporteur* spécial des *Nations unies* sur la liberté d'expression entre 2014 et 2020, précisait, dans son rapport sur la promotion et la protection du droit à la liberté d'opinion et d'expression, du 22 mai 2015, que « les technologies numériques actuelles donnent aux pouvoirs publics […] une capacité sans précédent d'empiéter sur le droit à la liberté d'opinion et d'expression »[750]. Cela se manifeste par l'atteinte aux données personnelles, par la censure, par la surveillance ou par les attaques aux dispositifs numériques de la société civile et des défenseurs des

[748] Voir par exemple : Observation Générale No. 31: *La nature de l'obligation juridique générale imposée aux États parties au Pacte*, adoptée le 29 mars 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, 26 mai 2004.
[749] Voir Conseil des droits de l'Homme, La promotion, la protection et l'exercice des droits de l'homme sur Internet, résolution 32/13, 18 juillet 2016, A/HRC/RES/32/13, § 1, voir également World Summit on the Information Society, Declaration of Principles, WSIS-03/GENEVA/DOC/ 4-E, 12 décembre 2003, § 1.
[750] Voir le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/29/32, 22 mai 2015, point 1.

droits humains. La résolution du 12 octobre 2009[751] du Conseil des droits de l'Homme des Nations unies invite tous les États à ne pas imposer des restrictions incompatibles avec l'article 19, paragraphe 3, du Pacte international relatif aux droits civils et politiques qui protège l'exercice du droit à la liberté d'opinion et d'expression. Le Conseil souligne la nécessité de ne pas imposer des restrictions à l'accès ou au recours des techniques d'information et de communication y compris Internet. De plus, il précise certaines catégories de discours qui ne peuvent pas subir des restrictions comme les discussions politiques, les informations sur les droits humains ou encore les activités du gouvernement et la corruption en son sein[752]. Certains droits comme celui à la liberté d'expression doivent être respectés par les États. L'action des États menant au blocage[753] et, par conséquent, à la censure de certains contenus peut porter atteinte aux droits des utilisateurs. Déjà en 2011, Franck la Rue, *rapporteur* spécial des *Nations Unies* sur la liberté d'expression entre 2008 et 2014, avait noté que la société civile et les défenseurs des droits humains étaient de plus en plus les cibles de cyber attaques[754]. Dix ans plus tard, l'actualité ne semble pas montrer une évolution positive[755].

353. En outre, après le respect du droit à la liberté d'expression et d'opinion, il est important de souligner la nécessité de respecter le droit à la vie privée. Et, en particulier, l'une de ses composantes qui est le respect du secret des correspondances. La Cour européenne des droits de l'Homme a d'ailleurs spécifié qu'une législation nationale qui

---

[751] Conseil des droits de l'Homme, Liberté d'opinion et d'expression, résolution 12/16, 12 octobre 2009, A/HRC/RES/12/16.
[752] *Ibid.* §5.
[753] Voir Conseil de l'Europe, *Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur Internet*, 2017, qui cite à p. 19 OSCE, Bureau du Représentant pour la liberté des médias, *Freedom of Expression on the Internet, Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating states*, 15 décembre 2011, voir en particulier les parties sur le blocage, : http://www.osce.org/fom/80723?download=true.
[754] Voir le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/17/27, 16 mai 2011, point 51.
[755] Voir par exemple les atteintes aux défenseurs des droits humains au Pakistan, voir Amnesty International, *Pakistan : les défenseurs des droits humains cible d'une campagne de cyberattaques*, 15 mai 2018. Disponible sur : https://www.amnesty.be/infos/actualites/article/pakistan-les-defenseurs-des-droits-humains-cible-d-une-campagne-de. Mais également en Afrique, voir notamment le cyberattaque contre un militant togolais https://www.amnesty.org/fr/latest/news/2021/10/togo-activist-targeted-with-spyware-by-notorious-hacker-group/ ou égyptiens : G. HUVELIN, *Amnesty International dénonce une campagne de phishing sophistiquée visant des défenseurs des droits de l'homme égyptiens*, Numerama, 12 mars 2019. https://www.numerama.com/cyberguerre/470836-amnesty-international-devoile-une-campagne-de-phishing-sophistiquee-visant-des-defenseurs-des-droits-de-lhomme-egyptiens.html.

prévoit des mesures de surveillance « crée, par sa simple existence, […] une menace de surveillance entravant forcement la liberté de communication entre usagers des services des postes et télécommunications et constituant par là une « ingérence d'une autorité publique » dans l'exercice du droit des requérants au respect de leur vie privée et familiale ainsi que de leur correspondance »[756].

354. Au contraire, les États ont l'obligation de restreindre l'accès à certains types d'informations et contenus, et cela résulte de leur obligation de protéger les individus de l'atteinte à certains droits fondamentaux. Pour cela, en deuxième lieu, ils ont l'obligation de *protéger et mettre en œuvre* des mesures pour respecter les obligations prises dans les traités internationaux et protéger, par conséquent, les individus. À cet égard, il s'agit notamment de prendre des mesures contre les contenus pédopornographiques pour protéger les droits des enfants, contre la haine en ligne pour protéger les individus contre les discriminations, contre la diffamation pour protéger le droit à la réputation ou encore contre les violences de genre pour protéger les femmes et les filles ainsi que les membres de la communauté LGBTQIA+[757]. De plus, les États doivent protéger les individus de l'utilisation d'Internet à des fins terroristes, en effet, comme le souligne l'Office des Nations unies contre les drogues et le crime « counterterrorism initiatives relating to Internet use may have an impact on the enjoyment of a range of human rights, including the rights to freedom of speech, freedom of association, privacy and a fair trial »[758].

355. Enfin, les États doivent assurer un recours utile aux individus qui ont subi une atteinte à leurs droits humains[759] au niveau administratif, judiciaire ou législatif.

---

[756] Voir Cour EDH, *Klass et autres c. Allemagne* du 6 septembre 1978, req. n° 5029/71, §41, ainsi que Cour EDH, *Malone c. Royaume Uni* du 2 août 1984, req. n° 8691/79, §64 et Cour EDH, *Weber et Saravia* du 29 juin 2006, req. n° 54934/00, §78.

[757] Lesbiennes, gays, bisexuels, transgenres, queers, personnes en questionnement, intersexes, asexuels, alliés et plus.

[758] UNODC, *The Use of the Internet for Terrorist Purposes*, 2012, point 33. Traduction de l'autrice : « les initiatives antiterroristes relatives à l'utilisation de l'Internet peuvent avoir un impact sur la jouissance d'une série de droits humains, y compris les droits à la liberté d'expression, à la liberté d'association, à la vie privée et à un procès équitable ».

[759] Voir G. RONA et L. AARONS, « State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace », 26 octobre 2016, *8 Journal of National Security Law and Policy*, 2016, p. 521 qui cite notamment l'article 2, paragraphe 3, a, du Pacte international relatif aux droits civils et politiques.

2. Une « due diligence du cyberespace »

356. Dans les développements qui vont suivre nous allons analyser le principe de diligence voulue (due diligence) qui s'impose aux États sur Internet. Comme on l'a vu précédemment, sauf pour la Convention du Conseil de l'Europe sur la cybercriminalité, il n'y a pas d'accords internationaux qui concernent les comportements illicites en ligne. Toutefois, plusieurs États membres de l'Union européenne, du Conseil de l'Europe et des Nations unies ont adopté des conventions internationales ou des directives européennes qui protègent leurs citoyens des infractions « traditionnelles » qui peuvent être perpétrées en ligne. C'est le cas de certains directives européennes mais également de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, ou encore de la Convention américaine relative aux droits de l'Homme qui prévoit à l'article 1, paragraphe 1, que « les États parties s'engagent à respecter les droits et libertés […] et à en garantir le libre et plein exercice à toute personne relevant de leur compétence, sans aucune distinction fondée sur la race, la couleur, le sexe, la langue, la religion, les opinions politiques ou autres, l'origine nationale ou sociale, la situation économique, la naissance ou toute autre condition sociale»[760].

357. Premièrement, il est intéressant de traiter la question de la diligence voulue parce qu'elle est souvent soulevée dans la pratique du droit international des droits humains quand une violation n'est pas en principe imputable à l'État[761]. En effet, elle peut être soulevée lorsque des actes ou des omissions sont imputables à des personnes physiques ou morales. Cela est le cas pour les cyberviolences, parce qu'elles sont perpétrées le plus souvent par des individus et, le cas échant, par les plateformes numériques.

358. Deuxièmement, elle intervient lorsqu'un droit indérogeable a été violé. La Cour européenne des droits de l'Homme a pu s'exprimer à cet égard à travers sa jurisprudence

---

[760] Article 1, paragraphe 1, de la Convention américaine relative aux droits de l'Homme
[761] H. RASPAIL, « Due Diligence et droits de l'homme », in S. CASSELLA (dir.), *Le standard de due diligence et la responsabilité internationale*, SFDI, Pedone, 2018, p. 111.

et notamment l'affaire *Opuz c. Turquie* dans laquelle la Cour a estimé que « le manquement – même involontaire – des États à leur obligation de protéger les femmes contre la violence domestique s'analyse en une violation du droit de celles-ci à une égale protection de la loi »[762]. Avec l'arrêt *Buturuga c. Roumanie*, la Cour a établi que les cyberviolences font partie des violences conjugales. Pour cela, il semble possible que les États aient une obligation de due diligence vis-à-vis des victimes d'atteintes sur Internet.

359. Enfin, il est intéressant d'aborder la notion de vulnérabilité à travers le prisme de la prévisibilité. L'État ne peut pas prévenir toutes les atteintes et pour cela la Cour européenne des droits de l'Homme a établi clairement qu'il « faut interpréter l'étendue de l'obligation positive de manière à ne pas imposer aux autorités un fardeau insupportable ou excessif »[763]. Toutefois, comme le souligne H. Raspail, « la prévisibilité des atteintes aux droits fondamentaux […] doit conduire l'État à adopter un comportement particulièrement diligent »[764] afin de « permettre une protection efficace, notamment des enfants et autres personnes vulnérables, et inclure des mesures raisonnables pour empêcher des mauvais traitements dont les autorités avaient ou auraient dû avoir connaissance »[765]. Or, sont considérées comme de personnes vulnérables les femmes victimes de violence conjugales[766], les mineurs[767] ou encore les militants et journalistes politiques[768]. Ces catégories se retrouvent également très exposées aux cyberviolences. En effet, les comportements illicites en ligne se manifestent à travers un continuum de violence pour les femmes victimes de violences conjugales à travers les logiciels espions (le cybercontrôle) ou encore l'atteinte au secret des correspondances. Les mineurs sont également surexposés à plusieurs types

[762] Cour EDH, 9 septembre 2009, *Opuz c. Turquie*, req. n° 33401/02, point 191.
[763] Cour EDH, 28 mars 2000, *Kilic c. Turquie*, req. n° 22492/93, §63. Voir également H. RASPAIL, « Due Diligence et droits de l'homme », in S. CASSELLA (dir.), *Le standard de due diligence et la responsabilité internationale*, SFDI, Pedone, 2018, pp. 115-116.
[764] H. RASPAIL, « Due Diligence et droits de l'homme », in S. CASSELLA (dir.), *Le standard de due diligence et la responsabilité internationale*, SFDI, Pedone, 2018, p. 116.
[765]Cour EDH, 10 mai 2001, *Z et autre c. Royaume Uni*, req. n° 29392/95, §73. Voir également H. RASPAIL, « Due Diligence et droits de l'homme », in S. CASSELLA (dir.), *Le standard de due diligence et la responsabilité internationale*, SFDI, Pedone, 2018, p. 116.
[766] Cour EDH, 9 septembre 2009, *Opuz c. Turquie*, req. n° 33401/02.
[767] Cour EDH, 10 mai 2001, *Z et autre c. Royaume Uni*, req. n° 29392/95.
[768] Cour EDH, 28 mars 2000, *Kilic c. Turquie*, req. n° 22492/93, §68.

d'atteintes : des atteintes sexuelles comme le gooming, physiques et psycologiques comme le cyberharcèlement et le « happy slapping ». Enfin, les journalistes et les défenseurs des droits humains qui sont la cible de messages haineux, de cyberharcèlement ou encore de cybersurveillance[769].

360. Or, grâce à des règles minimales, les États pourraient mieux identifier et sanctionner les cyberviolences et, par conséquent, respecter les obligations internationales de protection des droits humains. Ce faisant ils pourraient moins s'exposer à des recours en manquement. De plus, définir des règles minimales permettrait également de faciliter la coopération entre les différents acteurs engagés dans la lutte contre les violences en ligne de contenu.

B. La facilitation de la coopération entre les acteurs européens et internationaux

361. La Convention sur la cybercriminalité met en place un régime de coopération et d'assistance mutuelle sur les infractions informatiques entre les États parties. Comme l'explique le rapport explicatif du protocole additionnel contre la xénophobie et le racisme, grâce à la Convention, l'échange d'expériences communes utiles dans le traitement des affaires a pu être renforcé et la coopération facilitée, notamment en ce qui concerne l'extradition et l'entraide judiciaire[770]. À cet égard, la Convention a démontré son utilité. En effet, depuis son adoption plusieurs avancées ont été surlignées par les États membres. En témoigne le rapport du Conseil de l'Europe sur les avantages et les impacts concrets de la Convention[771]. Selon ce rapport, même si des améliorations doivent encore être atteintes, le traité a mis en place une collaboration internationale plus efficace entre les États parties comme Malte, la Bosnie Herzégovine ou encore la France

[769] Pour les cyberviolences contre les journalistes femmes, voir notamment J. POSETTI, N. SHABBIR et autres, *The Chilling: Global trends in online violence against women journalists*, UNESCO, 2021, p 20. Disponible sur : https://unesdoc.unesco.org/ark:/48223/pf0000377223

[770] Council of Europe, *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*, 28 January 2003, point 3.

[771] Conseil de l'Europe, *La Convention de Budapest sur la cybercriminalité : avantages et impact concrets*, T-CY (2020)16, 13 juillet 2020.

et la Hongrie[772]. Les États parties ont souligné comment la Convention sur la cybercriminalité avait pu faciliter la coopération à travers l'entraide judiciaire. La France, par exemple, en 2019 seulement, a envoyé 55 demandes d'entraide judiciaire pour des données électroniques se fondant sur la Convention. Également, la Serbie a souligné qu'elle avait reçu une entraide efficace par les autorités hongroises concernant une affaire relative à de la pédopornographie.

362. Or, nous constatons que la Convention a permis d'instaurer un système de coopération efficace vis-à-vis des infractions prévues dans le traité. Il suffirait ainsi d'y ajouter les infractions de contenu, à travers un troisième protocole additionnel, pour jouir de cette collaboration plus étroite en matière de comportements illicites de contenu.

363. Dans le cadre du droit de l'Union européenne, l'adoption d'une directive pourrait elle aussi faciliter la coopération entre les États. Cela, non seulement, comme on a indiqué précédemment concernant la récolte des données, mais également pour l'échange d'informations, de preuves et des bonnes pratiques. Elle s'inscrirait dans la mise en œuvre effective de l'espace de liberté, sécurité et justice prévu à l'article 3, paragraphe 2, du traité sur l'Union européenne[773] qui prévoit un espace de prévention et de lutte contre la criminalité. La coopération en matière pénale serait ainsi plus efficace si les États membres se munissaient d'un même cadre juridique sur les infractions en ligne, comme pour la pédocriminalité[774].

---

[772] Conseil de l'Europe, *La Convention de Budapest sur la cybercriminalité : avantages et impact concrets*, T-CY (2020)16, 13 juillet 2020, pp. 14-21.
[773] Article 3, paragraphe 2, du traité sur l'Union européenne.
[774] Voir S. ADALID, M. COMBET, C. MAZILLE, M. ROCCATI, « L'Espace de liberté sécurité justice : un droit à géométrie variable ? », *RTDEur.*, 2012/4 concernant le terrorisme : « Il est toutefois évident que la coopération pénale gagnerait en efficacité si tous les États membres connaissaient, par exemple les infractions terroristes. En la matière, seize incriminations sont désormais harmonisées. Les acteurs pénaux institués, bien que perfectibles, donnent déjà une large satisfaction. C'est, par exemple, le cas d'Eurojust, qui malgré les difficultés opérationnelles qu'il connaît, a traité 27 affaires de terrorisme en 2011 et a été associé à 33 équipes communes d'enquête, dont l'utilité n'est plus à démontrer ».

Conclusion du Chapitre IV

364. Les cyberviolences, comme les violences hors ligne, sont multiformes. Face à l'absence de règles uniformes et de la multiplicité de dispositions existants, nous avons constaté que plusieurs options existent pour mettre en place des règles minimales qui permettraient de mieux identifier et qualifier les comportements illicites en ligne. Grâce à une meilleure identification, il serait plus facile d'étudier ce phénomène et de prévoir une réponse efficace et adaptée pour protéger les droits fondamentaux des utilisateurs. L'adoption de ces règles permettrait également un meilleur respect des obligations positives des États.

CONCLUSION DU TITRE II

365. **La nécessité d'une qualification universellement acceptée -** Face à l'identification et au traitement fragmentaire des cyberviolences entrainant des conséquences négatives pour le respect des droits fondamentaux des utilisateurs, nous avons proposé l'adoption d'une définition universelle et des règles minimales identifiant les comportements illicites en ligne. Conscients des réticences de certains États, surtout en dehors de l'Union européenne, nous sommes convaincus que ces solutions pourraient être adoptés en premier lieu par les États de l'Union européenne. Cette première adoption serait un premier pas pour recueillir des données plus fiables afin d'étudier le phénomène. Mais surtout, cela permettrait d'avoir une protection uniforme et respectueuse des droits fondamentaux des utilisateurs.

Conclusion de la Partie I

366. La reconnaissance nécessaire des spécificités des cyberviolences - Les cyberviolences sont un phénomène complexe. Avec l'analyse des caractéristiques d'Internet, nous avons constaté que les violences en ligne ont des spécificités propres qui les distinguent des violences hors ligne. Sur Internet les contenus partagés peuvent y rester pour toujours et les utilisateurs en perdent la maîtrise causant, lorsque ces contenus sont illicites, des conséquences importantes sur la vie des victimes.

Grâce à Internet les barrières physiques s'effacent et les utilisateurs peuvent parvenir à toucher une multiplicité des cibles. De plus, grâce aux caractéristiques techniques d'Internet, nous constatons un phénomène d'amplification qui mène à la viralité de la diffusion des contenus et, par conséquent, à l'aggravation des leurs conséquences nuisibles.

367. Le pluralisme des définitions et la nécessité d'une qualification uniforme – Aucun État ou institution a adopté des dispositions juridiques contraignants qui prévoient une définition juridique de cyberviolence. Plusieurs formes de comportements illicites en ligne sont punies par les droits nationaux mais les dispositions varient d'un État à l'autre. De plus, certains États répriment ces comportements avec les mêmes dispositions prévues pour les infractions hors ligne. Cela entraine plusieurs conséquences négatives dans la prise en compte des spécificités des cyberviolences et de leurs conséquences, dans l'évaluation du phénomène et la protection hétérogène des droits fondamentaux d'un État à l'autre. Au vu de ces éléments, il nous semble nécessaire d'adopter une définition de cyberviolence qui soit accepté par les États de l'Union européenne et au-delà et qui sera complété par une liste non exhaustive de règles minimales, protégeant ainsi les droits fondamentaux des utilisateurs.

368. Le besoin d'adapter les mesures de prévention et de sanction des cyberviolences - La définition des cyberviolences et l'établissement des règles minimales doivent s'accompagner de mesures préventives et des sanctions dissuasives. Aujourd'hui, ces dernières ne semblent pas suffire à contrer l'ampleur des comportements illicites en

ligne. Pour cela, il serait souhaitable que ces dernières prennent en compte la dimension cyber et les conséquences que les violences en ligne causent aux victimes. Il sera question dans une deuxième partie d'étudier cette affirmation à travers l'analyse du régime des violences en ligne et, en particulier, des mesures préventives et des sanctions existantes afin de formuler des pistes d'amélioration.

PARTIE II : LE REGIME FRAGMENTAIRE D'ENCADREMENT DES CYBERVIOLENCES

369. Après avoir analysé la qualification des cyberviolences à travers l'étude de leurs caractéristiques et les spécificités, nous allons examiner leur régime.

Cette étude se concentrera sur les mesures en vigueur pour la prévention de ces violences et la sanction de leurs auteurs.

370. D'un côté, la prévention est essentielle pour éviter et éradiquer un phénomène. À cet égard, la question de la sensibilisation et de l'éducation sont fondamentales pour faire évoluer les mentalités et parvenir à une utilisation respectueuse d'Internet de des plateformes. Les mesures d'éducation et de sensibilisation sont encrées aux problématiques que nous trouvons également hors ligne. En effet, il ne faut pas oublier que les comportements illicites sur Internet sont la conséquence de rapports de domination et de pensées, entre autres, racistes, sexistes et transphobes que nous retrouvons hors ligne.

De l'autre côté, la sanction a également un rôle important, en particulier en matière dissuasive. Aujourd'hui, l'encadrement des cyberviolences et, en particulier, les sanctions encourues, sont encore méconnues par les utilisateurs. Il a une réelle méconnaissance du fait que les comportements illicites hors ligne sont également punis en ligne. De plus, les sanctions prévues contre les violences en ligne ne semblent pas être assez dissuasive, au moins dans les États de l'Union européenne. Alors que, comme nous l'avons vu dans les développements précédents, ces comportements illicites ont des conséquences significatives et spécifiques sur la vie de la victime qui sont, toutefois, très rarement pris en compte par le législateur et les autorités judiciaires.

371. Au vu de ces éléments, il d'agira d'analyser les mesures diversifiées de préventions et leurs effets mitigés (**Titre I**), pour ensuite étudier l'efficacité relative des sanctions et la construction d'un cadre répressif plus adapté aux enjeux d'Internet (**Titre II**).

TITRE I : UNE PREVENTION DIVERSIFIEE AUX EFFETS MITIGES

372. Les mesures de prévention sont essentielles pour traiter le phénomène des cyberviolences. Avec le terme « mesures préventives » ou « de prévention » nous faisons référence à toutes les mesures juridiques ou non, destinées à éviter les comportements illicites en ligne y compris la récidive. Plusieurs mesures sont adoptées pour faire face aux comportements illicites en ligne et nous y retrouvons des initiatives mises en place pour les infractions hors ligne, comme l'éducation et la sensibilisation, mais également des solutions techniques qui ont fait leur apparition avec les progrès technologiques. Ces mesures sont multiples comme le sont les acteurs qui les mettent en œuvre. Les États, les entreprises privées, ainsi que la société civile jouent un rôle principal dans la prévention des infractions en ligne.

373. Aujourd'hui, les initiatives et les dispositions en vigueur ne semblent pas suffire à prévenir efficacement les comportements illicites en ligne. Les stratégies des acteurs privés, en particulier les plateformes, sont souvent pointés du doigts pour le manque de modération et d'investissements. Mais également les régimes de responsabilités de ces derniers ne semblent plus être adéquats pour permettre une régulation respectueuse des droits fondamentaux des utilisateurs.

374. Au vu de ces éléments, il s'agira d'analyser la multiplicité d'acteurs et des mesures existantes en constante évolution (**Chapitre V**) pour ensuite étudier de quelle manière il serait nécessaire d'améliorer la prévention (**Chapitre VI**).

Chapitre V : Une prévention multi acteurs et évolutive

375. Depuis plusieurs années nous assistons au développement des mesures préventives par les États, les organisations régionales et la société civile à travers l'adoption de mesures juridiques ou bien des politiques publiques qui visent à freiner les comportements illicites sur les plateformes.

376. Nous considérons ces acteurs comme « traditionnels » car historiquement ce sont eux qui, dès l'apparition d'un phénomène néfaste, se sont mobilisés pour l'endiguer (**Section I**). Nous allons également analyser les mesures adoptées par les entreprises privées, c'est-à-dire les plateformes numériques, qui sont en première ligne et à la diffusion de contenus illicites dans leurs réseaux (**Section II**).

Section I : Une prévention uniforme par les acteurs traditionnels

377. Nous analyserons l'existence de plusieurs mesures de prévention mises en place par les États, les organisations régionales ainsi que la société civile. D'un côté, des mesures d'éducation et de sensibilisation sont adoptées par les États (**§I**). De l'autre, il existe également des mesures techniques qui, toutefois, sont peu développées et très souvent controversées (**§II**).

I. L'éducation et la sensibilisation, mesures centrales de prévention des cyberviolences

378. Nous constatons que la prévention passe notamment par des actions de sensibilisation et d'éducation. Ces mesures peuvent prendre plusieurs formes, par exemple : des campagnes de sensibilisation auprès des écoles, sur la voie publique ou sur Internet, ainsi que, des formations qui peuvent être ponctuelles ou régulières auprès d'un public spécifique (entre autres : des mineurs, des agents de police ou autres fonctionnaires).

379. Dans les développements qui vont suivre, il s'agira d'analyser ces mesures qui sont très répandues (**A**) et dont efficacité est difficile à mesurer (**B**).

A. L'élaboration lente des mesures préventives

380. Les mesures préventives peuvent être prévues dans les traités internationaux ou dans d'autres instruments régionaux ou nationaux. Certaines conventions internationales mentionnent explicitement l'objet préventif alors que d'autres prévoient un ensemble d'obligations dont l'exécution devrait permettre une prévention effective[775]. C'est le cas notamment de l'article 5 de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains qui « décline une obligation générale de prévention à travers plusieurs autres obligations imposées aux États parties »[776].

La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels et la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique reposent sur le principe des « quatre P » : « prevention, protection, prosecution and partnerships »[777]. La première se fixe l'objectif de « prévenir et de combattre l'exploitation et les abus sexuels concernant des enfants »[778] et consacre un chapitre entier aux mesures préventives[779]. La seconde, prévoit une série de mesures pour prévenir les violences faites aux femmes, notamment des obligations en matière de sensibilisation, d'éducation, mais également des formations à destination de certains professionnels[780]. La prévention est donc l'un des piliers de ces conventions. Cependant, les traités ne sont pas les seuls instruments juridiques à prévoir des dispositions préventives.

---

[775] S. TOUZÉ, « La notion de prévention en droit international des droits de l'homme », in E. DECAUX et S. TOUZÉ (Dir), *La prévention des violations des droits de l'homme,* Publications de l'Institut international des droits de l'homme n°25, Pedone, 2013, pp. 19-20.

[776] *Ibid.* p. 20.

[777] En français « prévention, protection, poursuite et partenariats ». Voir Conseil de l'Europe, Instruments internationaux, disponible sur : https://www.coe.int/fr/web/cyberviolence/international-instruments Voir également E. D'URSEL, « La Convention du Conseil de l'Europe sur la prévention et la lutte contre les violences à l'égard des femmes : une révolution silencieuse ? », *Revue trimestrielle des droits de l'homme*, n° 113/2018, 2018 sur l'approche des « quatre P » adopté dans la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, pp. 33-35. E. D'Ursel utilise le terme de « politiques intégrées » plutôt que « partnerships ».

[778] Article 1, a, de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, STCE n° 201, Lanzarote, 25 octobre 2007.

[779] *Ibid.* Chapitre II.

[780] Chapitre III de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, STCE n° 210, Istanbul, 11 mai 2011.

381. En droit de l'Union européenne, il existe la directive 2013/40/UE du Parlement et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information qui vise à « faciliter la prévention » des infractions contre les systèmes d'information[781]. Une autre directive a un objet plus spécifique. Il s'agit de la directive 2011/93/UE du Parlement européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie[782]. L'article 23 de la directive dispose que :

> 1. Les États membres prennent les mesures appropriées, telles que *l'éducation et la formation*, pour décourager et réduire la demande qui favorise toutes les formes d'exploitation sexuelle des enfants.
> 2. Les États membres prennent les mesures appropriées, y compris par l'Internet, telles que des *campagnes d'information et de sensibilisation*, des programmes de recherche et d'éducation, le cas échéant en coopération avec des organisations pertinentes de la société civile et d'autres parties intéressées, afin de sensibiliser l'opinion à ce problème et de réduire le risque que des enfants ne deviennent victimes d'abus sexuels ou d'exploitation sexuelle.
> 3. Les États membres favorisent la *formation régulière* des fonctionnaires susceptibles d'entrer en contact avec des enfants victimes d'abus sexuels ou d'exploitation sexuelle, y compris les policiers de terrain, visant à leur permettre d'identifier les enfants victimes et victimes potentielles d'abus sexuels ou d'exploitation sexuelle et de les prendre en charge[783].

382. Cet exemple illustre de manière concrète les mesures qui sont majoritairement adoptées par les organisations régionales et les États ainsi que par les acteurs de la société civile. Ces dispositions se traduisent par des campagnes nationales de sensibilisation, de formation auprès des jeunes mais également des parents et du personnel enseignant, de la justice et de police.

---

[781] Article 1 directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.
[782] Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil. Italique de l'autrice.
[783] Article 23 de la directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil. Italique de l'autrice.

383. Ces mesures préventives ne sont pas, pour la plupart, spécifiques aux cyberviolences mais peuvent s'appliquer également pour prévenir les comportements illicites en ligne. Cependant, nous assistons également à l'apparition de dispositions préventives *ad hoc* pour la sphère cyber. Cela vaut pour la protection des mineurs, des femmes mais également pour la prévention d'actes terroristes et de recrutement à des fins de terrorisme.

384. Dans le prolongement des directives adoptées par l'Union européenne, le Parlement européen et du Conseil ont adopté le 19 octobre 2022 le règlement 2022/2065 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (« Digital Services Act »). Ce dernier prévoit à l'article 35 (i) bis l'adoption de mesures de sensibilisation[784] par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche.

385. Nous pouvons également mentionner certaines mesures préventives adoptées par les États. D'abord, en Italie, la loi sur le cyberharcèlement auprès des jeunes, non seulement, contient des dispositions spécifiques pour la prévention, mais fait de cette dernière le cœur de l'action contre le cyberharcèlement. Elle prévoit l'implication des services sociaux et éducatifs, en particulier les écoles[785], et le déploiement des campagnes de sensibilisation à travers les principaux médias[786]. Elle prévoit également des actions de formation du personnel des écoles en collaboration avec les forces de l'ordre et les associations[787]. Ainsi, le 13 janvier 2021 un décret a été publié pour préciser des lignes directrices pour l'application de cette loi avec l'objectif de permettre aux enseignants et opérateurs scolaires de réduire le phénomène de cyberharcèlement[788] dans leur institution. En parallèle, le ministère de l'éducation italien a lancé des campagnes pour

[784] Article 35 (i) du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[785] Article 3, paragraphe 4, Legge n° 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, del 29 maggio 2017(17G00085), GU Serie Generale n.127 del 03-06-2017.
[786] *Ibid.* article 3, paragraphe 5.
[787] *Ibid.* article 4, paragraphe 3.
[788] Voir decreto ministeriale 18 del 13 gennaio 2021 emanato con nota 482 del 18 febbraio 2021. Disponible sur : https://miur.gov.it/documents/20182/92942/NOTA+LINEE+B+E+CB++2021+.0000482.18-02-2021.pdf/0a28bfe8-459e-8cb3-8c4d-0f4e9b5ce683?version=1.0&t=1617971437453

lutter contre la cyberintimidation et a élaboré, depuis 2018, une plateforme de formation destinée aux enseignants référents en matière de (cyber)harcèlement dans les écoles pour pouvoir approfondir leur compétences psychopédagogiques et sociales à ce sujet. Le même ministère a également créé un site nommé « Generazioni Connesse »[789], co-financé par l'Union européenne, qui permet de trouver les informations utiles concernant les cyberviolences à destination des jeunes, enseignants et parents.

Ensuite, en France, le chapitre VI de la loi 2020-766, du 24 juin 2020, visant à lutter contre les contenus haineux sur Internet prévoit des dispositions sur la prévention de la diffusion de contenus haineux en ligne. La loi a, entre autres, ajouté dans le Code de l'éducation des dispositions venant préciser la dimension « cyber ». Par exemple, l'article 121-1 du Code de l'éducation indique que « les écoles, les collèges et les lycées assurent une mission d'information sur les violences, *y compris en ligne* »[790]. De plus, l'article L312-9, sur la formation à l'utilisation responsable des outils et des ressources numériques dispensé à l'école, a été complété avec des dispositions sur la lutte contre la diffusion des contenus haineux. L'article précise que « [la formation] contribue au développement de l'esprit critique, *à la lutte contre la diffusion des contenus haineux en ligne* et à l'apprentissage de la citoyenneté numérique »[791]. Ainsi, la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire prévoit qu'« une information sur les risques liés au harcèlement scolaire, notamment au cyberharcèlement, est délivrée chaque année aux élèves et parents d'élèves »[792]. Ces mesures, prévues en France et en Italie, sont seulement destinées aux plus jeunes.

386. Nous pouvons également mentionner l'action de la société civile. En France, par exemple, au-delà de l'action gouvernementale, le tissu associatif travaillant sur ces questions est très actif. Nous pouvons citer les actions de préventions organisées par l'ONG « Respect Zone », ou par la plateforme « E-enfance », « Point de contact » ainsi que l'association « Marion la main tendue ». Ces dernières sensibilisent les jeunes aux

---

[789] Voir le site Internet de la plateforme « Generazioni Connesse », disponible sur : https://www.generazioniconnesse.it/site/it/home-page/

[790] Article L121-1 du code de l'éducation. Les mots en italique, par l'autrice, indiquent l'ajout opéré par la loi 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet.

[791] *Ibid.* article L. 312-9. Les mots en italique, par l'autrice, indiquent l'ajout opéré par la loi 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet.

[792] Article 1 de la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire.

risques d'Internet et à la manière d'utiliser Internet et les réseaux sociaux. De plus, il existe d'autres associations spécialisées sur les cyberviolences sexuelles et sexistes comme le collectif « Stop Ficha », « En avant toutes » ou encore « Echap ». Enfin, nous pouvons citer les travaux du « Centre Hubertine Auclert », centre francilien pour l'égalité femmes-hommes qui travaille sur le sujet des cyberviolences, notamment conjugales, et qui organise des séances de formation et sensibilisation pour les professionnels.

387. Enfin, d'autres États, en particulier, les membres de l'Union européenne mènent des initiatives de sensibilisation contre les cyberviolences. On peut citer l'initiative « Pantallas Amigas »[793] organisée en Espagne ou encore l'initiative « Klicksafe »[794] organisée par le gouvernement allemand et co-financée par l'Union européenne. Des campagnes de sensibilisation sont également organisées par l'Union européenne. Par exemple, en 2017 la campagne « NON.NO.NEIN »[795] a été lancée contre les violences faites aux femmes, dont les cyberviolences. Il existe également la « Strategy for a Better Internet for Children »[796] (en francias : stratégie pour un meilleur internet pour les enfants), qui propose une série d'actions menées conjointement par la Commission européenne et par les États membres. L'Union européenne finance également des projets de prévention comme « SELMA Hacking Hate »[797] programme de deux ans mis en place par des acteurs venant de cinq États européens (Belgique, Danemark, Allemagne, Grèce et Royaume-Uni) et qui s'appuie sur une approche d'apprentissage social et émotionnel auprès des 11-16 ans pour s'attaquer au problème du discours de haine en ligne.

388. Ces mesures, ainsi que d'autres qui n'ont pas été mentionnées[798], montrent que le sujet de la prévention est un point important pour la lutte contre les violences en ligne et,

---

[793] Plus d'informations sur la campagne « Pantallas Amigas », voir : https://www.pantallasamigas.net/quienes-somos/
[794] Pour plus d'informations sur la campagne « Klicksafe », voir : https://www.klicksafe.de/
[795] Pour plus d'informations sur la campagne « NON.NO.NEIN » : https://ec.europa.eu/justice/saynostopvaw/#prettyPhoto
[796] Pour plus d'informations sur la stratégie « Better Internet for Kids », voir : https://www.betterInternetforkids.eu/en-GB/policy/better-Internet
[797] Pour plus d'information sur le projet « SELMA Hacking Hate » : https://hackinghate.eu/about/
[798] Pour approfondir voir : A. VAN DER WILK, *Cyber violence and hate speech online against women*, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament September 2018, pp. 59-62 ;

cela, au niveau international, régional et national. Toutefois, il est nécessaire d'analyser l'efficacité de ces mesures, ce qui est nécessairement compliqué compte tenu de l'absence d'études en la matière.

B. L'efficacité relative des mesures d'éducation et sensibilisation

389. Certains auteurs se sont penchés sur l'analyse des mesures de prévention contre les cyberviolences et plus particulièrement contre le cyberharcèlement entre jeunes en milieu scolaire. Nous constatons que les analyses à cet égard sont très peu nombreuses. Les études que nous allons analyser se concentrent sur les effets des programmes de sensibilisation, en particulier, sur la baisse des comportements violents en ligne et de la victimisation[799]. Nous pouvons mentionner l'analyse de Catherine Blaya, professeure en sciences de l'éducation qui est une référence pour les questions de cyberviolences à l'école. Elle a mené en 2015 une analyse sur l'efficacité des programmes d'interventions contre la cyberviolence et le cyberharcèlement auprès des jeunes[800]. Dans cette étude on y retrouve l'évaluation de l'efficacité des programmes en Amérique du nord[801], en Angleterre et dans les États non anglophones de l'Europe. Concernant l'Angleterre, aucun programme ne donne des résultats significatifs sur la baisse des comportements violents et de la victimisation. Des résultats intéressants se trouvent principalement dans quatre des dix programmes évalués, et, en particulier, dans un projet en Amérique du nord et trois programmes en Europe (en Allemagne, en Italie et en Espagne). Ces quatre derniers présentent des caractéristiques communes : premièrement, le fait de s'intéresser aux développements des compétences sociales comme l'empathie ou l'estime de soi des bénéficiaires. Deuxièmement, ils sont tous inclus dans des programmes scolaires de façon formelle, et, troisièmement, ils impliquent les élèves de manière active[802]. Les

---

ainsi que, Conseil de l'Europe, Comité de la Convention sur la cybercriminalité, *Étude cartographique sur la cyberviolence*, 2018, pp. 28-32.

[799] Le fait d'être considéré ou de se considérer une victime.

[800] C. BLAYA, « Les programmes d'intervention contre la cyberviolence et le cyberharcèlement : quels moyens, quelle efficacité ? », *Les dossiers des sciences de l'éducation*, 33, 2015, 131-153.

[801] Blaya choisit des programmes analysés dans une autre étude : F. MISHNA, C. COOK, M. SAINI, M.-J. WU, R. McFADDEN, « Interventions for children, youth, and parents to prevent and reduce cyber abuse », *Campbell Systematic Reviews*, 2009.

[802] C. BLAYA, « Les programmes d'intervention contre la cyberviolence et le cyberharcèlement : quels moyens, quelle efficacité ? », *Les dossiers des sciences de l'éducation*, 33, 2015, point 47.

effets constatés se manifestent principalement par une connaissance plus étendue du phénomène des cyberviolences. Cependant, il n'y a pas d'effet sur les changements de comportement des bénéficiaires[803]. Sauf quelques exceptions, par exemple le programme espagnol « ConRed » qui contribuerait à la diminution des comportements agressifs sur Internet[804] ou le programme italien « Noncadiamointrappola! » qui montre une augmentation significative des stratégies d'évitement des situations de violence et de résolution de conflits[805].

390. L'étude de Blaya pointe du doigt également l'absence d'évaluations scientifiques sur l'efficacité de l'intervention et de la prévention[806] et cela est constaté également par un autre groupe de chercheurs qui ont analysé l'efficacité des stratégies de prévention contre le cyberharcèlement auprès des jeunes[807]. Il s'agit d'une étude publiée par des chercheurs de l'Université de Cambridge et de Floride[808]. Ces derniers ont analysé l'efficacité des programmes d'intervention et de prévention du cyberharcèlement (« cyberbullying »), à travers une revue systématique et méta-analytique d'études publiées et non publiées entre les années 2000 et 2017 sur les programmes d'intervention et de prévention. Leur analyse montre que les programmes d'intervention en matière de cyberharcèlement étaient efficaces pour réduire la perpétration des cyberviolences[809], ainsi que la victimisation[810]. L'étude se conclut en montrant que les programmes d'intervention et de prévention étudiés sont efficaces mais, comme dans l'analyse de Blaya, il a été souligné qu'il serait nécessaire de mener des recherches supplémentaires pour mieux comprendre les raisons

[803] *Ibid*. point 49. Voir également : F. MISHNA, C. COOK, M. SAINI, M.-J. WU, R. McFADDEN, « Interventions for children, youth, and parents to prevent and reduce cyber abuse », *Campbell Systematic Reviews*, 2009, p. 8.
[804] *Ibid*. point 41.
[805] *Ibid*. point 46.
[806] Voir l'un de rares études sur la matière : F. MISHNA, C. COOK, M. SAINI, M.-J. WU, R. McFADDEN, « Interventions for children, youth, and parents to prevent and reduce cyber abuse », *Campbell Systematic Reviews*, 2009, ainsi que F. MISHNA, C. COOK, M. SAINI, M.-J. WU, R. McFADDEN, « Interventions to prevent and reduce cyber abuse of youth: A systematic review », *Research on Social Work Practice*, 21(1), 5–14, 2010.
[807] Voir également : H. GAFFNEY, « Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review », *Aggression and Violent Behavior*, 2018, p. 13.
[808] H. GAFFNEY, « Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review », *Aggression and Violent Behavior*, 2018.
[809] *Ibid.* pp. 7 et 12 point 4.1.
[810] *Ibid.* p. 12 point 4.2.

de la variation de l'efficacité[811]. L'efficacité des programmes est soulignée pour certains aspects, notamment la victimisation ou la baisse de comportements violents. Toutefois, cela n'est pas le cas pour le changement de comportements des jeunes. Par exemple, ils continuent de visiter des sites inappropriés ou de communiquer leurs informations personnelles en ligne sans prendre des précautions[812].

391. Pour cela, il serait nécessaire de conduire des études analytiques[813] supplémentaires, mais également de ne pas se restreindre à l'analyse des bienfaits sur les jeunes et comprendre si certaines campagnes de prévention grand public ont des effets sur les adultes ou si des campagnes auprès des jeunes ont des effets sur les parents et leur utilisation d'Internet. En effet, le phénomène des cyberviolences n'intéresse pas seulement les mineurs, bien au contraire il concerne tous les utilisateurs peu importe leur âge.

392. Après avoir analysé des formes de prévention qu'on pourrait définir comme « traditionnelles », il convient d'étudier d'autres techniques de prévention mises en place par les États.

II. L'élaboration controversée des mesures techniques préventives

393. D'abord, nous constaterons l'absence des lois techniques préventives, c'est-à-dire des lois qui prévoient le retrait préventif de certains contenus (**A**). Ensuite, nous verrons qu'il existe des dispositifs capables de retirer des contenus avant leur publication dont l'usage est controversé (**B**).

---

[811] *Ibid.* p. 16 point 5.3.
[812] Voir par exemple : F. MISHNA, C. COOK, M. SAINI, M.-J. WU, R. McFADDEN, « Interventions for children, youth, and parents to prevent and reduce cyber abuse », *Campbell Systematic Reviews*, 2009, p. 8.
[813] Blaya conseille de mener ces études à travers « une approche méthodologique mixte en termes d'évaluation, car connaître le sens que donnent les acteurs aux actions mises en œuvre ainsi que le contexte et les conditions de mise en œuvre documenterait de façon pertinente les conditions de l'efficacité ». Ainsi, elle souligne l'absence d'information sur le rapport coût/mise en œuvre et efficacité de l'intervention qui est souvent un des freins principaux de l'action. Il serait donc souhaitable d'intégrer ces données également. Voir C. BLAYA, « Les programmes d'intervention contre la cyberviolence et le cyberharcèlement : quels moyens, quelle efficacité ? », *Les dossiers des sciences de l'éducation*, 33, 2015, point 49.

A. L'absence des lois techniques préventives contre les contenus illicites

394. Il est intéressant d'analyser si des lois préventives existent et notamment des lois contenant des mesures techniques de prévention. Aucune loi technique préventive est inscrite, à ce jour, dans les législations nationales étudiées, sauf une qui s'éloigne du sujet des cyberviolences mais qui est intéressante à analyser. Il s'agit des lois contre l'exposition des mineurs aux contenus pornographiques. En effet, plusieurs États de l'Union européenne ont prévu des dispositions juridiques pour obliger les sites pornographiques à contrôler l'âge des internautes qui les visitent.

395. En France, depuis l'adoption de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales[814], il est imposé aux sites pornographiques de mettre en place un contrôle de l'âge. La mise en œuvre de cette mesure est contrôlée par le Conseil supérieur de l'audiovisuel (CSA)[815] qui peut saisir la justice en cas de manquement à ce contrôle afin de bloquer le site fautif. Cependant, l'application de cette obligation est, dans les faits, assez difficile à cause des atteintes qu'un tel contrôle pourrait porter aux individus qui visitent ces sites. Cela a été également souligné par la Commission nationale de l'informatique et des libertés dans l'avis du 3 juin 2021 sur le décret de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique[816]. Dans cet avis, nous pouvons lire les préoccupations de la Commission nationale de l'informatique qui estime que la vérification de la majorité d'âge ne doit pas conduire « à collecter des données

[814] Article 23 de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales. Voir également le décret d'application de la loi : décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

[815] Depuis le 31 décembre 2021, le CSA et la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi) ont fusionnés pour devenir l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom).

[816] CNIL, Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique. Disponible sur : https://cdnx.nextinpact.com/data-next/file-uploads/D-2021-069_1.CSA%20v%C3%A9rification%20d'%C3%A2ge%20_VD-2-1.pdf

directement identifiantes de leurs utilisateurs »[817], ce qui porterait atteinte au règlement 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[818]. En effet, plusieurs droits pourraient être atteints, comme le droit à la vie privée. Mais également, nous pouvons penser au risque de détournement des données et l'usurpation d'identité. La Commission estime préférable d'utiliser des dispositifs qui consistent en la fourniture d'une preuve de majorité d'âge en s'appuyant sur un organisme tiers de confiance pour assurer un double anonymat. Ainsi, elle exclut le traitement de données biométriques[819]. À cet égard, le législateur européen a également prévu dans le règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (« Digital Services Act ») que « les fournisseurs de plateformes en ligne accessibles à des mineurs mettent en place des mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de la sûreté et de la sécurité des mineurs au regard de leur service » [820]. Et, il ajoute que « le respect des obligations énoncées […] n'impose pas aux fournisseurs de plateformes en ligne de traiter des données à caractère personnel supplémentaires afin de déterminer si le destinataire du service est mineur »[821]. De plus, un autre article du règlement prévoit que les plateformes adoptent « de mesures ciblées visant à protéger les droits de l'enfant, y compris la vérification de l'âge et des outils de contrôle parental, ou des outils permettant d'aider les mineurs à signaler les abus ou à obtenir un soutien, s'il y a lieu »[822].

---

[817] *Ibid.* point 13.
[818] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[819] Au sens de l'article 8 du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[820] Article 28, paragraphe 1, Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[821] *Ibid.* article 28, paragraphe 3.
[822] *Ibid.* article 35 (j).

396. En Italie, une loi a également été adoptée en juin 2020[823] qui prévoit l'introduction du contrôle parental par défaut pour les mineurs[824]. Il s'agit d'un filtre préventif qui est configuré dans les appareils électroniques et qui pourra être enlevé seulement par la personne titulaire du contrat avec le fournisseur de service (une personne qui a atteint la majorité), en appelant gratuitement ce dernier[825]. Cette loi prévoit que ces services de contrôle parental pré-activés constituent, d'un côté, un filtre pour les contenus inappropriés pour les mineurs et, de l'autre, un blocage pour les contenus réservés à un public de plus de 18 ans (qui correspond à la majorité légale en Italie)[826]. Or, cela a suscité de vives critiques par certains experts qui se demandent quels types de contenus entrent dans la définition de « contenus inappropriés pour les mineurs ». Pour ces experts, il y aurait un fort risque de censure[827] générale de certains sites et contenus. D'autres se demandent également comment cette loi pourra être mise en œuvre dans les faits, en rappelant que dans d'autres États comme l'Angleterre un projet de loi similaire a été abandonné après des années de problèmes techniques et de préoccupations relatives aux possibles atteintes à la vie privée[828]. L'Allemagne est attentive à ces lois car, depuis

[823] Legge n. 70 del 25 giugno 2020 di conversione del D.L. n. 28/2020, *Misure urgenti in materia di intercettazioni, di ordinamento penitenziario, di giustizia civile, penale, amministrativa e contabile e per l'introduzione del sistema di allerta Covid-19.*

[824] Article 7 bis de la legge n. 70 del 25 giugno 2020 di conversione del D.L. n. 28/2020, *Misure urgenti in materia di intercettazioni, di ordinamento penitenziario, di giustizia civile, penale, amministrativa e contabile e per l'introduzione del sistema di allerta Covid-19.*

[825] *Ibid.* article 7 bis, paragraphe 2.

[826] Texte original : « I contratti di fornitura nei servizi di comunicazione elettronica disciplinati dal codice di cui al decreto legislativo 1° agosto 2003, n. 259, devono prevedere tra i servizi preattivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto ». Voir article 7 bis, paragraphe 1, de la legge n. 70 del 25 giugno 2020 di conversione del D.L. n. 28/2020, *Misure urgenti in materia di intercettazioni, di ordinamento penitenziario, di giustizia civile, penale, amministrativa e contabile e per l'introduzione del sistema di allerta Covid-19.*

[827] Voir les propos de l'avocat Fulvio Speranza spécialiste du droit d'Internet, A. LONGO, *Filtro automatico al porno su Internet, ecco la norma firmata Lega*, La Repubblica, 19 juin 2020. Disponible sur : https://www.repubblica.it/economia/2020/06/19/news/filtro_automatico_al_porno_su_Internet_ecco_la_norma_firmata_lega-259545443/. Voir également P. REMER, Siti porno: ecco la legge che li blocca, *La legge per tutti*, 22 juin 2020. Disponible sur : https://www.laleggepertutti.it/410336_siti-porno-ecco-la-legge-che-li-blocca

[828] J. WATERSON, *UK drops plans for online pornography age verification system*, The Guardian, 16 octobre 2019. Disponible sur : https://www.theguardian.com/culture/2019/oct/16/uk-drops-plans-for-online-pornography-age-verification-system Voir également un article antérieur : J. WATERSON and A. HERN, *UK age-verification system for porn delayed by six monthS*, The Guardian, 20 juin 2019.
Disponible sur : https://www.theguardian.com/technology/2019/jun/20/uks-porn-age-verification-system-to-be-delayed-indefinitely

2021, le gouvernement souhaite également obliger les fabricants d'ordinateurs et de téléphone à installer un filtrage d'âge pour les contenus pornographiques[829].

397. Nous avons pu trouver une seule disposition préventive d'ordre technique intéressante dans le droit de l'Union européenne. Il s'agit du règlement 2021/784 du Parlement européen et du Conseil, du 17 mai 2021, relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne. Ce dernier prévoit que les plateformes doivent adopter des mesures spécifiques, dont « des moyens techniques appropriés pour identifier et retirer promptement le contenu à caractère terroriste ou bloquer l'accès à ce contenu »[830].

398. Une autre forme de prévention aux risques de cyberviolence pourrait être l'obligation d'âge minimum pour s'inscrire dans les réseaux sociaux. Aujourd'hui il n'y a pas de texte sur le sujet en droit de l'Union européenne. Dans la majorité des États membres de l'Union européenne, la loi autorise les inscriptions à partir de 13 ans. Toutefois, ces limitations d'âge ne sont pas effectives. En effet, les plateformes ne procèdent pas à un contrôle strict de l'âge. En témoignent les chiffres exposés par une enquête de l'association « Génération numérique » qui estime que 63% des enfants de 11-12 ans ont au moins un compte sur un réseau social[831].

En France, une loi a été adoptée visant à instaurer une majorité numérique à 15 ans pour s'inscrire sur les réseaux sociaux[832]. Cette dernière loi impose aux réseaux sociaux comme TikTok ou Instagram de refuser l'inscription des enfants de moins de 15 ans sauf si l'autorisation d'inscription est donnée par l'un des titulaires de l'autorité parentale et d'informer les enfants et leurs parents sur les risques des usages numériques et des

---

[829] D. CROSSLAND, *German plan for age filters across web to stop under-18s accessing pornography*, The Times, 22 juillet 2021. Disponible sur : https://www.thetimes.co.uk/article/german-plan-age-stop-under-18s-accessing-pornography-w9xpdl9rm

[830] Article 5, paragraphe 2 (a), du règlement 2021/784 du Parlement européen et du Conseil relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, 17 mai 2021.

[831] Génération numérique, *Les pratiques numériques des jeunes de 11 à 18 ans*, enquête 2021. Disponible sur : https://asso-generationnumerique.fr/wp-content/uploads/2021/03/Enque%CC%82te-2021-des-pratiques-nume%CC%81riques-des-11-18-ans.pdf

[832] Loi n°2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, publiée au Journal Officiel du 8 juillet 2023.

moyens de prévention. Elle prévoit également que les titulaires de l'autorité parentale peuvent demander la suspension d'un compte de leur enfant de moins de 15 ans et d'activer un dispositif pour contrôler le temps passé sur le réseau. La loi prévoit que ce sont les réseaux qui garantissent cette vérification par l'utilisation de solutions techniques conformes à un référentiel élaboré par l'Autorité de régulation de la communication audiovisuelle et numérique, après consultation de la CNIL[833]. La loi s'applique également aux comptes déjà existants.

399. Malgré l'absence de lois « techniques » préventives contre les cyberviolences, il existe des mesures préventives de filtrage mises en place par des acteurs privés, que cela soit par les fournisseurs d'accès ou par la société civile.

B. L'utilisation controversée des nouvelles technologies comme moyen de prévention

400. Il est utile d'analyser également certaines formes de prévention mises en œuvre par les plateformes. Ces mesures se manifestent à travers des systèmes de filtrage de contenus jugés illicites facilités par l'intelligence artificielle. Concrètement, il s'agit d'un système de reconnaissance de contenus estimés illicites par la plateforme vis-à-vis de ses standards de communauté qui permet d'empêcher la publication de ces contenus ou de les effacer après publication et avant le signalement par les utilisateurs. Dans le centre d'assistance de la plateforme Twitter plusieurs mesures sont prévues. Parmi elles, le fait de cacher un tweet non conforme aux standards de la communauté avant de l'effacer. En effet, à la place du contenu estimé illicite par la plateforme, que l'utilisateur a essayé de publier, il y aura un message qui indique que le contenu n'est pas disponible car il a violé les règles de Twitter[834].

[833] Article 4 de la loi n°2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, publiée au Journal Officiel du 8 juillet 2023.
[834] Twitter Help Center, Platform Use Guidelines, Our range of enforcement options, disponible sur : https://help.twitter.com/en/rules-and-policies/enforcement-options

401. Les outils de détection des contenus illicites peuvent être conçus pour vérifier des contenus déjà identifiés ou bien pour analyser les caractéristiques d'un nouveau contenu. Cela est possible, car ces outils sont « nourris » par les données récoltées de l'analyse des contenus retirés précédemment dans la plateforme. Par exemple, ils peuvent détecter des images pré-identifiées comme des logos ou des symboles spécifiques. Ou bien la nudité[835]. Ces pratiques des plateformes ont été critiquées à plusieurs reprises. En effet, comme il avait déjà été soulevé dans les développements précédents, ces filtrages peuvent donner lieu à une véritable censure. Cela a été le cas pour certaines œuvres d'art[836], mais également pour des photos de personnes en surpoids parce qu'elles étaient jugées pornographiques[837]. Cela serait causé par un problème lié aux paramétrages des outils de détection des contenus illicites. En effet, l'outil, face à une photo d'une personne en surpoids détecterait « trop » de peau et considèrerait cela comme de la nudité et de la pornographie. Ce « trop » serait lié au fait que les outils de détection se basent sur des photos, majoritaires sur les réseaux sociaux, des personnes minces. La nudité est souvent à l'origine de la sur-censure qui ne porte pas seulement atteinte à la liberté d'expression mais aussi peut avoir d'autres types de conséquences sur les utilisateurs. En témoigne l'expérience de deux pères aux États-Unis qui ont fait l'objet d'une enquête judiciaire pour pédocriminalité pour avoir envoyé des photos du sexe de leur enfant à un médecin lors d'une téléconsultation[838]. Nous ne connaissons pas le chiffre exact de contenus effacés avant la publication. En effet, grâce aux rapports d'application des standards de communautés de Facebook ou bien celui de YouTube, nous connaissons le

---

[835] Voir : E. LLANSÓ, J. Van HOBOKEN, P. LEERSSEN, J. HARAMBAM, *Artificial Intelligence, Content Moderation, and Freedom of Expression,* Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 26 February 2020, p. 6.

[836] Voir §85 de cette thèse.

[837] Voir par exemple L. CHAHUNEAU, *Grossophobie : la Une de Télérama censurée par Facebook et Instagram, les internautes contre-attaquent,* Le Parisien, 7 février 2020. Disponible sur : https://www.leparisien.fr/societe/grossophobie-la-une-de-telerama-censuree-par-facebook-et-instagram-les-internautes-contre-attaquent-07-02-2020-8255514.php. Voir aussi A. WHEELER, *« TikTok we need to talk » : Lizzo slams social media app for body shaming,* The Guardian, 5 mars 2020. Disponible sur : https://www.theguardian.com/music/2020/mar/05/lizzo-tiktok-body-shaming-censorship-social-media

[838] Courrier International, *Modération. Ils envoient des photos du sexe de leur enfant malade à un médecin, Google les étiquette comme pédocriminels,* 23 août 2022. Disponible sur : https://www.courrierinternational.com/article/moderation-ils-envoient-des-photos-du-sexe-de-leur-enfant-malade-a-un-medecin-google-les-etiquette-comme-pedocriminels?utm_medium=Social&utm_source=Facebook&Echobox=1661268523&fbclid=IwAR0beYB-l7gsyu-JqhPM-PmbuLvANpCtuz85DMltgWo5EwrUtlwt1CLhinE&fs=e&s=cl

nombre de contenus retirés avant le signalement des utilisateurs, toutefois il s'agit de contenus qui avaient déjà été publiés[839].

402. Ce filtrage *a priori* peut entraîner des atteintes aux droits des utilisateurs. En particulier, une atteinte à leur liberté d'expression et au droit à l'information. En outre, cela ne permet pas d'identifier et poursuivre les auteurs des contenus illicites. À cet égard, Human Rights Watch souligne que les plateformes des réseaux sociaux n'ont pas trouvé le moyen de garantir que les contenus qu'ils suppriment puissent être préservés, archivés et mis à disposition des enquêteurs[840]. Au contraire, ce filtrage avant publication a pu être très utile en matière de terrorisme. À cet égard, Twitter a communiqué que les trois-quarts des 300 000 comptes terroristes supprimés entre janvier et juin 2017 l'ont été avant qu'ils publient un contenu[841].

403. Une autre forme de prévention est effectuée par les utilisateurs. En effet, les plateformes permettent aux individus de paramétrer les contenus qu'ils souhaitent voir lorsqu'ils se connectent au réseau social. En effet, sur Twitter, Facebook ainsi que YouTube, les utilisateurs peuvent masquer les contenus qu'ils jugent indésirables en paramétrant leur fil d'actualité[842]. Cela, toutefois, n'est qu'une forme de prévention personnelle et subjective. Elle n'empêche pas la publication et la visualisation des contenus illicites par l'ensemble des utilisateurs.

404. Nous pouvons également analyser des actions de la société civile pour prévenir les cyberviolences. Nous pouvons mentionner application française « Bodyguard »[843] qui permet d'analyser et modérer les contenus haineux sur YouTube, Instagram, Twitter et Twitch avant que l'utilisateur les lise. Unique en son genre, cette application a protégé

---

[839] Voir Google, *Application du règlement de la communauté YouTube*, 2021 ainsi que Facebook, *Community Standards Enforcement Report,* Q3, 2021.
[840] Human Rights Watch, *"Video Unavailable" Social Media Platforms Remove Evidence of War Crimes,* 10 September 2020. Disponible sur : https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes cité par UNICRI, UNCCT, *Countering terrorism online with artificial intelligence*, 2021, p.42
[841] Voir le communiqué de presse de la Commission européenne : *Fighting Terrorism Online: Internet Forum pushes for automatic detection of terrorist propaganda*, 6 décembre 2017.
Disponible sur : https://ec.europa.eu/commission/presscorner/detail/en/IP_17_5105
[842] Voir : R. BADOUARD, *Les nouvelles lois du web. Modération et censure*, Seuil, octobre 2020, p. 63.
[843] Pour plus d'informations sur l'application BodyGuard, voir : https://www.bodyguard.ai/fr/particuliers

en 2020 plus de 50 000 personnes en Europe[844]. L'application est disponible pour les particuliers ainsi que pour les familles et les entreprises. Elle dispose d'outils de détection des contenus illicites qui sont programmés en plusieurs langues (français, anglais et italien). Pour les particuliers, elle permet à la personne qui la télécharge de régler les contenus qu'elle souhaite voir apparaître ou pas. Pour cela, elle propose des niveaux de protection (basse, moyenne, forte ou maximum) pour différents types de contenus comme les insultes, les moqueries physiques mais aussi le racisme, la LGBTQIA+ phobies, la misogynie ou le harcèlement sexuel. Cette solution permet aux utilisateurs de ne pas voir les commentaires et contenus haineux qui les concernent. Toutefois elle ne traite pas les autres contenus auxquels les utilisateurs peuvent être exposés. D'une part, cette application a le mérite d'éviter que l'utilisateur soit exposé à des contenus haineux, et, ainsi, qu'il subisse les conséquences de ces violences comme la dépression, la perte d'estime de soi ou encore la censure. De l'autre, elle a un inconvénient car elle ne permet pas d'identifier et de faire sanctionner les personnes qui ont publié des commentaires haineux. En effet, l'utilisateur qui est censé vouloir se protéger des commentaires haineux ne verra pas les contenus illicites, sauf s'il décide d'aller les visionner dans un espace dédié où ils sont stockés pour un temps donné par l'application[845]. Dans ce cas, l'utilisateur pourra essayer d'identifier l'auteur et le signaler, mais si la personne ne regarde pas les commentaires filtrés, ces derniers seront ensuite effacés et l'auteur ne pourra pas être sanctionné. L'utilisateur sera protégé car il ne voit pas les contenus haineux mais les auteurs de ces contenus ne seront ni puni ni sensibilisés.

405. Enfin, nous pouvons citer une autre solution qui se situe entre la prévention et la sanction. Il s'agit du « shadow ban » (interdiction de l'ombre)[846], c'est-à-dire de la possibilité de rendre un contenu invisible pour les utilisateurs, et, par conséquent, réduire son affichage afin de limiter sa visibilité tout en évitant de le supprimer[847].

---

[844] C. PARIS, *Bodyguard Rewind : retour sur l'année 2020,* 1er janvier 2021.
[845] Voir la rubrique des questions fréquentes posées sur le site BodyGuard et, en particulier, la question « Est-ce que vous conservez les commentaires qui me sont destinés ? », disponible sur : https://www.bodyguard.ai/fr/faq
[846] Ces mesures seront également étudiées sous le prisme de la sanction, voir chapitre VII de cette thèse.
[847] Voir : R. BADOUARD, *Les nouvelles lois du web. Modération et censure,* Seuil, octobre 2020, pp. 60-67. Ainsi que du même auteur « Shadow ban. L'invisibilisation des contenus en ligne », *Revue Esprit*, novembre

406. Après avoir analysé les différentes formes de sensibilisation et d'éducation ainsi que les acteurs impliqués, il convient d'étudier leur efficacité.

Section II : L'efficacité relative des mesures préventives des acteurs privés

407. Face à l'essor et à la croissance du phénomène des cyberviolences, nous avons vu se développer un véritable multilatéralisme du cyberespace pour prévenir les atteintes en ligne qui compte les États, les organisations régionales et internationales ainsi que le secteur privé. Parmi ces acteurs, les entreprises, et en particulier, les plateformes, sont en première ligne et affichent publiquement leur engagement pour améliorer la prévention des comportements illicites.

408. Dans les développements qui vont suivre, il s'agira, d'une part, d'analyser l'essor d'une diplomatie du cyber espace (**§I**) et, d'autre part, de mesurer l'efficacité des mesures mises en œuvre par les acteurs privés (**§II**).

I. La montée de la diplomatie du cyber espace pour la défense des droits humains

409. Depuis plusieurs années, les sujets liés au cyberespace ont pris de plus en plus de place dans les enceintes internationales. On peut mentionner le Sommet mondial sur la société de l'information organisé par les Nations unies et qui a créé, en 2005, le Forum sur la gouvernance d'Internet. Ce dernier est une plateforme mondiale de débats sur les politiques publiques relatives à Internet. Son mandat, au début fixé à 5 ans, a été reconduit pour 10 ans par l'Assemblée générale des Nations unies en 2015[848]. Cela démontre l'intérêt et l'utilité grandissante de ces enjeux.

410. Il est important d'analyser quels types de collaborations existent vis-à-vis des cyberviolences de contenu. On constate que les rendez-vous mondiaux organisés par les

2021. Disponible sur : https://esprit.presse.fr/article/romain-badouard/shadow-ban-l-invisibilisation-des-contenus-en-ligne-43629

[848] Assemblée générale des Nations Unies, résolution 70/125, 16 décembre 2015, A/RES/70/125, § 63.

États sont le plus souvent tournés vers des préoccupations liées à la cybersécurité ou à la transformation technologique[849]. Le sujet des cyberviolences revient moins souvent sur le devant de la scène et des négociations. En 2019, la France et la Nouvelle Zélande ont lancé l'« Appel de Christchurch », après l'attentat terroriste du 15 mars 2019 à Christchurch (Nouvelle Zélande). L'auteur de la tuerie avait relayé en direct ses actes sur les réseaux sociaux pendant plusieurs minutes. Cet appel a permis de réformer le Forum mondial d'Internet contre le terrorisme et de mettre en place un protocole de gestion de crise[850] commun pour les États et les entreprises pour répondre plus efficacement aux attaques terroristes diffusés en direct en ligne. Ce protocole a déjà été utilisé à deux reprises : en 2019, pendant la diffusion de l'attentat de Yom Kippour à Halle en Allemagne et, en 2020, lors de la fusillade de Glendale aux États-Unis. Toutefois, nonobstant l'adoption de ce protocole, la vidéo de Halle a tout de même circulé sur le réseau Twitch pendant trente-cinq minutes[851]. Un autre attentat, en 2022, à Buffalo (États-Unis) a également pu circuler sur les réseaux sociaux en direct[852]. Malgré une efficacité encore limitée, nous pouvons souligner que cet appel a le mérite de renforcer la coopération entre les États, les institutions et les entreprises engagées dans la lutte contre le partage des contenus illicites[853].

---

[849] Voir par exemple aux États-Unis le Cyber Security Summit, plus d'informations sur : https://cybersecuritysummit.com/. En France, le Forum international de la cybersécurité organisé par la Gendarmerie nationale, plus d'informations sur : https://www.forum-fic.com/
Sur la transformation numérique et les enjeux sociaux liés au numérique, nous pouvons mentionner le GovTech Summit, plus d'informations sur https://www.govtechsummit.eu/, ainsi que le Paris Cyber Summit, voir https://www.paris-cyber-summit.com/

[850] Voir European Commission, *Security Union: Commission welcomes political agreement on removing terrorist content online,* 10 décembre 2020. Disponible sur : https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372

[851] *Attentat de Halle en Allemagne : La diffusion en ligne de la vidéo de l'attaque montre la difficulté à stopper les « live »*, 20 Minutes avec l'AFP, 10 octobre 2019. Disponible sur : https://www.20minutes.fr/monde/2624675-20191010-attentat-halle-allemagne-diffusion-ligne-video-attaque-montre-difficulte-stopper-lives

[852] D-J. RAHMIL, *« Il y a eu un loupé » : pourquoi vous n'auriez jamais dû voir la vidéo de l'attentat de Buffalo*, L'ADN, 16 mai 2022. Disponible sur : https://www.ladn.eu/media-mutants/reseaux-sociaux/comment-video-attentat-buffalo-virale/

[853] Les soutiens de l'appel de Christchurch sont multiples, on compte aujourd'hui 54 États, la Commission européenne, le Conseil de l'Europe, l'UNESCO, ainsi que les principaux fournisseurs de service en ligne (Amazon, Facebook, Google, Microsoft, Dailymotion, Twitter, YouTube et Qwant).Voir : https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites-et-evenements/article/l-appel-de-christchurch-quelles-avancees-12-05-21

411. Une autre initiative multilatérale qui concerne le terrorisme en ligne est celle du « EU Internet Forum ». Lancé en 2015, ce forum compte les ministres de l'intérieur des États membres de l'Union européenne et les représentants de plateformes en ligne, ainsi que EUROPOL, l'Union européenne et son coordinateur au terrorisme[854]. Cette initiative a comme objectif de s'attaquer à l'utilisation d'Internet à des fins terroristes à travers la réduction de l'accessibilité des contenus terroristes en ligne et l'augmentation de la diffusion de récits alternatifs[855].

412. Nous pouvons également mentionner l'« Alliance to better protect minors online » qui a vu le jour en 2017 sous l'impulsion de la Commission européenne. Elle est composée d'entreprises des nouvelles technologies et des médias[856], des organisations non gouvernementales ainsi que le Fonds des Nations Unies pour l'enfance (UNICEF). Elle a comme objectif d'améliorer l'environnement numérique pour les mineurs à travers la sensibilisation, la collaboration renforcée entre acteurs et l'outillage des utilisateurs. Cette coalition d'acteurs se focalise sur les contenus, les comportements et les contacts illicites, c'est-à-dire, parmi d'autres, les contenus violents, le cyberharcèlement et l'extorsion à des fins sexuels[857]. L'évaluation de cette initiative en 2018 a montré les forces et les faiblesses de cette coopération. Elle a l'avantage de compter parmi ses membres une multitude d'acteurs, d'avoir la capacité de formaliser des engagements qui ont incité les entreprises à redynamiser leurs efforts. Ainsi, la présence de la Commission européenne est un gage de légitimité et de visibilité[858]. Cependant, elle a également des faiblesses, notamment le fait que les engagements pris par les entreprises membres de

---

[854] European Commission, EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online, Press release, 3 décembre 2015. Disponible sur : https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243

[855] Les contre-récits et récits alternatifs au terrorisme sont des discours qui combattent les discours de propagande terroriste en discréditant et en déconstruisant les récits sur lesquels ils reposent.

[856] Les entreprises members sont multiples : ASKfm, BT Group, Deutsche Telekom, Disney, Facebook, Google, KPN, The LEGO Group, Liberty Global, Microsoft, Orange, Rovio, Samsung Electronics, Sky, Snap, Spotify, Sulake, Super RTL/Mediengruppe RTL Deutschland, TikTok, TIM (Telecom Italia), Telefónica, Telenor, Telia Company, Twitter, Vivendi, Vodafone. Pour plus d'informations, voir : https://digital-strategy.ec.europa.eu/en/policies/protect-minors-online

[857] Pour avoir plus d'informations sur leur plan d'action, voir l'« Alliance's statement of purpose » disponible sur : https://digital-strategy.ec.europa.eu/en/policies/protect-minors-online

[858] Voir : Ramboll Management Consulting, *Evaluation of the implementation of the Alliance To Better Protect Minors Online*, Final report, European Commission, 2018, p. 5. Disponible sur : https://op.europa.eu/en/publication-detail/-/publication/122e3bdd-237b-11e9-8d04-01aa75ed71a1/language-en

l'Alliance ne sont pas nouveaux et certains d'entre eux ne sont pas mesurables. Cela rend difficile leur évaluation[859].

413. Enfin, nous pouvons citer la « WeProtect Global Alliance », organisation indépendante qui a comme mission de protéger les mineurs des abus sexuels en ligne. Elle réunit, comme l'exemple précèdent, des entreprises privées, des gouvernements, des organisations de la société civile et des organisations internationales[860].

414. Ces exemples montrent la multiplication d'initiatives multilatérales pour s'attaquer aux différentes formes de cyberviolences. Ces types de coalitions existent également au niveau national, nous pouvons citer l'Observatoire de la haine en ligne en France, créé suite à l'adoption de la loi 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet, qui réunit les plateformes d'Internet ainsi que des chercheurs et des associations. Ces alliances témoignent également de la nécessité d'impliquer plusieurs acteurs à la fois : les décideurs politiques, le secteur privé, les expertes ainsi que les membres de la société civile. Toutefois, nonobstant la participation des plateformes à ces initiatives, il est nécessaire d'analyser leurs véritables efforts pour éradiquer les cyberviolences de leurs réseaux. En effet, les mesures prises par ces entreprises privées ne sont pas toujours efficaces. On constate que derrière des discours proactifs et des effets d'annonce, se cache une inaction volontaire justifiée par la recherche de profits économiques.

II. Des mesures insuffisantes des acteurs privés

415. Les plateformes se sont engagées depuis plusieurs années à veiller à la prévention et à l'effacement des contenus illicites. On l'avait déjà souligné en citant le Code de conduite signé avec la Commission européenne ou bien l'accord avec la Fédération mondiale des annonceurs pour mieux lutter contre les contenus haineux[861]. Toutefois,

---

[859] *Ibid.* p. 6.
[860] Sur leur site, au 30 août 2023, on dénombre 102 gouvernements (des États asiatiques, africains, arabes ainsi qu'européens), 66 entreprises (entre autres : Amazon, Google, Apple, Twitter, Snap), 92 organisations non gouvernementales et 9 organisations internationales et régionales (entre autres : EUROPOL, l'Union européenne, l'Union africaine, INTERPOL, l'UNCEF et l'UNODC). Voir https://www.weprotect.org/alliance/
[861] Voir chapitre § 325 de cette thèse.

ces engagements ne sont pas contraignants. Il n'en reste pas moins que les plateformes sont obligées de se conformer aux textes internationaux, régionaux[862] ou aux dispositions nationales[863]. Malgré la difficulté de les responsabiliser du fait de leur statut particulier[864], il faut souligner que ces derniers ont pu contribuer de manière positive à la lutte contre les cyberviolences. Toutefois, les collaborations entre les plateformes et les acteurs traditionnels ne sont pas toujours efficaces.

416. Nous nous concentrons sur les collaborations entre les plateformes et les États. D'autres formes de collaboration existent, par exemple entre les acteurs privés et les organisations internationales[865], toutefois ces dernières restent marginales et n'apportent pas d'éléments significatifs à notre analyse.

417. Dans les prochains développements il s'agira d'analyser la stratégie préventive défaillante des plateformes au regard de leur modèle économique (**A**) pour ensuite étudier les mesures préventives existantes portant atteinte aux droits humains des utilisateurs (**B**).

A. La logique économique primant sur la prévention

418. Certaines plateformes sont fondées sur des modèles économiques discutables. Il conviendra d'analyser les pratiques des deux plateformes contrôlées par l'entreprise Meta[866], c'est-à-dire Facebook et Instagram. Ces dernières ont fait l'objet en 2021 de

---

[862] Par exemple la directive 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant 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 (directive «Services de médias audiovisuels»), en particulier l'article 28 ter, ou le Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

[863] Voir en France l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

[864] Ce point sera approfondi dans le chapitre suivant.

[865] Voir par exemple le partenariat entre l'UNESCO et le réseau TikTok pour lutter contre le négationnisme sur Internet, voir : *Holocauste : l'UNESCO, le Congrès juif mondial et TikTok partenaires contre le négationnisme,* ONU Info, 27 janvier 2022. Disponible sur : https://news.un.org/fr/story/2022/01/1113052. Ainsi que, celui entre ONU Femmes et TikTok pendant la campagne Orange Day contre les violences faites aux femmes y compris en ligne, voir L. BROSSELIN, *TikTok et l'ONU Femmes lancent un forum de discussion et de sensibilisation sur le cybersexisme*, L'ADN, 17 décembre 2021. Disponible sur : https://business.ladn.eu/news-business/actualites-annonceurs/tiktok-un-women-forum-sensibilisation-cybersexisme/

[866] Société mère de Facebook, anciennement appelé Facebook mais toujours sous la direction de Mark Zuckerberg.

révélations de la part de Frances Haugen, lanceuse d'alerte et ancienne employée de Facebook. Les documents internes qu'elle a révélés montrent, entre autres, que les deux réseaux sociaux n'ont pas mené d'actions de prévention contre les violences en ligne pour donner la priorité à leurs profits économiques et commerciaux. Parmi les révélations de la lanceuse d'alerte qui a été interviewée par le Congrès américain ainsi que par l'Assemblée nationale en France et le Parlement européen, il y a des documents qui montrent que Meta a, à plusieurs reprises, privilégié le profit économique plutôt que de réagir à des atteintes à la démocratie ou à la santé physique et mentale de ses utilisateurs. Ces propos ont été considérés comme faux par Monica Bickert, chargée de la politique des contenus de Facebook[867].

419. Nous nous sommes basés, faute d'avoir accès à l'ensemble des documents dévoilés par la lanceuse d'alerte, aux articles de presse des journalistes qui ont pu analyser ces écrits, ainsi que certains documents publiés par les plateformes elles-mêmes après le scandale médiatique.

420. Premièrement, on constate que les choix de Facebook sont dictés par la perception du public, les risques commerciaux et la menace politique de la réglementation. Deuxièmement, les réactions de la plateforme arrivent, si elles arrivent, très lentement et avec retard. À cet égard, un salarié avait écrit une note lors de son départ en précisant « we were willing to act only after things had spiraled into a dire state »[868]. En effet, on constate que l'action de la plateforme est plus une réaction et que la prévention n'est pas très efficace. Un exemple est celui de la traite des êtres humains. En automne 2019, Facebook a mené une action contre l'utilisation de Facebook et Instagram à des fins de traite, qui était notamment facilitée par le partage de mots clés et de hashtags[869]. Cela a conduit à la suppression de 129 191 contenus et à la désactivation d'environ 1000 comptes. Toutefois, cette initiative positive arrive très tard par rapport aux signalements

---

[867] Voir : D. LELOUP, A. PIQUARD, *Facebook ne place pas les profits avant les gens*, Le Monde, 11 octobre 2021.
[868] Voir : A. LA FRANCE, *History will not judge us Kindly*, The Atlantic, 25 octobre 2021. Disponible sur : https://www.theatlantic.com/ideas/archive/2021/10/facebook-papers-democracy-election-zuckerberg/620478/. Traduction par l'autrice : « Nous n'étions prêts à agir qu'après que les choses se soient détériorées… ».
[869] Sur la puissance des hashtags, voir §§ 129-131 de cette thèse.

initiaux des tels actes illicites. En effet, dès mars 2018, des signalements avaient été faits constatant la présence de profils Instagram qui proposaient la vente de femmes domestiques victimes de traite. En octobre 2019, la BBC relevait ce trafic après avoir mené une enquête clandestine[870]. Suite à cela, Facebook avait supprimé 700 profils Instagram mais, selon un rapport interne, des contenus étaient restés sur la plateforme[871]. Comme le décrit le journal Atlantic, Meta a décidé de mener une action plus sérieuse contre la traite des êtres humains seulement quand Apple en octobre 2019 a menacé de retirer les applications Facebook et Instagram de son App store[872]. Il s'agirait donc d'une réaction motivée par les importantes conséquences commerciales que la manœuvre d'Apple aurait causé. Troisièmement, lorsqu'il s'agit de prévenir la diffusion de contenus illicites, notamment les contenus violents et haineux, nous constatons que, non seulement la plateforme n'agit pas, mais ses algorithmes amplifient l'extrémisme et incitent à la violence[873]. À cet égard, on peut se concentrer sur deux arguments.

421. D'une part, Facebook ne consacre pas les mêmes moyens financiers à la modération des contenus dans tous les États où il est disponible. Comme le souligne Madame Haugen, « les pays les plus fragiles ont la version la moins sécurisée de Facebook »[874]. En effet, les efforts économiques et monétaires sont tournés principalement vers les États-Unis et l'Europe. Pour certains États, il y a un manque préoccupant de modérateurs maîtrisant certaines langues et dialectes et cela vaut également pour l'intelligence artificielle. En effet, comme l'explique le journal « Le Monde », les systèmes informatiques ont besoin de « classifiers », des algorithmes qui leur permettent d'identifier les contenus illicites. Mais cette opération est possible seulement grâce à la collecte d'un grand nombre des données dans la langue correspondante. Or, pour donner un exemple : dans les documents dévoilés par la lanceuse d'alerte il n'y a aucun « classifiers » en matière de haine en ligne en langue oromo ou amharique[875]. Cela a

[870] Voir O.PINNELL, J. KELLY, *Slave markets found on Instagram and other apps,* BBC News Arabic, 31 octobre 2019. Disponible sur : https://www.bbc.com/news/technology-50228549
[871] Voir : E. CUSHING, *How Facebook fails 90 percent of its users,* The Atlantic, 25 octobre 2021. Disponible sur : https://www.theatlantic.com/ideas/archive/2021/10/facebook-failed-the-world/620479/
[872] Il s'agit du magasin virtuel d'Apple où il est possible de télécharger les applications.
[873] Cela vaut également pour l'amplification de la désinformation ou de la polarisation politique.
[874] A. PIQUARD, *Facebook hors des États-Unis : les failles d'une tour de Babel,* Le Monde, 26 octobre 2021.
[875] *Ibid.*

comme conséquence, d'un côté, que les contenus publiés dans des langues non reconnues par l'intelligence artificielle ne sont pas analysés et filtrés. De l'autre côté, que certains contenus sont censurés par des modérateurs qui ne maîtrisent pas la langue et qui interprètent mal le sens des mots[876]. On découvre que, en 2019, l'ONG Avaaz a publié un rapport dans lequel elle pointe du doigt le comportement passif de Facebook vis-à-vis des milliers de commentaires haineux sur Facebook contre les bengalis, en particulier les musulmans, habitant dans l'État de Assam en Inde[877]. Les musulmans auraient été traités de « porcs », « violeurs », « terroristes » et « parasites » en toute impunité[878]. Selon le rapport de Avaaz, parmi les 800 publications analysées par l'ONG, 26,5% d'entre elles étaient des contenus haineux et ces derniers avaient été partagés 99,650 fois comptabilisant environ 5,4 millions de vues. Cependant, l'intelligence artificielle de Facebook, censée détecter les contenus haineux, n'a pas fonctionné car elle ne connaissait pas la langue assamais. Comme le souligne Avaaz, cela est une grande faiblesse pour la plateforme, non seulement dans ce cas, mais également pour les autres minorités ethniques qui sont souvent la cible d'attaques haineuses.

422. D'autre part, les algorithmes de la plateforme permettent à certains contenus problématiques d'être plus visibles. Cela a été le cas pour des contenus violents et la nudité, notamment auprès d'utilisateurs qui avaient peu de connaissances de la plateforme et qui étaient désarmés face à de tels contenus[879]. En effet, ils ne connaissaient pas les fonctionnalités qui permettaient de cacher les publications, de bloquer des personnes indésirables ou de signaler les contenus illicites. Ainsi, les documents internes de Facebook font état en 2019 du fait que les publications avec des réactions

---

[876] Par exemple, le mot « zamel » est une insulte au Maroc mais au Yemen il s'agit d'un chant populaire. Egalement, comme le souligne Le Monde, l'expression « Al chabab » qui est le nom d'une organisation terroriste, c'est également une expression courante dans certains dialectes qui n'a rien d'illicite. Voir : M. UNTERSINGER, D. LELOUP, Pour modérer 220 millions d'utilisateurs en langue arabe, Facebook n'emploie que 766 modérateurs, Le Monde, 16 novembre 2021.

[877] AVAAZ, *Megaphone for hate - Disinformation and hate speech on Facebook during Assam's citizenship count*, Octobre 2019, pp. 7-9. Disponible sur : https://avaazpress.s3.amazonaws.com/FINAL-Facebook%20in%20Assam_Megaphone%20for%20hate%20-%20Compressed%20(1).pdf

[878] *Ibid.* p. 9.

[879] K. JACOBY, *Facebook fed posts with violence and nudity to people with low digital literacy*, USA Today, 23 novembre 2021. Disponible sur : https://eu.usatoday.com/story/tech/2021/11/23/facebook-posts-violence-nudity-algorithm/6240462001/

colériques[880] sont plus susceptibles d'aller à l'encontre des standards de communautés. Toutefois, ces publications ont plus de probabilité d'apparaître dans les fils d'actualités que les autres publications, par exemple celles qui ont reçu seulement des appréciations « j'aime ». Cela se produit car, les publications avec des réactions colériques génèrent plus de vues et des commentaires et cela est économiquement plus intéressant pour la plateforme. Les équipes de Facebook ont pu empêcher la diffusion, auprès d'un grand nombre d'utilisateurs, de publications qui suscitent de la colère en modifiant le poids de l'algorithme. Toutefois, ce type d'action de la part des salariés ne trouve pas toujours gain de cause. En effet, comme le montrent les documents publiés par Madame Haugen, Mark Zuckerberg aurait refusé la demande des équipes de Facebook de ne pas prioriser la diffusion des contenus pour les personnes en fonction du comportement de leurs amis de Facebook, cela, afin d'empêcher la diffusion de contenus haineux et incitant à la violence[881].

423. Enfin, grâce aux révélations de la lanceuse d'alerte, on découvre que selon des enquêtes internes, Instagram serait nocif pour les adolescents. En particulier, on peut lire qu'un adolescent sur cinq considère qu'Instagram le fait sentir plus mal dans sa peau[882]. Cela n'est pas étonnant quand l'on sait que des contenus pro-anorexie ont été suggérés aux utilisateurs[883]. Toutefois, les accusations faites à la plateforme ont été démenties par Facebook qui, pour répondre à ces accusations, a publié les enquêtes en question ainsi qu'un communiqué sur son site Internet[884]. L'existence de ces études concernant l'impact sur la santé mentale des adolescents vis-à-vis de leur utilisation de la plateforme

---

[880] Sur Facebook les utilisateurs peuvent ajouter des réactions aux contenus qu'ils visionnent. Ils peuvent cliquer sur l'icône « j'aime » mais également choisir des icones qui expriment : amour, soutien, rire, stupeur, tristesse ou colère.

[881] Voir A. LA FRANCE, *History will not judge us Kindly*, The Atlantic, 25 octobre 2021. Disponible sur : https://www.theatlantic.com/ideas/archive/2021/10/facebook-papers-democracy-election-zuckerberg/620478/.

[882] Voir le document partagé par le Wall Street Jounal qui reproduit l'étude interne de Facebook : Facebook, *Teen Mental Health Deep Dive*, octobre 2019, p. 23. Disponible sur : https://s.wsj.net/public/resources/documents/teen-mental-health-deep-dive.pdf

[883] Voir A. PIQUARD, F. REYNAUD, *Des pro-anorexie aux pro-QAnon : Facebook face aux effets de ses recommandations automatiques*, Le Monde, 27 octobre 2021.

[884] Pour les enquêtes voir Instagram, *Hard life moments-mental health deep drive*, Original Research, disponible sur : https://about.fb.com/wp-content/uploads/2021/09/Instagram-Teen-Annotated-Research-Deck-1.pdf Pour le communiqué voir : K. NEWTON, *Using research to improve your experience*, Instagram, 14 septembre 2021. Disponible sur : https://about.instagram.com/blog/announcements/using-research-to-improve-your-experience

n'est pas mauvaise en soi. Au contraire, elles permettent de formuler des solutions à leurs effets néfastes. Toutefois, une fois identifiées, ces solutions positives à mettre en œuvre pour réduire les effets négatifs de la plateforme doivent être adoptées et non pas être mises de côté pour favoriser la logique marchande.

424. Après avoir constaté les réticences de certaines plateformes d'adopter des mesures de prévention, il convient également de mentionner que ces dernières ont mis en œuvre des formes préventives de filtrage et de blocage sous demande des autorités étatiques.

B. L'existence des mesures préventives portant atteinte aux droits humains

425. Certains comportements problématiques avaient été constaté par le rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression du Conseil des droits de l'Homme des Nations unies. En effet, ce dernier, dans son rapport de 2016 souligne que les États, à l'aide du secteur privé, filtrent ou bloquent certains contenus de façon inutile ou disproportionnée[885]. Ces mesures techniques visent à restreindre l'accès à des données[886] et peuvent s'accompagner du retrait et de la suppression d'un contenu[887]. Plusieurs exemples récents viennent conforter cette analyse, en particulier au Vietnam où Amnesty international a dénoncé le filtrage préventif et le blocage des contenus politiques sur Facebook et YouTube. Ces deux plateformes se sont pliées aux demandes du gouvernement de supprimer des contenus critiquant le régime en place, comme le démontre le rapport de l'ONG publié en 2020[888]. On y lit, par exemple, que Facebook, sous la pression du gouvernement, qui avait suspendu les serveurs locaux et rendu plus lents ses services, a cédé aux demandes des autorités nationales et a officiellement adapté ses politiques aux demandes internes du gouvernement. Cela a fait augmenter la censure et porté atteinte à la liberté d'expression en matière politique, en

---

[885] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/32/38, 11 mai 2016, points 34-50.
[886] Voir Q. VAN ENIS, « Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 137.
[887] Le blocage et le filtrage seront traités plus en détail dans le chapitre VII de cette thèse.
[888] Amnesty International, *Let us breathe! Censorship and criminalization of online expression in Viet Nam*, 2020.

violation du droit international des droits humains [889]. Au Vietnam, un média du gouvernement a signalé qu'en 2020 Facebook avait supprimé plus de 2000 publications, ce qui correspond à une augmentation de 500% de suppressions par rapport à 2019 en se conformant à 95% des demandes du gouvernement. Le réseau YouTube s'était conformé à 90% de toutes les demandes.[890] Le rapport d'Amnesty souligne également que le Vietnam est le premier État dans le sud-est asiatique à avoir des mesures si restrictives et qu'il y a un risque que d'autres États s'en aspirent. La Thaïlande semble déjà avoir suivi l'exemple vietnamien, en effet, le ministère de l'économie numérique a porté plainte à plusieurs reprises contre Facebook pour ne pas s'être adapté aux politiques de restriction des contenus considérés illicites, y compris les insultes à la monarchie thaïlandaise [891]. Les enquêtes d'Amnesty ont également démontré que certains contenus disparaissaient des plateformes sans que les auteurs aient une notification[892]. De plus, certaines suppressions par YouTube étaient faites sans être suivies d'explications[893]. Ces comportements problématiques de la part des plateformes sont confirmés également par les enquêtes de l'ONG Reporters Sans Frontières. Selon leur rapport publié en 2017 sur la censure et la surveillance des journalistes, il est indiqué que la plateforme Facebook a développé un outil pour censurer des contenus selon les zones géographiques et cela pour satisfaire les demandes de certains États comme la Chine[894].

426. Ces exemples nous amènent à parler du respect du principe de la neutralité des réseaux. En effet, en filtrant les informations et en mettant en valeur certains contenus plus que d'autres, les plateformes sont soupçonnées d'aller à l'encontre du principe de neutralité. Ce principe, dont le concept a été popularisé par le professeur Tim Wu[895], prévoit que tout individu a le droit d'accéder aux mêmes contenus sur Internet et à travers n'importe quel fournisseur d'accès. Il a été introduit dans le droit matériel de l'Union européenne par le règlement 2015/2120 du Parlement européen et du Conseil, du

[889] *Ibid.* p. 23.
[890] *Ibid.* p. 23.
[891] *Ibid.* p. 22.
[892] *Ibid.* p. 31.
[893] *Ibid.* p. 26.
[894] Reporters without borders, *Censorship and surveillance of journalists: an unscrupulous business*, 2017, p. 5.
[895] Voir : T. WU, *Network Neutrality, Broadband Discrimination*, Journal of Telecommunications and Hight Technology, Vol.2, 2003.

25 novembre 2015, établissant des mesures relatives à l'accès à un Internet ouvert qui a ensuite été modifié par le règlement 2018/1971 du Parlement européen et du Conseil, du 11 décembre 2018, établissant l'Organe des régulateurs européens des communications électroniques (ORECE) et l'Agence de soutien à l'ORECE (Office de l'ORECE).

L'article 3, paragraphe 1, du règlement n°2015/2120 prévoit que :

> « Les utilisateurs finals ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'Internet »[896].

Cela implique que tout individu doit pouvoir bénéficier des mêmes informations et que les fournisseurs doivent s'abstenir de : « bloquer, de ralentir, de modifier, de restreindre, de perturber, de dégrader ou de traiter de manière discriminatoire des contenus, des applications ou des services spécifiques ou des catégories spécifiques de contenus, d'applications ou de services »[897] sauf dans certaines conditions[898].

427. À plusieurs reprises, les plateformes, telles que Facebook ou Twitter, ont dû s'expliquer face à des atteintes présumées à la neutralité. Comme cela a été le cas lors de la suspension du compte de l'ancien président Donald Trump[899] ou encore en certaines

---

[896] Article 3, paragraphe 1, du Règlement 2015/2120 du Parlement européen et du Conseil, du 25 novembre 2015, établissant des mesures relatives à l'accès à un Internet ouvert et aux prix de détail pour les communications à l'intérieur de l'Union européenne.
[897] *Ibid.* article 3, paragraphe 3.
[898] Voir la suite de l'article 3, paragraphe 3, du Règlement 2015/2120 du Parlement européen et du Conseil, du 25 novembre 2015, établissant des mesures relatives à l'accès à un Internet ouvert et aux prix de détail pour les communications à l'intérieur de l'Union européenne. Voir également : C. CASTETS-RENARD, *Droit du marché unique numérique et intelligence artificielle*, Bruylant, 2020, pp. 156-157.
[899] La suspension du compte de Donald Trump avait été faite dans une logique répressive mais aussi préventive. En effet, elle survenait à la suite de l'assaut au Capitole à Washington le 6 janvier 2021 pour contester l'élection de Joe Biden. L'ancien président Donald Trump est alors soupçonné d'avoir incité les émeutiers d'entrer de façon illicite dans le capitole à travers des discours vidéo et des contenus écrit publiés sur ses comptes personnels dans les réseaux sociaux. Voir : V-L BENABOU, *Bannir l'ex-président des Etats-Unis d'un réseau social. So what ?*, Le Club des juristes, 6 juillet 2021. Disponible sur : https://blog.leclubdesjuristes.com/bannir-ex-president-etats-unis-reseau-social-facebook-so-what/

périodes particuliers, comme pendant des élections électorales où Facebook a été soupçonné de manipuler les sujets en tendance dans son réseau[900].

Conclusion du Chapitre V

428. Les mesures préventives devraient être au cœur de la lutte contre les cyberviolences. Aujourd'hui nous constatons l'existence d'une multiplicité de mesures éducatives et de sensibilisation dont les effets sont peu mesurables.

Des mesures techniques préventives existent et devrait être développées en faisant attention au respect des droits fondamentaux des individus. En effet, leur utilisation est souvent pointée du doigt à cause des risques identifiés allant à l'encontre des droits des utilisateurs. Enfin, malgré l'engagement du secteur privé et, en particulier, des plateformes leurs mesures restent insuffisantes et, dans certains États, leur action préventive entraine des atteintes graves aux droits et libertés des populations.

[900] *USA : Zuckerberg défend la neutralité de Facebook*, Le Figaro, 13 mai 2016. Disponible sur : https://www.lefigaro.fr/flash-eco/2016/05/13/97002-20160513FILWWW00130-usa-zuckerberg-defend-la-neutralite-de-facebook.php?web=1&wdLOR=c44E89EFB-D390-4A48-A064-7186343A1CDA

Chapitre VI : La nécessaire amélioration de la prévention, dernier rempart contre les cyberviolences

429. Aujourd'hui face à la multiplication des atteintes sur Internet, nous constatons que les mesures préventives existantes sont insuffisantes et que leurs effets sont mitigés. Pour contenir le phénomène des cyberviolences, il est nécessaire de repenser ces mesures et le rôle des acteurs engagés. Mais également de se fonder sur le système existant pour les rendre plus efficaces.

430. À cet égard, il s'agira, d'une part, d'analyser la possibilité de mieux responsabiliser les plateformes qui jouissent aujourd'hui d'un système de responsabilité allégé **(Section I)**. D'autre part, d'étudier la possibilité de renforcer et consolider les mesures préventives existantes **(Section II)**.

Section I : L'amélioration de la prévention par la responsabilisation des plateformes

431. Au sein de l'Union européenne, lors de l'essor des plateformes, les autorités de régulation avaient privilégié l'expansion des acteurs et activités numériques en prévoyant un régime de responsabilité allégé. Cependant, avec le développement rapide du commerce électronique, la multiplication des plateformes et des contenus partagés, ainsi que face au problème de la régulation des activités numériques et des contenus illicites, les autorités ont changé progressivement leur positionnement.

432. Dans les développements qui vont suivre, d'une part, nous analyserons le régime de responsabilité allégé des plateformes **(§I)** et, d'autre part, nous étudierons le renforcement progressif de la responsabilité **(§II).**

I. L'inefficacité de la prévention du fait de la responsabilité « allégée » des plateformes

433. Il est nécessaire de revenir sur la distinction entre les hébergeurs des contenus et les éditeurs. En premier lieu, les hébergeurs ont été définis dans la 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 et, en France, par l'article 6-I-2 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, comme des entités 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 les destinataires de ces services »[901]. Selon la Cour de justice de l'Union européenne, le statut d'hébergeur s'applique lorsque le prestataire d'un service ne joue pas « un rôle actif de nature à lui confier une connaissance ou un contrôle des données stockées »[902]. En second lieu, les éditeurs sont définis par la même loi à l'article 6-III-1 comme « les personnes dont l'activité est d'éditer un service de communication au public en ligne »[903]. Alors que l'hébergeur rend seulement accessible des contenus conçus par des tiers sans y avoir un rôle actif, l'éditeur a un véritable rôle actif sur les contenus qu'il publie en ligne. Cette différence entraîne une diversité des régimes de responsabilité. L'éditeur pourra voir sa responsabilité engagée pour tout type de contenu[904]. Au contraire, l'hébergeur n'est responsable ni civilement ni pénalement, sauf s'il avait connaissance du caractère illicite du contenu et qu'il n'a pas agi promptement pour le retirer ou rendre son accès impossible[905].

434. Dans les développements qui vont suivre, il s'agira d'analyser le régime allégé de responsabilité des plateformes (**A**) pour ensuite étudier les mesures insuffisantes de modération adoptées par ces dernières (**B**).

---

[901] Article 6-I-2 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[902] CJUE, GC, 23 mars 2010, *Sté Google c/ Sté Louis Vuitton Malletier*, affaires C-236/08 à C-238/08, point 120.
[903] Article 6-III-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[904] *Ibid*. article 6-I-3.
[905] *Ibid*. articles 6-I-2 et 6-I-3.

A. Le régime de responsabilité allégé des plateformes

435. Au début de la réflexion et de la production législative concernant Internet, le législateur européen avait assuré un statut favorable aux plateformes. La 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 en est un exemple. En effet, elle instaure un régime spécial de responsabilité des plateformes qui, originairement, avait été prévu pendant les années 2000 pour faciliter le développement d'Internet. La directive prévoit, entre autres, la prohibition pour les États membres de l'Union européenne d'imposer aux plateformes une obligation générale de surveillance des contenus ou de rechercher activement des faits illicites[906]. Ainsi, elle envisage la possibilité pour les États membres d'imposer aux plateformes une obligation de coopérer avec les autorités[907]. Grâce à ce régime d'irresponsabilité, les représentants des plateformes ont toujours plaidé pour être définis comme des hébergeurs, cela afin d'éviter d'être considérés responsables des contenus illicites publiés. On compte tout de même certaines exceptions, par exemple, lorsqu'en avril 2018, Mark Zuckerberg, PDG de Meta, lors d'une audition devant le Congrès américain a déclaré que Facebook était responsable des contenus mis en ligne[908]. Cependant, l'approche vis-à-vis de la responsabilité des plateformes est en train de changer, en particulier après l'adoption des règles spéciales applicables au droit d'auteur qui ouvrent une brèche à ce régime d'irresponsabilité[909] ainsi qu'aux obligations réservées aux plateformes par le règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (« Digital Services Act »)[910], notamment en matière de retrait de contenus illicites. Responsabiliser plus les plateformes pourrait permettre un

---

[906] Article 15 (1) de la 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.
[907] *Ibid.* article 15 (2).
[908] The Washington Post, *Transcript of Mark Zuckerberg's Senate hearing*, 11 avril 2018. Disponible sur : https://www.washingtonpost.com/news/the- switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/
[909] Voir : C. CASTETS-RENARD, *Droit du marché unique numérique et intelligence artificielle*, Bruxelles, Bruylant, 1e édition, 2020, p. 116.
[910] Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

plus grand engagement de leur part pour prévenir les violences en ligne en renforçant les instruments à leur portée.

B. Les mesures insuffisantes de modération des plateformes

436. Après avoir traité la question de la responsabilité, il est intéressant d'analyser la question des modérateurs. En effet, c'est un sujet crucial en matière de modération *a priori* et *a posteriori* de la publication des contenus. La modération peut se faire *ex ante,* c'est-à-dire avant la publication des contenus ou *ex post,* c'est-à-dire une fois que les contenus sont accessibles aux utilisateurs de la plateforme. De plus, dans la modération *a posteriori* on peut parler de filtrage réactif, lorsque les contenus estimés illicites sont signalés par les utilisateurs ou proactif lorsque les contenus sont identifiés et filtrés par les modérateurs eux-mêmes ou par des outils automatiques[911]. La modération peut être menée par des êtres humains, par des outils d'intelligence artificielle ou bien de façon hybride (à la fois par des êtres humains et par l'intelligence artificielle).

437. Avant de procéder à l'analyse de l'encadrement du travail de modération, il faut expliquer en quoi il consiste. Il comprend l'analyse des contenus publiés sur le réseau social, c'est-à-dire les images, les vidéos et les files audio, afin de les retirer lorsqu'ils enfreignent la loi ou les règles de la plateforme. Le Digital Services Act définit la « modération des contenus » comme : « les activités, qu'elles soient automatisées ou non, entreprises par des fournisseurs de services intermédiaires qui sont destinées, en particulier, à détecter et à identifier les contenus illicites ou les informations incompatibles avec leurs conditions générales, fournis par les destinataires du service, et à lutter contre ces contenus ou ces informations, y compris les mesures prises qui ont une incidence sur la disponibilité, la visibilité et l'accessibilité de ces contenus ou ces informations, telles que leur rétrogradation, leur démonétisation, le fait de rendre l'accès à ceux-ci impossible ou leur retrait, ou qui ont une incidence sur la capacité des destinataires du service à fournir ces informations, telles que la suppression ou la

[911] G. SARTOR, A. LOREGGIA, *The impact of algorithms for online content filtering or moderation,* Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament, September 2020, p. 21.

suspension du compte d'un destinataire »[912]. Au vu de ces éléments, les modérateurs sont exposés tout au long de leur journée de travail à un très grand volume de contenus violents, agressifs, à caractère sexuel mais également racistes ou complotistes.

438. Plusieurs constats sont à exposer. Premièrement, il faut souligner qu'il n'existe pas une obligation pour les plateformes d'employer un nombre minimum de modérateurs. Cela pose des problèmes lorsqu'on constate que certaines plateformes disposent d'un très faible nombre de modérateurs comparé au nombre de personnes inscrites et actives. En effet, selon le document transmis par Facebook au Conseil supérieur de l'audiovisuel (CSA)[913] en 2020, il y aurait environ 15 000 modérateurs pour les 2,9 milliards d'utilisateurs mensuels dans le monde. C'est-à-dire, un modérateur pour 190.000 utilisateurs[914]. D'après la publication des documents internes de Facebook par la lanceuse d'alerte Frances Haugen, il y aurait environ 766 modérateurs qui s'occupent de la modération manuelle de contenus publiés pour les 220 millions d'utilisateurs en langue arabe[915]. Ainsi, et comme nous l'avions exposé également dans les développements précédents, les dépenses et investissements pour la modération ne sont pas les mêmes d'une langue à l'autre. Comme le souligne le journal Le Monde après avoir eu accès aux documents internes de Facebook : « sur une semaine, en août 2019, les dépenses de modération humaine des contenus haineux ont été consacrées à 37,7 % à l'anglais américain, loin devant l'espagnol (4,8 %) ou le portugais (4,7 %) »[916]. Twitter,

---

[912] Article 3 (t) du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

[913] Voir les questionnaires de Facebook et Twitter soumis conformément au titre III de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information au Conseil supérieur de l'audiovisuel pour son premier bilan. CSA, Bilan des mesures de lutte contre la manipulation de l'information sur les plateformes en ligne mises en œuvre en 2020, 2021. Disponibles ici : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Lutte-contre-les-infox-le-CSA-publie-son-premier-bilan

[914] Voir le questionnaire aux opérateurs de plateformes en ligne soumis conformément au titre III de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. CSA, Bilan des mesures de lutte contre la manipulation de l'information sur les plateformes en ligne mises en œuvre en 2020, 2021. Disponible ici : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Lutte-contre-la-manipulation-de-l-information-le-CSA-publie-le-bilan-des-mesures-mises-en-oeuvre-par-les-plateformes-en-ligne-en-2020

[915] M. UNTERSINGER et D. LELOUP, *Pour modérer 220 millions d'utilisateurs en langue arabe, Facebook n'emploie que 766 modérateurs,* Le Monde, publié le 16 novembre 2021. Disponible sur : https://www.lemonde.fr/pixels/article/2021/11/16/facebook-emploie-766-moderateurs-en-langue-arabe-pour-220-millions-d-utilisateurs-arabophones_6102312_4408996.html

[916] A. PIQUARD, *Facebook hors des États-Unis : les failles d'une tour de Babel,* Le Monde, 26 octobre 2021. Disponible sur : https://www.lemonde.fr/pixels/article/2021/10/25/facebook-hors-des-etats-unis-les-failles-d-une-tour-de-babel-face-aux-discours-de-haine_6099809_4408996.html

selon les informations partagées avec le Conseil supérieur de l'audiovisuel[917], employait en 2020 seulement 1867 modérateurs pour environ 152 millions d'utilisateurs actifs en 2019[918]. La plateforme justifie ce faible nombre en disant que la modération à grande échelle ne peut pas être assurée seulement avec des moyens humains et c'est pour cela qu'elle investit le plus sur la technologie et l'intelligence artificielle. Les modérateurs représentent plus d'un tiers des effectifs de Twitter, mais cela reste dérisoire compte tenu du nombre de contenus publiés chaque jour sur le réseau, 500 millions environ[919], et du nombre d'utilisateurs. Nous pouvons également souligner la création de l'initiative « BlueSky »[920] et financé à la hauteur de 13 millions par Twitter en décembre 2019. Le but de cette initiative est de développer des normes décentralisées adaptées à l'ensemble des plateformes afin de modérer les contenus. Une sorte de protocole décentralisé à appliquer pour la modération des contenus. Le projet a été ouvert sous liste d'attente à un certain nombre d'internautes intéressés pour tester la version beta. En deux jours, plus de 30 000 personnes se sont inscrites. Depuis avril 2023 elle a été lancé sur Android et le téléchargement est possible seulement sur invitation.

En somme, la modération humaine n'est qu'une faible partie de la modération, en raison du fait qu'elle est le plus souvent automatisée.

439. Deuxièmement, il n'y a pas une réglementation pour assurer un cadre de travail respectueux des droits des modérateurs. En effet, ces derniers sont pour la plupart embauchés par des entreprises sous-traitantes[921] basées souvent dans des États à faible revenus dépourvus d'un cadre juridique protecteur en matière de droits sociaux. Cela complique la modération et expose les travailleurs à des conditions de travail difficiles et peu protectrices de leur santé mentale et physique. D'une part, concernant la complexification de la modération, le Rapporteur spécial sur la promotion et la protection

---

[917] Voir le questionnaire de Twitter soumis conformément au titre III de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information au Conseil supérieur de l'audiovisuel pour son premier bilan, p.12. CSA, Bilan des mesures de lutte contre la manipulation de l'information sur les plateformes en ligne mises en œuvre en 2020, 2021. Disponibles ici : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Lutte-contre-les-infox-le-CSA-publie-son-premier-bilan

[918] *Ibid.* p. 1.

[919] Voir le site « Internet live stats » et, en particulier, les « Twitter usage statistics ». Disponible sur : https://www.internetlivestats.com/twitter-statistics/

[920] J. GRABER, G. VELEZ, *How it Started*, Bluesky blog, 28 février 2022. Disponible sur https://blueskyweb.xyz/blog/2-28-2022-how-it-started

[921] Par exemple les entreprises Accenture, Cognizant et Covalen.

du droit à la liberté d'opinion et d'expression avait souligné en 2016 que « certaines grandes plateformes externalisent la modération des contenus, ce qui accroît encore la distance entre les modérateurs de contenus et les décideurs en interne, et exacerbe les incohérences dans l'application des décisions. Les intermédiaires qui opèrent sur des marchés divers font inévitablement face à des « jugements de valeur complexes », à des problèmes dus à la diversité des sensibilités culturelles et à la « difficulté de trancher face aux conflits de lois »[922]. Ainsi, on pourrait également ajouter la difficulté de la langue. D'autre part, les modérateurs ne reçoivent pas une protection adéquate face à la pénibilité de leur travail. En effet, à part l'exposition de contenus extrêmement violents, ils sont soumis à des rythmes stressants et à des contrôles de performance très stricts[923]. Cela en étant sous-payés, en particulier dans certains États européens, comme l'Ukraine[924], ou dans des États à faible revenus comme le Kenya[925] où une plainte a été déposé par un ancien modérateur contre Meta et la société sous-traitante « Sama » à cause des conditions de travail et des méthodes de recrutement trompeuses[926].

440. Les conséquences néfastes de cette activité sur les modérateurs ont été prouvées, en particulier le développement du syndrome du stress post-traumatique[927]. À cet égard,

---

[922] Conseil des droits de l'Homme, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 11 mai 2016, A/HRC/32/38, point 54.

[923] D. GILBERT, *Les conditions de travail infernales des modérateurs de Facebook,* Vice, 21 janvier 2020. Disponible sur : https://www.vice.com/fr/article/z3beea/les-conditions-de-travail-infernales-des-moderateurs-de-facebook

[924] D. ANTONIUK, *Ukrainian content moderators among Facebook's lowest paid workers,* The Kyiv post, 25 octobre 2021. Disponible sur : https://www.kyivpost.com/technology/ukrainian-content-moderators-among-facebooks-lowest-paid-workers.html. Voir également : E. ROTH, *Facebook content moderators protest low wages with mobile billboard*, The Verge, 19 octobre 2021. Disponible sur : https://www.theverge.com/2021/10/19/22726915/facebook-content-moderators-protest-low-wages

[925] Suite, très probablement, à une enquête publiée par le journal Time (voir note 25) qui pointe du doigt les conditions de travail pénibles des modérateurs de Meta basés au Kenya et notamment du faible niveau de rémunération par rapport aux modérateurs basés aux États-Unis et en Europe, Meta a augmenté leur salaire de 30% à 50%. Cependant ces derniers demeurent parmi les moins bien rémunérés par la plateforme dans le monde. Voir : B. PERRIGO, *Facebook Content Moderators in Kenya to Receive Pay Rise Following TIME Investigation*, Time, 2 mars 2022. Disponible sur : https://time.com/6153778/facebook-moderators-kenya-sama/

[926] B. PERRIGO, *Inside Facebook's African Sweatshop*, Time, 2 mars 2022. Disponible sur : https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/

[927] C. NEWTON, *The terror queue,* The Verge, 16 décembre 2019. Disponible sur : https://www.theverge.com/2019/12/16/21021005/google-youtube-moderators-ptsd-accenture-violent-disturbing-content-interviews-video. Voir également : C. NEWTON, *Half of all Facebook moderators may develop mental health issues*, The Verge, 13 mai 2020. Disponible sur : https://www.theverge.com/interface/2020/5/13/21255994/facebook-content-moderator-lawsuit-settlement-mental-health-issues

Meta, en 2021, suite à une action en justice de groupe menée par une salariée, a été condamné à payer 52 millions de dollars à ses modérateurs qui ont eu des conséquences psychologiques graves après avoir modéré des contenus de la plateforme[928]. Ce problème ne concerne pas seulement Meta, mais également d'autres plateformes comme TikTok. En 2022, une plainte a été déposée contre ce dernier et sa maison mère ByteDance[929] par deux modératrices, en cause : l'exposition à des contenus très violents et l'absence de protection de la plateforme vis-à-vis d'elles.

441. La modération humaine nécessite la prise en charge de la sécurité et de la santé des modérateurs. Ce besoin existe également parmi les professionnels étatiques, comme les agents de police[930]. La question qu'on pourrait se poser est celle de savoir si les plateformes, ainsi que les autorités de contrôle, pourraient se passer de modérateurs humains. Pour le moment, la réponse est non. Car les plateformes qui font usage pour la plupart d'outils d'intelligence artificielle, comme Twitter, nous montrent que la seule modération automatique ne fonctionne pas. En effet, les logiciels ne sont pas assez performants et il faudrait attendre encore des années pour pouvoir les rendre plus efficaces. Nous verrons qu'une solution intermédiaire serait celle de faciliter et développer la modération hybride, c'est-à-dire celle opérée à la fois par les êtres humains et l'intelligence artificielle.

---

[928] Voir : Superior court of the State of California, *Selena Scola v. Facebook*, Case No. 18-civ-05135 et l'accord signé par Facebook. Disponible sur : https://s3.documentcloud.org/documents/6889329/Facebook-Settlement.pdf

[929] United States District Court, Northern District of California, *Reece Young and Ashley Velez v. ByteDance Inc. And TikTok Inc.*, 24 mars 2022, case n° 3:22-cv-01883. Disponible sur : https://www.documentcloud.org/documents/21508707-reece-young-and-ashley-velez-v-bytedance. Voir également : B. ALLYN, *Former TikTok moderators sue over emotional toll of 'extremely disturbing' videos*, NPR, 24 mars 2022. Disponible sur : https://www.npr.org/2022/03/24/1088343332/tiktok-lawsuit-content-moderators?t=1648220484526

[930] *« C'est impressionnant » : le nombre de signalements pour pédopornographie et terrorisme en ligne s'envole,* Le Parisien avec AFP, 4 juin 2022. Disponible sur : https://www-leparisien-fr.cdn.ampproject.org/c/s/www.leparisien.fr/amp/faits-divers/cest-impressionnant-le-nombre-de-signalements-pour-pedopornographie-et-terrorisme-en-ligne-senvole-04-06-2022-EBBYLO6V6VHKJL6CW4F6EKEBD4.php

II. Le renforcement progressif de la responsabilité des plateformes

« Un comportement responsable et diligent des fournisseurs de services intermédiaires est indispensable pour assurer un environnement en ligne sûr, prévisible et de confiance pour permettre aux citoyens de l'Union et aux autres personnes d'exercer leurs droits fondamentaux garantis par la charte des droits fondamentaux de l'Union européenne, en particulier la liberté d'expression et d'information et la liberté d'entreprise, le droit à la non-discrimination et la garantie d'un niveau élevé de protection des consommateurs »[931].

442. La 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 e-commerce) avait instauré un régime d'irresponsabilité pour les plateformes d'hébergement. Toutefois un mouvement de responsabilisation a commencé à s'instaurer à travers des projets de loi, la jurisprudence et des nouvelles dispositions juridiques que cela soit au sein des droits nationaux ou en droit de l'Union européenne.

443. Dans les développements qui vont suivre, il s'agira d'étudier le renforcement des obligations des hébergeurs (**A**) pour ensuite approfondir la question de la nomination d'un représentant légal des plateformes hors de leur État de domiciliation (**B**).

A. Le renforcement des obligations des hébergeurs

444. D'abord, nous constatons un renforcement dans le droit national. La loi allemande Netzwerkdurchsetzungsgesetz (NetzDG) adoptée le 1er septembre 2017 en est un exemple. Elle avait été l'une des premières lois à prévoir des mesures plus strictes pour les hébergeurs, en particulier l'obligation de retirer des contenus manifestement illicites sous 24 heures. Cette loi a été reprise par plusieurs États qui l'ont érigée comme un modèle, et comme un instrument, pour plusieurs d'entre eux, de restriction de la liberté

[931] Considérant 3 du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

d'expression sur les réseaux sociaux[932]. Il s'agit d'États démocratiques, comme la France ou l'Australie, ou autoritaires comme le Venezuela, qui a adopté en 2017 une loi contre la haine, pour la tolérance et la coexistence pacifique[933]. Cette dernière est beaucoup plus restrictive que la loi allemande car elle a un champ d'application plus large : elle prévoit l'obligation pour plateformes de retirer les contenus haineux dans un délai de 6 heures[934] et utilise un langage vague qui pourrait permettre une atteinte à la liberté d'expression, notamment des dissidents politiques[935]. En Australie, après l'attentat terroriste de Christchurch[936], une loi a été adoptée en 2019 pour amender le Code pénal[937]. Cette dernière prévoit des mesures pour responsabiliser les hébergeurs. En particulier, elle crée de nouvelles infractions pénales vis-à-vis des plateformes qui n'assurent pas le retrait rapide ou ne cessent pas « expeditiously » (en français « rapidement ») d'héberger un « abhorrent violent matériel »[938] (en français « matériel violent odieux »). Cependant, cette loi a été fortement critiquée. En effet, elle a été adoptée sans prendre en compte les avis des juristes et experts. Par exemple, David Kaye, rapporteur spécial des Nations unies pour la promotion et la protection du droit à la liberté d'expression et Fionnuala Ni Aoláin, rapporteuse spéciale sur la promotion et la protection des droits humains et des libertés fondamentales dans la lutte contre le terrorisme, ont écrit un courriel[939] au

---

[932] Consulter la liste exhaustive d'États sur : J. MCHANGAMA et J. FISS, The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship, Justitia, novembre 2019.

[933] Ley Constitucional Contra el Odio, por la Convivencia Pacífica y la Tolerancia, Gaceta Oficial N° 41.274, 9 novembre 2017. Disponible sur : https://finanzasdigital.com/2017/11/gaceta-oficial-n-41-274-ley-constitucional-odio-la-convivencia-pacifica-la-tolerancia/

[934] Article 22 de la Ley Constitucional Contra el Odio, por la Convivencia Pacífica y la Tolerancia, Gaceta Oficial N° 41.274, 9 novembre 2017. Disponible sur : https://finanzasdigital.com/2017/11/gaceta-oficial-n-41-274-ley-constitucional-odio-la-convivencia-pacifica-la-tolerancia/

[935] J. MCHANGAMA et J. FISS, The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship, Justitia, novembre 2019.

[936] Voir §410 de cette thèse.

[937] Voir : Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019. Disponible sur : https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1201_first-senate/toc_pdf/1908121.pdf;fileType=application%2Fpdf

[938] Voir §474.34 de la nouvelle législation. Voir : https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1201_first-senate/toc_pdf/1908121.pdf;fileType=application%2Fpdf

[939] Rapporteur spécial des Nations Unies pour la promotion et la protection du droit à la liberté d'expression et rapporteuse spéciale sur la promotion et la protection des droits humains et des libertés fondamentales dans la lutte contre le terrorisme, *Amendment to the Criminal Code on Sharing of Abhorrent Violent Content*, 4 avril 2019. Disponible sur : https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24533

gouvernement australien. Dans ce message, ils avaient communiqué leur souhait de transmettre des commentaires sur le projet de loi, mais ce dernier avait déjà été adopté avant qu'ils n'en aient eu l'occasion[940]. Dans cette lettre, les deux rapporteurs expriment leurs craintes face au terme « expeditiously » et à la définition de « terrorist act » et « abhorrent violent material ». En premier lieu, concernant le retrait rapide des contenus, selon eux, la loi n'est pas très précise sur les délais offerts aux plateformes pour réagir. Ainsi, l'instauration de délais courts aurait des conséquences négatives sur la liberté d'expression. En effet, l'obligation des plateformes de retirer les contenus dans des délais très courts ne donnerait pas assez de temps à ces dernières pour analyser les contenus signalés, ce qui pourrait mener à un excès de prudence et à l'effacement de contenus licites. En second lieu, concernant la définition de « terrorist act » et « abhorrent violent material », les deux rapporteurs soulignent que ces nouvelles dispositions exacerbent une incertitude juridique. Par exemple, ils mettent en garde sur le fait que certains contenus qui pourraient sembler haineux pourraient être des reportages sur des actes violents ou simplement des œuvres artistiques.

445. Ces lois montrent une volonté étatique qui vise à responsabiliser les plateformes dans le retrait des contenus illicites, en leur donnant aussi beaucoup de pouvoir au niveau de la prise de décision et, par conséquent, en entraînant, si les mesures sont trop restrictives, un risque d'atteinte aux droits fondamentaux des utilisateurs.

446. Nous avons assisté à cette responsabilisation également à travers la jurisprudence, par exemple, dans l'arrêt *Ireland Limited c. Eva Glawischnig-Piesczek*[941]. La Cour de justice de l'Union européenne a atténué les obligations de l'article 15 de la directive e-commerce[942] en estimant qu'il est légitime que la juridiction compétente puisse exiger

[940] E. DOUEK, *Australia's New Social Media Law Is a Mess*, Lawfare, 10 avril 2019. Disponible sur : https://www.lawfareblog.com/australias-new-social-media-law-mess
[941] CJUE, 3 octobre 2019, *Glawischnig-Piesczek v. Facebook Ireland*, aff. C-18/18.
[942] 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.

de l'hébergeur « qu'il bloque l'accès aux informations stockées, dont le contenu est identique à celui déclaré illicite antérieurement, ou qu'il retire ces informations »[943].

447. Cette tendance est confirmée par l'adoption du règlement 2021/784 du Parlement européen et du Conseil, du 29 avril 2021, relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne. Ce dernier prévoit l'obligation pour les fournisseurs de service d'hébergement de retirer des contenus à caractère terroriste ou en bloquer l'accès dans un délai d'une heure à compter de la réception de l'injonction[944]. De plus, le règlement impose aux plateformes d'adopter des mesures spécifiques pour « protéger ses services contre la diffusion au public de contenus à caractère terroriste »[945], parmi lesquelles : des mesures techniques pour identifier et retirer promptement le contenu. Par exemple des filtres, des algorithmes ou des systèmes facilités de signalement[946]. La responsabilisation est également confirmée par l'adoption du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE[947] qui prévoit plusieurs dispositions à destination des plateformes pour lutter contre le partage de contenus illicites en ligne. D'abord, il faut souligner que le règlement ne modifie pas la règle fixée par l'article 15 de la directive 2000/31/CE du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique concernant l'obligation générale de surveillance[948]. En effet, l'article 8 du règlement dispose que « les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent ou de rechercher activement des faits ou des circonstances révélant des activités illégales »[949]. Ainsi, le nouveau règlement prévoit plusieurs injonctions à agir contre les contenus

---

[943] CJUE, 3 octobre 2019, *Glawischnig-Piesczek v. Facebook Ireland*, aff. C-18/18, point 37.
[944] Article 3, paragraphe 3, du règlement 2021/784 du Parlement européen et du Conseil relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, 17 mai 2021.
[945] *Ibid.* article 5.
[946] Voir F. DUBUISSON, J. PIERET, Société de l'information, médias et liberté d'expression, *JEDH*, 2021/4-5, p. 369.
[947] Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[948] Article 15 de la 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.
[949] Article 8 du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

illicites. Par exemple, l'article 9 dispose que le fournisseur qui reçoit une injonction d'agir contre un ou plusieurs contenus illicites doit informer l'autorité qui a émis l'injonction dans les meilleurs délais concernant les suites données à cette dernière[950]. L'article 18 prévoit également la notification des soupçons d'infraction pénale aux services répressifs et judiciaires de l'État membre ou des États membres concernés des soupçons d'infraction pénale[951]. Enfin, l'article 34 dispose que « les fournisseurs de très grandes plateformes en ligne[952] et de très grands moteurs de recherche en ligne recensent, analysent et évaluent de manière diligente tout risque systémique au sein de l'Union découlant de la conception ou du fonctionnement de leurs services et de leurs systèmes connexes, y compris des systèmes algorithmiques, ou de l'utilisation faite de leurs services » [953].

Cela comprend, entre autres, les risques liés à la diffusion de contenus illicites, ainsi que tout effet négatif avéré ou prévisible pour l'exercice des droits fondamentaux et lié aux violences sexistes, à la protection de la santé publique et des mineurs[954].

Le règlement instaure un régime hybride qui, d'un part, soumet les plateformes à des mécanismes de contrôle mises en œuvre par l'Union européenne et les États membres ; et, de l'autre, responsabilise les acteurs privés qui devront trancher si un contenu est licite ou non à la suite de signalements d'utilisateurs, de « signaleurs certifiés » et d'autorités publiques[955].

Le règlement, comme souligne l'ONG Reporters sans frontières, marque la fin de l'« irresponsabilité de principe » des plateformes. En effet, elles devront identifier et

---

[950] *Ibid.* article 9.
[951] L'article 18, paragraphe 1, du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE dispose que « Lorsqu'un fournisseur de services d'hébergement a connaissance d'informations conduisant à soupçonner qu'une infraction pénale présentant une menace pour la vie ou la sécurité d'une ou de plusieurs personnes a été commise, est en train d'être commise ou est susceptible d'être commise, il informe promptement les autorités répressives ou judiciaires de l'État membre ou des États membres concernés de son soupçon et fournit toutes les informations pertinentes disponibles ».
[952] Il s'agit des plateformes qui ont plus de 45 millions d'utilisateurs, par exemple Meta, Twitter ou YouTube.
[953] *Ibid.* article 34, paragraphe 1.
[954] Voir l'article 34, paragraphe 1, b) et c) du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE
[955] Voir : F. DUBUISSON, J. PIERET, Société de l'information, médias et liberté d'expression, *JEDH*, 2021/4-5, p. 369.

évaluer l'impact de leurs activités en particulier sur les droits fondamentaux[956]. Il est important de souligner que la responsabilisation des plateformes peut avoir des avantages liés à un meilleur traitement des comportements illicites et aussi des inconvénients. Dans les États autoritaires, elle peut être synonyme de censure et de poursuite des dissidents politiques. Dans les États démocratiques, il y a également des risques avérés, comme nous l'avons vu précédemment avec l'application de la loi NetzDG, d'atteinte à la liberté d'expression. Avoir un règlement comme le Digital Services Act permet une application uniforme des dispositions au sein de l'Union européenne et une garantie minimale d'engagement des plateformes vis-à-vis des atteintes aux utilisateurs. Les droits fondamentaux sont omniprésents dans le texte du règlement et au centre de la réflexion[957].

B. La nécessité de nommer un représentant légal des plateformes d'hébergement hors de leur État de domiciliation

448. Les plus grandes plateformes sont basées aux États-Unis (par exemple : Facebook et Instagram) et en Chine (par exemple : TikTok). Pour les responsabiliser et faciliter les échanges avec les filiales implantées dans l'ensemble des États, il serait nécessaire de nommer un représentant légal pour chaque plateforme.

449. Selon la section 5 (1) loi allemande NetzDG « les fournisseurs de réseaux sociaux sont tenus de désigner immédiatement une personne [qui puisse] être assignée dans le cadre des procédures visées à l'article 4 ou dans le cadre d'une procédure judiciaire devant les tribunaux allemands pour diffusion de contenus illicites. Il en va de même pour la signification ou la notification des actes introductifs d'instance. »[958]. Ainsi, la

---

[956] Voir : Reporters Sans Frontières, *Digital Services Act : RSF se félicite de la reprise de ses propositions et appelle à poursuivre l'effort*, 9 mai 2022. Disponible sur https://rsf.org/fr/digital-services-act-rsf-se-f%C3%A9licite-de-la-reprise-de-ses-propositions-et-appelle-%C3%A0-poursuivre-l

[957] Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

[958] Traduction libre de l'autrice. Version en anglais de la section 5 (1) de la loi Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG) du 1er septembre 2017 : « Providers of social networks shall immediately name a person authorised to receive service in the Federal Republic of Germany and shall draw attention to this fact on their platform in an easily recognisable and directly accessible manner. It shall be possible to effect

section 5 (2) prévoit également que « afin de permettre la réception de demandes d'informations de la part des autorités répressives allemandes, il convient de désigner une personne en République fédérale d'Allemagne qui est autorisée à recevoir de telles demandes »[959].

450. Plusieurs États ont suivi l'exemple allemand et ont adopté, ou essayer d'adopter, des lois nationales qui prévoient la désignation d'un représentant national pour faciliter les échanges avec les plateformes et notamment effectuer les réquisitions judiciaires plus efficacement. En France, la proposition de loi visant à lutter contre les contenus haineux sur Internet (dite Avia) prévoyait de désigner « une personne physique située sur le territoire français exerçant les fonctions d'interlocuteur référent chargé de recevoir les demandes de l'autorité judiciaire […] et les demandes du Conseil supérieur de l'audiovisuel […] »[960]. Toutefois, cette disposition a été censurée par le Conseil constitutionnel en raison de la contrariété avec la Constitution française, comme la plupart des dispositions de la proposition de loi. Le Conseil d'État avait également commenté cette proposition dans un avis du 16 mai 2019 en disant que « des précisions quant au rôle attendu de ce représentant légal paraissent nécessaires »[961]. Cependant, la même disposition avait été adoptée en 2018 par la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information qui prévoit la désignation d'un représentant légal exerçant les fonctions d'interlocuteur référent sur le territoire français[962]. La Turquie, toujours en prenant l'exemple de la loi allemande NetzDG, a

---

service on this person in procedures pursuant to section 4 or in judicial proceedings before German courts on account of the dissemination of unlawful content. The same shall also apply to the service of documents initiating such proceedings ».

[959] Traduction libre de l'autrice. Version en anglais de la section 5 (1) de la loi Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG) du 1er septembre 2017 : « To enable the receipt of requests for information from German law enforcement authorities, a person in the Federal Republic of Germany shall be named who is authorised to receive such requests. The person so authorised shall be obliged to respond to such requests for information pursuant to the first sentence within 48 hours of receipt. In cases where the requested information is not exhaustively provided, reasons for this shall be included in the response. »

[960] Article 5, 10, de la proposition de loi visant à lutter contre les contenus haineux sur Internet adoptée par l'Assemblée nationale le 13 mai 2020. Disponible sur : https://www.assemblee-nationale.fr/dyn/15/textes/l15t0419_texte-adopte-seance

[961] Conseil d'État, Avis sur la proposition de loi visant à lutter contre les contenus haineux sur Internet, 16 mai 2019. Disponible sur : https://www.conseil-etat.fr/avis-consultatifs/derniers-avis-rendus/a-l-assemblee-nationale-et-au-senat/avis-sur-la-proposition-de-loi-visant-a-lutter-contre-la-haine-sur-internet

[962] Voir l'article 13 de la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

adopté un amendement en juillet 2020 à la loi n° 5651 nommée « the Law on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts » en incluant plusieurs obligations pour les plateformes de réseaux sociaux ayant plus d'un million d'utilisateurs par jour en Turquie. L'une d'entre elles prévoit la désignation d'un représentant légal habitant en Turquie[963].

451. En droit de l'Union européenne, la proposition de règlement relatif à un marché unique des services numériques prévoit des dispositions concernant la nomination et les devoirs des représentants légaux. L'article 11, paragraphe 1, du règlement prévoit que « les fournisseurs de services intermédiaires qui n'ont pas d'établissement au sein de l'Union, mais qui proposent des services dans l'Union désignent, par écrit, une personne morale ou physique pour agir comme leur représentant légal dans un des États membres dans lequel le fournisseur propose ses services »[964]. Ce qui est à souligner est que, l'article 13, prévoit, non seulement que le représentant légal sera chargé de répondre aux questions des autorités des États membres, de la Commission et du Comité concernant le respect et la mise en œuvre du règlement[965]. Mais également, que ce dernier « *peut être tenu pour responsable du non-respect des obligations prévues dans le présent règlement,* sans préjudice de la responsabilité du fournisseur de services intermédiaires et des actions en justice qui pourraient être intentées contre lui »[966].

452. Cette disposition est très importante car elle permettrait aux plateformes de ne pas se déresponsabiliser et d'avoir une pression supplémentaire, en particulier pour superviser la mise en œuvre du règlement et l'effectivité d'éventuelles sanctions[967].

---

[963] O. ÇETINKAYA, A. GÜNGÖRDÜ, *When national laws and international standards are at odds: human rights responsibilities of social media platforms under Turkey's new internet law,* International Bar Association, 2021. Disponible sur : https://www.ibanet.org/human-rights-responsibilities-of-social-media-platforms-under-Turkey-new-internet-law

[964] Article 13, paragraphe 1, du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

[965] *Ibid. a*rticle 13, paragraphe 2.

[966] *Ibid. a*rticle 13, paragraphe 3.

[967] Voir : M-E. ANCEL, « Un an de droit international privé du commerce électronique », *Communication, commerce électronique,* LexisNexis, n°1, janvier 2021, p. 2.

Section II : L'amélioration de la prévention par le renforcement juridique et politique

453. Après avoir analysé la responsabilisation des plateformes, il est intéressant de montrer que, d'un côté, le renforcement de la prévention pourrait se faire avec la ratification d'instruments juridiques existants qui permettraient l'adoption des mesures préventives à large échelle (**§I**). De l'autre, l'amélioration de la prévention pourrait se produire à travers le renforcement des mesures déjà en place (**§II**).

I. Le renforcement de la prévention par l'adoption des instruments juridiques existants

454. Comme exposé dans les développements précédents, certains instruments internationaux prévoient des dispositions sur la prévention et la sanction des comportements illicites en ligne. Pour cela, il serait nécessaire que les États, ainsi que l'Union européenne en tant qu'organisation internationale, les ratifient afin d'assurer une protection effective. C'est le cas également pour de projet de textes en cours de discussion au sein des enceintes européennes, qu'il faudrait défendre et adopter.

455. En premier lieu, il s'agit d'analyser la nécessité de ratifier des conventions existantes qui permettraient une meilleure prévention des comportements illicites en ligne (**A**). Ainsi, en second lieu, de montrer l'intérêt de soutenir des propositions juridiques prévenant les cyberviolences (**B**).

A. La ratification et la mise en œuvre effective des conventions internationales

456. Certaines conventions internationales prévoient des dispositions sur la prévention et la sanction des comportements illicites en ligne. Nous nous concentrerons en particulier sur certaines conventions du Conseil de l'Europe.

457. Premièrement, il faudrait que l'ensemble des États membres du Conseil de l'Europe, mais aussi les non membres et/ou observateurs[968], ratifient la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique. En effet, le Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO) dans sa première recommandation qui concerne la dimension numérique des violences à l'égard des femmes[969] met en avant l'utilité de ratifier la Convention en tant qu'outil de lutte contre la dimension numérique

[968] Pour plus d'informations sur les relations du Conseil de l'Europe avec les États non-membres, voir : https://www.coe.int/fr/web/der/non-member-states

[969] GREVIO, Recommandation générale n°1 sur la dimension numérique de la violence à l'égard des femmes adoptée le 20 octobre 2021.

de la violence à l'égard des femmes et de la violence domestique. En effet, la Convention définit les principaux termes et concepts des violences faites aux femmes qui peuvent s'appliquer également à l'espace numérique et est dotée de mesures de prévention, protection et poursuite. Le GREVIO dit offrir une interprétation de la Convention qui ne fait pas de distinction entre la violence exercée contre les femmes dans le monde réel et dans le monde virtuel[970].

À cet égard, une bonne nouvelle nous parvient de l'Union européenne qui l'a ratifiée le 1er juin 2023, après plusieurs années de négociations et blocages. La présidente de la Commission européenne, Ursula von der Leyen, s'est réjouie en soulignant que « l'Union européenne envoie un signal fort : nous sommes déterminés à prévenir, condamner et combattre la violence à l'égard des femmes et des filles sous toutes ses formes »[971]. Il faut préciser que la ratification aura des conséquences sur les dispositions qui relèvent des compétences exclusives de l'Union européenne, comme la coopération judiciaire et pénale. Il est donc important de continuer à plaider pour que les États membres, les plus réfractaires, s'engagent à appliquer également les dispositions qui relèvent de leurs compétences exclusives.

458. Plusieurs dispositions de la Convention peuvent être adoptées par les États l'ayant ratifiée pour lutter contre les cyberviolences. D'abord, l'article 5, paragraphe 2, prévoit que les États prennent des mesures législatives nécessaires afin de prévenir les actes de violences. Selon la recommandation, ce devoir de diligence « s'applique à toutes les manifestations de la violence à l'égard des femmes, y compris aux formes numériques de cette violence et aux violences commises avec l'aide, ou par l'intermédiaire, de la technologie »[972]. Cela vaut également pour les articles 33, 34 et 40 qui concernent des comportements intentionnels que les États parties à la Convention doivent ériger en infraction pénale dans leur ordre juridique interne. Premièrement, l'article 33 correspond à la violence psychologique et comme le rappelle le GREVIO, « toutes les formes de

[970] *Ibid*. point 32.
[971] Commission européenne, *Stop à la violence à l'égard des femmes : la Commission salue l'adhésion de l'UE à la convention d'Istanbul*, 1er juin. Disponible sur : https://france.representation.ec.europa.eu/informations/stop-la-violence-legard-des-femmes-la-commission-salue-ladhesion-de-lue-la-convention-distanbul-2023-06-01_fr
[972] *Ibid*. point 34.

violence à l'égard des femmes commises dans l'espace numérique ont des conséquences psychologiques et pourraient être considérées comme des violences psychologiques qui s'exercent en ligne ou qui supposent le recours à la technologie »[973]. La violence psychologique peut s'exercer à travers plusieurs comportements illicites comme les intimidations ou les menaces en ligne, l'incitation au viol ou au suicide ; ainsi, elle peut aller de pair avec la violence économique qui peut également s'exercer en ligne, par exemple, à travers le contrôle des comptes bancaires. Deuxièmement, l'article 34 invite les États parties à prendre des mesures législatives pour ériger en infraction pénale le harcèlement. Comme nous l'avions déjà souligné, le rapport explicatif de la convention avait reconnu qu'il était visé à cet article, au même titre que le harcèlement hors ligne, le fait de harceler en utilisant les technologies de l'information et de la communication[974]. Enfin, la recommandation du GREVIO indique que l'article 40 qui concerne le harcèlement sexuel peut être soulevé pour plusieurs infractions en ligne comme : la diffusion non consentie d'images ou de vidéos ; la prise, la production ou l'obtention non consentie d'images ou de vidéos intimes ; l'exploitation, la contrainte et les menaces ; les brimades à caractère sexuel ; et le « cyber flashing »[975].

459. Ensuite, il serait nécessaire que les États ratifient également le premier protocole à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Comme indiqué dans le rapport explicatif du protocole, ce dernier a un double objectif : d'un côté, harmoniser le droit pénal matériel concernant le racisme et la xénophobie sur Internet, et, de l'autre, améliorer la coopération internationale dans ce domaine[976]. Ratifier ce protocole additionnel permettrait d'inscrire des infractions dans le droit interne des États parties pour « prévenir l'abus des systèmes informatiques à des fins racistes dans des Parties qui n'ont pas une législation très bien définie dans ce

---

[973] *Ibid*. point 43.
[974] Conseil de l'Europe, Rapport explicatif de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, 11 mai 2011, point 182.
[975] GREVIO, Recommandation générale n°1 sur la dimension numérique de la violence à l'égard des femmes adoptée le 20 octobre 2021, point 38. Le « cyber flashing » désigne une forme de cyberviolence qui consiste à envoyer une photo à caractère sexuel non sollicitée, souvent par l'intermédiaire du Bluetooth.
[976] Conseil de l'Europe, Rapport explicatif du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, 28 janvier 2003, point 3.

domaine »[977]. De plus, la ratification permettrait de faciliter la coopération internationale, en particulier l'extradition et l'entraide judiciaire. La simple ratification de la Convention sur la cybercriminalité ne suffit pas à freiner les infractions de contenus, notamment en ce qui concerne les discours haineux à caractère raciste et xénophobe. En effet, le protocole additionnel a élargi la portée de la Convention dans ses dispositions sur le fond mais également sur la procédure et la coopération internationale pour couvrir les infractions concernant la propagande raciste et xénophobe[978].

460. Enfin, une autre convention importante est la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels. À ce jour, les États membres du Conseil de l'Europe ont tous ratifié cette convention, toutefois les États non membres comme les États-Unis ou bien le Mexique ne l'ont pas encore fait. Il serait important que les États non membres s'engagent également en ratifiant la convention, qui est un outil de lutte contre l'exploitation et les abus sexuels des mineurs en ligne. En effet, la Convention mentionne expressément les infractions qui peuvent être facilitées par les technologies de l'information et la communication. Par exemple, c'est le premier instrument juridique international à reconnaître le grooming comme une infraction pénale[979]. La Convention demande aux États parties de prendre des mesures législatives pour éduquer les enfants, entre autres, aux risques de l'utilisation des nouvelles technologies de l'information et de la communication (TIC)[980] mais aussi pour ériger en infraction sexuelle l'accès des contenus illicites de pornographie enfantine par les biais des TIC[981].

461. Il faut souligner que la simple ratification de ces conventions ne suffit pas. En effet, il est nécessaire que les États parties se donnent les moyens pour les mettre en œuvre, notamment avec des budgets à la hauteur. En témoigne, par exemple, la France qui a ratifié la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels en 2011 et qui demeure le troisième État dans le monde

[977] *Ibid.* point 3.
[978] *Ibid.*, point 7.
[979] Article 23 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.
[980] *Ibid.* article 6.
[981] *Ibid.* article 20.

hébergeur de contenus pédocriminels derrière les États-Unis et les Pays-Bas[982]. Enfin, il est nécessaire que les États soutiennent les propositions des textes qui concernant spécifiquement les violences en ligne.

B. Le soutien aux propositions juridiques prévenant les cyberviolences

462. Depuis plusieurs années, nous assistons à une multiplication des propositions législatives pour lutter contre les cyberviolences au niveau national ainsi que régional.

463. Au sein de l'Union européenne, le 14 décembre 2021, une résolution a été adoptée par le Parlement européen contenant des recommandations à la Commission européenne sur la lutte contre la violence en ligne à caractère sexiste[983] et lui demandant de présenter des propositions sur la lutte contre les cyberviolences de genre. Quelques mois après, le 8 mars 2022, la Commission européenne a présenté une proposition de directive sur la lutte contre la violence à l'égard des femmes et la violence domestique qui prévoit, entre autres, des mesures pour lutter contre les violences en ligne. Cette proposition inclut plusieurs dispositions contre les cyberviolences en partant du constat que la réglementation en la matière est « extrêmement fragmentée » et « d'importantes lacunes juridiques ont été constatées tant au niveau de l'Union européenne qu'au niveau des États membres »[984]. Elle prévoit également des mesures de prévention spécifiques aux cyberviolences, en particulier, la sensibilisation des jeunes et la formation et l'information des professionnels[985]. La proposition fixe des règles minimales pour encadrer les infractions en ligne et des sanctions applicables. Les règles minimales concernent le partage non consenti des contenus à caractère sexuel ou manipulées (les « deepfakes »[986]), les infractions liées à la traque furtive et au cyberhacèlement ainsi que

---

[982] Point de contact, *Rapport annuel 2019*, 2020, p. 8.
[983] Résolution du Parlement européen du 14 décembre 2021 contenant des recommandations à la Commission sur la lutte contre la violence fondée sur le genre : cyberviolence, 2020/2035(INL).
[984] Proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD), p. 4.
[985] Article 36 et 37 de la proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD).
[986] Voir §§ 163-170 de cette thèse.

l'incitation à la violence ou à la haine en ligne[987]. De plus, elle prévoit des sanctions[988] et invite les États membres à faciliter l'adoption de mesures d'autorégulation par les plateformes[989]. La proposition de directive va dans la bonne direction pour assurer la protection des femmes et des filles face aux cyberviolences auxquelles elles sont surexposées. Cela dit, les infractions citées dans le texte pourraient être mieux définies. Par exemple, la définition du harcèlement en ligne s'apparente plus à la définition du raid numérique. Ce texte permettrait d'harmoniser les droits nationaux de l'ensemble des États membres, de reconnaître les spécificités des cyberviolences et adopter un cadre préventif commun. Pour cela, les États membres devraient œuvrer pour soutenir ce texte et l'enrichir pour qu'il puisse être adopté en garantissant la prévention, la protection et la sanction face au phénomène des cyberviolences de genre. Cela pourrait permettre dans un deuxième temps d'adopter une directive plus généraliste sur les cyberviolences afin d'assurer une protection pour l'ensemble des utilisateurs.

464. D'autres mesures juridiques préventives existent. Par exemple, aux États-Unis, des clauses au contrat de mariage prévoient qu'en cas de divorce les « futurs ex-conjoints s'engagent à « ne pas poster, tweeter ou d'aucune manière partager sur les réseaux sociaux des images ou tout contenu positif, négatif, insultant, embarrassant ou flatteur sur l'autre » »[990]. Comme le souligne maître Féral-Schuhl, cela permettrait de rapporter la preuve de l'absence de consentement lors de la publication des contenus.

II. Le renforcement des mesures de prévention existantes

465. Comme nous l'avons vu dans les développements précédents, des mesures préventives pour faire face aux cyberviolences existent. Cependant ces dernières devraient être renforcées. Nous nous concentrerons, en premier lieu, sur le renforcement

---

[987] Articles 7, 8, 9 et 10 de la proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD).
[988] Qui seront étudiées dans le chapitre suivant de cette thèse.
[989] Article 45 de la proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD).
[990] C. FÉRAL-SCHUHL, *Cyberdroit - Le droit à l'épreuve de l'Internet 2020-2021*, 02/2020, 8è édition, p. 1546.

des mesures de sensibilisation et de formation (**A**) pour ensuite, en second lieu, traiter la question de la modération et de l'amélioration des moyens techniques (**B**).

A. La consolidation des mesures de sensibilisation et formation

466. Certaines mesures prises à l'échelle étatique sont positives et peuvent avoir des effets à long terme, c'est le cas notamment de la sensibilisation et la formation. Toutefois ces mesures devraient être renforcées, rendues obligatoires et généralisées. Améliorer la sensibilisation signifie la généraliser non seulement auprès des mineurs mais également auprès des adultes et jeunes adultes. En effet, si ce sont les jeunes qui utilisent le plus les plateformes des réseaux sociaux, les adultes en font également usage et sont à l'origine de comportements illicites. Les sensibilisations et formations doivent s'inscrire dans des plans nationaux globaux pour prévenir les cyberviolences avec une attention particulière à la promotion des droits humains et être rendues obligatoires, à travers les systèmes d'éducation mais également au sein des entreprises, de la fonction publique et de l'ensemble de la population afin de toucher un public large et varié. Comme le rappelait le rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. Frank La Rue, les « mesures prises en réponse aux infractions relevant de l'article 20 du Pacte international relatif aux droits civils et politiques », notamment tout appel à la haine nationale, raciale et religieuse et cela y compris sur Internet, peuvent prendre la forme de campagnes d'information « organisées en vue de diffuser des messages de tolérance et de respect d'autres droits »[991].

467. Ainsi, comme affirmé précédemment, il faudrait conduire des études analytiques et fixer des objectifs chiffrés pour mesurer l'impact de ces mesures et les améliorer au fil des années. De plus, des formations obligatoires doivent être mises en place pour les professionnels qui travaillent en contact avec les victimes (agents de police, de santé ou encore personnel des écoles) avec des fonds dédiés. En effet, l'existence des mesures

[991] Voir rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-septième session, A/67/357 du 7 septembre 2012, point 59.

légales contre les cyberviolences ne sont pas suffisantes sans une connaissance approfondie du sujet qui permette leur bonne mise en œuvre. En témoigne, l'arrêt *Volodina c. Russie* dans lequel la Cour européenne des droits de l'Homme estime que, malgré l'existence d'outils juridiques pour poursuivre les actes de cyberviolences, la réticence des autorités à ouvrir une enquête pénale et la lenteur des procédures a abouti à l'impunité de l'auteur d'actes de cyberviolences conjugales[992]. Les autorités avaient notamment refusé d'ouvrir une enquête pénale pour les menaces de mort reçues par la victime sur Internet au motif qu'elles n'étaient pas « réelles »[993].

468. Ainsi, des actions de prévention spécifiques doivent être menées auprès des populations plus à risque et plus exposées aux cyberviolences, comme les femmes et les membres de la communauté LGBTQI+. Selon l'Agence des droits fondamentaux de l'Union européenne, les femmes entre 16 et 29 ans sont les plus touchées par le cyberharcèlement, suivies par les 30-44 ans et les 45-54 ans. On estime qu'au moins 25% des femmes ayant de 16 à 29 ans ont subi du cyberharcèlement dans les cinq dernières années[994].

469. Certaines mesures, concernant la formation, sont prévues dans la proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, en particulier aux articles 36 et 37. Ces types de mesures pourraient également figurer dans la proposition de texte que nous avons présenté dans développements précédents, afin de compléter les dispositions relatives aux définitions et aux règles minimales en introduisant des obligations relatives à la prévention.

470. Une autre mesure intéressante pour améliorer la prévention serait la mise en œuvre au niveau national d'un observatoire de la haine en ligne, comme celui instauré en France

---

[992] Cour EDH, *Volodina c. Russie* du 14 décembre 2021, req. n° 40419/19, §68.
[993] *Ibid.* §11.
[994] European Union Agency for Fundamental Rights, *Fundamental Rights Survey*, 2019. Disponible sur : https://fra.europa.eu/en/data-and-maps/2021/frs Voir également : EIGE, *Combating coercive control and psychological violence against women in the EU Member States*, Publications Office of the European Union, 2022. Disponible sur : https://eige.europa.eu/publications/combating-coercive-control-and-psychological-violence-against-women-eu-member-states

par l'article 16 de la loi du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet. Ce dernier est composé par des plateformes, des associations, des membres des administrations publiques et des chercheurs. Cette nouvelle entité a comme mission « d'analyser et de quantifier le phénomène de haine en ligne, d'en améliorer la compréhension des ressorts et des dynamiques, de favoriser le partage d'information et le retour d'expérience entre les parties prenantes »[995]. Aujourd'hui, à seulement deux ans de la création de l'observatoire, il est difficile d'apprécier la portée et l'efficacité de ses travaux. Cependant les objectifs de l'observatoire vont dans la bonne direction. En effet, l'observatoire permettrait de mesurer l'ampleur du phénomène de la diffusion de contenus haineux pour pouvoir mieux l'appréhender et sensibiliser un large public au niveau national. À l'échelle européenne, un observatoire européen de la haine en ligne a été créé en 2021 soutenu par le programme Droits, égalité et citoyenneté de la Commission européenne. Cette entité est composée par un consortium de quatre partenaires[996] venant de la société civile et du monde universitaire. L'observatoire publie régulièrement des articles sur la haine en ligne dans les États de l'Union européenne avec une analyse du lexique opérée par l'intelligence artificielle. Des articles thématiques sont également publiés, mais nous ne pouvons pas encore mesurer les effets de ce jeune observatoire. Il serait souhaitable de mesurer l'efficacité de ces observatoires et de permettre que les informations récoltées circulent plus efficacement dans l'ensemble des États, afin d'utiliser les analyses et les recommandations des différents acteurs impliqués.

471. Enfin, il faudrait que les acteurs étatiques et les plateformes travaillent main dans la main avec la société civile, en particulier les ingénieurs qui ont mis au point des technologies qui permettent d'identifier les contenus haineux et de les effacer. L'application Bodyguard en est un exemple[997]. Cependant, des technologies plus performantes pourraient être développées pour identifier les contenus haineux juste après la publication et avant la visualisation par la potentielle victime. D'autres technologies

[995] Observatoire de la haine en ligne : analyser pour mieux lutter sur le site du Conseil supérieur de l'audiovisuel (aujourd'hui ARCOM), 15 octobre 2020. Disponible sur : https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Observatoire-de-la-haine-en-ligne-analyser-pour-mieux-lutter
[996] « Textgain », une entreprise de technologie du langage émanant de l'Université d'Anvers, « Dare to be Grey », une organisation néerlandaise, « PDCS » qui est une ONG slovaque et l'université de sciences appliquées de Utrecht. Pour en savoir plus : https://eooh.eu/about-us
[997] Voir § 404 de cette thèse.

au service des victimes existent et devraient être utilisées par l'ensemble des États, comme celle développée par « StopNCII.org ». Il s'agit d'un outil géré par le service anglais d'assistance téléphonique contre le « revenge porn » qui fait partie de l'ONG anglaise « SWGfL » et qui permet de créer un hachage de l'image diffusée sans le consentement de la victime, c'est-à-dire d'utiliser un algorithme pour attribuer une valeur unique au contenu. Grâce à cela, toutes les copies de ce contenu auront la même valeur. Après avoir créé cette valeur, elle pourra être partagée avec les entreprises partenaires[998] et ces dernières auront la possibilité de détecter et de supprimer les contenus illégaux et leurs copies. Selon le site, grâce à cet outil, depuis 2015 plus de 200 000 contenus sexuels partagés contre le consentement de la victime ont été retirés d'Internet.

B. L'amélioration des techniques de modération

472. Face aux contenus illicites en ligne, la modération par les plateformes est inévitable. Comme nous l'avons expliqué dans les développements précédents, la modération est assurée par des humains, par des outils alimentés par l'intelligence artificielle ou les deux. La modération humaine est très chère et les contenus auxquels les modérateurs sont exposés ont des conséquences psychologiques et physiques néfastes. De plus, il serait impossible, au vu de la quantité de contenus publiés par minute sur les réseaux sociaux de compter seulement sur la modération humaine.

473. Aujourd'hui les avancées technologiques permettent à des systèmes informatiques, à travers l'apprentissage automatique, de prendre des décisions. Cet apprentissage nécessite l'analyse d'une grande quantité des données. Selon les chercheurs, l'avancée plus importante de l'apprentissage automatique est celle des « deep neural networks » (réseaux neuronaux profonds) qui permettent un « deep learning » (apprentissage profond). Ces réseaux permettent aux systèmes informatiques de reconnaître des caractéristiques complexes dans des contenus qui impliquent le discours humain, les

[998] Au 6 août 2023, les entreprises partenaires étaient Facebook, Instagram, Tik Tok, Reddit, Bumble, Threads, et Only Fans. Pour en savoir plus, voir : https://stopncii.org/

images ou bien les textes[999]. Toutefois, la marge d'erreur de ces systèmes est encore très grande, et cela peut causer un retrait excessif des contenus licites ou bien un retrait insuffisant des contenus illicites. En effet, si l'intelligence artificielle arrive à filtrer facilement certains contenus, par exemple des images pédopornographiques, d'autres sont plus difficilement analysables. En effet, si certains contenus peuvent être retirés en analysant seulement une photo, d'autres doivent être étudiés en analysant le contexte et avec une compréhension des facteurs sociétaux, politiques, culturels et historiques. Dans ces cas, l'intervention humaine est essentielle. Un exemple précis est celui de la modération des contenus violents. Nous avons assisté à plusieurs reprises à des attentats terroristes en direct sans que les modérateurs humains, ni les outils automatiques aient réussi à les détecter avant leur mise en ligne[1000] ; alors que des outils d'intelligence artificielle ont effacé des contenus violents qui auraient pu être utilisés comme preuve contre des crimes de guerre[1001].

474. La seule modération humaine, comme la seule modération automatique sont insuffisantes. Pour cela il faudrait renforcer l'analyse du contexte des contenus publiés. Comme souligné par l'étude commissionné par l'Ofcom (équivalent anglaise de l'Arcom française), les contenus illicites sont produits par une petite proportion d'utilisateurs. L'intelligence artificielle pourrait s'intéresser à ces utilisateurs malveillants, en regardant leurs relations et la nature de leurs interactions. Ce faisant, une liste d'utilisateurs suspects pourrait être créée pour ensuite pouvoir identifier et supprimer plus rapidement les nouveaux contenus illicites provenant de ces profils[1002]. De plus, la modération hybride devrait être privilégiée et développée. En effet, les avantages offerts par l'intelligence artificielle se mêlent avec celles de la modération humaine. L'intelligence artificielle peut réduire les effets néfastes de la modération et l'exposition des êtres

---

[999] Cambridge Consultants, *Use of AI in online content*, Report produced on behalf of Ofcom, 2019, p. 4.
[1000] Voir : G. SARTOR, A. LOREGGIA, *The impact of algorithms for online content filtering or moderation*, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament, September 2020, p. 46.
[1001] UNICRI, UNCCT, *Countering terrorism online with artificial intelligence*, 2021, p.42. Voir également Human Rights Watch, *"Video Unavailable" Social Media Platforms Remove Evidence of War Crimes, 10* September 2020. Disponible sur : https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes
[1002] Cambridge Consultants, *Use of AI in online content*, report produced on behalf of Ofcom, 2019, p. 54.

humains à des contenus violents tout en améliorant leur efficacité dans le traitement des contenus. D'une part, en développant les échanges entre les humains et la machine pour les contenus dont cette dernière a des incertitudes, en priorisant les contenus à montrer selon la potentielle dangerosité. De l'autre, par la transmission de contenus nuisibles de façon floutés pour réduire les risques d'exposition des humains. Nous parlons ici d'une technique appelée « Visual question answering (VQA) » (réponse à des questions visuelles). À travers cette dernière, les outils automatiques aident les humains à identifier un contenu illicite sans le regarder. Par exemple, face à une photo pédopornographique, l'humain peut poser plusieurs questions à la machine pour identifier la nature du contenu et décider de le supprimer sans le regarder et être exposé à des images qui pourraient lui causer des traumas[1003]. Il n'en reste pas moins que la quantité des modérateurs humains doit être sensiblement augmentée, ainsi que, leur formation, leur expertise, notamment linguistique et leur sensibilisation aux risques de discriminations.

De plus, il faudrait améliorer la qualité des systèmes de filtrage automatiques, en particulier, en évitant les biais humains intentionnels ou inconscients qui pourraient être introduits dans les algorithmes. Il est essentiel que pendant la « formation » des algorithmes les préjugés soient limités et soient adaptés aux réalités de chaque État. Cela vaut également pour la modération humaine car les humains peuvent également avoir des préjugés, ne pas être formés sur certaines situations ou bien ne pas parler correctement la langue qui figure dans le contenu. Mais également, un contenu considéré comme inoffensif hier peut être considéré offensif aujourd'hui. Nous pensons par exemple à un changement de loi ou à changement de politique interne de la plateforme, comme Meta l'a fait au sujet des contenus négationnistes.
Le Groupe de travail sur les régimes de responsabilité des réseaux sociaux et de leurs utilisateurs[1004] a publié un rapport le 22 septembre 2022 à l 'occasion du second Sommet pour l'information et la démocratie. Dans ce rapport, un groupe d'experts et expertes

[1003] *Ibid*. p. 61.
[1004] Ce groupe de travail est une instance qui fait partie du Forum sur l'information et la démocratie, entité internationale fondée par 11 organisations indépendantes représentant différents champs d'expertise et régions du monde et a comme objectif de « mettre en œuvre des garanties démocratiques dans l'espace global de la communication et de l'information ». Pour plus d'information, voir https://informationdemocracy.org/fr/le-forum/#mandate.

internationaux recommande que la suppression des contenus devrait être faite par des êtres humains et non par des algorithmes en fonction d'un seuil de complexité établi par une coalition d'experts en droit international des droits humains et de la société civile. Ils suggèrent également que les réseaux sociaux devraient être obligés d'assurer un certain niveau de modération humaine qui soit représentative des minorités, avec des personnes formées sur le contexte géopolitique local, le droit local et le droit international, et maîtrisant les langues des contenus à modérer[1005]. Enfin, il serait nécessaire de renforcer la collaboration avec la société civile et notamment avec les signaleurs de confiance (« trusted flaggers ») comme prévu par le Digital Services Act[1006]. Il faut également assurer une plus grande transparence dans l'utilisation de l'intelligence artificielle pour éviter les dérives à son utilisation[1007] et pour garantir que les contenus filtrés l'aient été sur des bases raisonnables et non discriminatoires[1008]. À cet égard, plusieurs ONG avaient souligné que les rapports de transparence publiés par les plateformes n'étaient pas complets[1009]. Améliorer la transparence pourrait également permettre d'éliminer l'imprévisibilité et l'incertitude de l'utilisateur face à la modération[1010]. Ainsi, comme souligné par le rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, « toutes les entreprises du secteur des TIC devraient respectent les Principes directeurs relatifs aux entreprises et aux droits de l'homme[1011] et tenir compte des droits de l'homme par défaut ainsi que dans la

---

[1005] Forum on Information and Democracy, *Accountability regimes for social networks and their users*, Policy framework, September 2022, p.19.
[1006] Article 22 du règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[1007] Par exemple, une technologie utilisée par les plateformes pour identifier des contenus pédopornographiques a voulu être utilisé par le Bureau central d'enquête de New Delhi pour des affaires criminelles ordinaires. Voir : J. SINGH, CBI *Reportedly Asks Social Media Firms to Use Intrusive PhotoDNA Technology to Track Suspects*, 1 janvier 2019. Disponible sur : https://gadgets360.com/social-networking/news/cbi-reportedly-asks-social-media-firms-to-use-intrusive-photodna-technology-to-track-suspects-1971042 Voir également, A. LAWSON, *Automation in moderation: Preserving fundamental rights while moderating online content at scale*, Observer Research Foundation, 14 avril 2021. Disponible sur : https://www.orfonline.org/expert-speak/automation-moderation-preserving-fundamental-rights-moderating-online-content-scale/
[1008] G. SARTOR, A. LOREGGIA, *The impact of algorithms for online content filtering or moderation*, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament, September 2020, p. 47.
[1009] Voir : A. DE STREEL et al., *Online Platforms' Moderation of Illegal Content Online*, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, 652.718, June 2020, p. 46.
[1010] Cambridge Consultants, *Use of AI in online content*, report produced on behalf of Ofcom, 2019, p. 41.
[1011] Il s'agit de 31 principes adoptés par le Conseil des droits humains des Nations Unies le 16 juin 2011. Disponibles sur : https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_fr.pdf

conception de leurs produits »[1012]. Enfin, le filtrage des contenus ne sera jamais parfait et les erreurs, de la part des systèmes informatiques ou bien des humains, sont inévitables. Cependant, il faudrait que chaque système de modération soit doté des mesures pour identifier et réagir aux erreurs[1013]. Le Digital Services Act marque une avancée en matière de transparence, en effet, il prévoit des obligations cumulatives de transparence vis-à-vis de plusieurs sujets, par exemple : la modération des contenus, à travers la publication de rapports au moins une fois par an sur les procédures de modération (article 15), la publicité (article 39) ou encore le système de recommandation (article 27)[1014].

475. Pour conclure, il faut souligner que la diffusion de contenus illicites n'est pas un problème strictement lié à la technologie mais bien un problème social amplifié par les nouvelles technologies. Et cela ne peut pas être résolu par l'intelligence artificielle ou par la modération humaine, il faut développer des mesures durables, par exemple à travers l'éducation, pour faire changer en profondeur une partie de la société qui prône, entre autres, des valeurs discriminatoires, racistes et misogynes.

[1012] Voir rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, point 42.
[1013] G. SARTOR, A. LOREGGIA, *The impact of algorithms for online content filtering or moderation*, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament, September 2020, p. 49.
[1014] Règlement du Parlement européen et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE. Voir également R. MOUTOT, Lutter contre les contenus illicites et imposer une plus grande transparence aux plateformes : publication du *Digital Services Act* au JOUE, *Dalloz Actualité*, 10 janvier 2023.

Conclusion du Chapitre VI

476. L'amélioration de la prévention passe par la responsabilisation des plateformes qui ont vu leur régime évoluer depuis l'essor d'Internet. En effet, si à l'origine l'attention était portée à l'expansion d'Internet, du commerce électronique et des plateformes. Aujourd'hui, au sein de l'Union européenne la défense des droits fondamentaux des utilisateurs est devenue une priorité, en témoigne l'adoption du Digital Services Act. Mais cela n'est pas le cas dans des États autoritaires qui se servent de la responsabilisation des plateformes pour réduire et porter atteinte aux droits et libertés des individus. Le renforcement des mesures préventives est possible également à travers le renforcement des mesures existantes et la révision de modèles inefficaces de modération. Cependant, ces mesures ne seront pas satisfaisantes à long terme si un changement sociétal ne s'opère pas à travers la lutte contre les discriminations et la haine même hors ligne.

CONCLUSION DU TITRE I

477. Une stratégie préventive contre les comportements illicites en ligne à perfectionner - Les mesures de prévention contre les comportements illicites en ligne sont nécessaires pour permettre de construire une réponse globale au phénomène des cyberviolences. En effet, la solution ne se situe pas seulement dans la sanction mais elle doit être trouvé en amont avec des initiatives et des mesures destinées à éviter que les contenus illicites soient diffusés. Plusieurs acteurs sont mobilisés à ces fins, non seulement les autorités nationales mais également les plateformes et les membres de la société civile. Avec le constat clair que les mesures existantes ne suffisent pas aujourd'hui pour éviter les cyberviolences, il faut repenser la stratégie de prévention par l'ensemble des acteurs. Cette amélioration serait possible à travers le renforcement de la responsabilité des plateformes, l'investissement massif dans la modération, notamment hybride, ainsi que la consolidation et l'amélioration d'initiatives, juridique ou non, déjà existantes qui pourraient être plus efficaces si mieux évaluées et financées, comme l'éducation et la prévention.

TITRE II : L'EFFICACITE RELATIVE DES SANCTIONS. VERS LA CONSTRUCTION D'UN CADRE ADAPTE AUX ENJEUX D'INTERNET

478. Après avoir étudié les mesures de prévention, nous allons analyser les mesures répressives existantes contre les violences en ligne. Cette étude est intéressant compte tenu des différentes fonctions de la sanction. En effet, l'existence même de la sanction peut avoir une fonction de prévention qui permet d'empêcher la commission des comportements illicites. Pour parvenir à cet objectif, il est nécessaire que les mesures adoptées soient dissuasives. Outre à ce rôle préventif, la sanction a également une fonction répressive auprès des auteurs. À cet égard, elle a des conséquences, non seulement sur l'auteur, mais aussi sur les auteurs potentiels qui seront moins susceptibles d'agir de façon illicite, il faudrait cependant que la peine soit juste pour éviter qu'elle soit prise à la légère.

Nous pouvons également rappeler la fonction réparatrice pour la victime qui est essentielle pour rétablir la justice sociale et individuelle et, ainsi, permettre à la victime de se reconstruire. Le constat que nous faisons aujourd'hui en matière de sanction de cyberviolences est que ces dernières correspondent souvent aux mêmes mesures adoptées pour les comportements hors ligne et, très peu d'entre elles, prennent en compte les spécificités de la sphère cyber et les conséquences sur les utilisateurs.

479. Aujourd'hui, plusieurs acteurs sont impliqués dans l'adoption de mesures répressives, qu'elles aient ou pas une valeur juridique. En effet, aux côtés du législateur, nous trouvons également les plateformes qui ont la capacité d'adopter des sanctions pour les comportements allant à l'encontre de leurs conditions générales d'utilisation.

480. Au vu de ces éléments, dans les prochains développements, il s'agira d'étudier les sanctions existantes et rechercher comment adopter des mesures dissuasives (**Chapitre VII**) pour ensuite analyser la proportionnalité de ces dernières (**Chapitre VIII**).

Chapitre VII : La recherche d'une sanction dissuasive

481. Dans l'histoire des sanctions nous avons assisté, sauf dans certains États (en particulier, à faible revenus ou dictatoriaux), à une évolution des législations concernant les peines encourues à la suite d'un comportement illicite. Progressivement, les peines corporelles ont laissé la place aux peines privatives de liberté qui ont été elles-mêmes adoucies dans certains États à travers l'apparition de la probation[1015] et du sursis[1016]. Ensuite, au milieu du XXe siècle des peines alternatives sont instaurées, par exemple : l'amende, la confiscation ou les interdictions professionnelles. Enfin, entre les années 1970 et 1990 nous assistons à la création de peines prévoyant des services à la communauté[1017], comme des travaux d'intérêt général. Selon J. Pradel ces évolutions sont dues à l'humanisation mais également aux coûts des mesures privatives de liberté et à l'échec de certaines sanctions.

482. Plusieurs Codes pénaux distinguent les peines des mesures de sureté. On distingue les peines d'emprisonnement, de détention ou d'amendes aux mesures de placement en établissement spécialisés ou la liberté surveillé et l'interdiction professionnelles[1018]. Cette distinction est fondée sur le principe : « la peine rétribuant une faute et tendant à l'absence de récidive alors que la mesure de sureté est uniquement préventive »[1019]. Dans le cadre de cette étude nous parlerons plus généralement de sanction, en effet ce que pourrait être une mesure de sureté dans un État pourrait être une peine dans un autre. Plusieurs droits nationaux, comme le droit italien, prévoient une trilogie de peines : les

---

[1015] La probation est une pratique née aux États-Unis qui s'est développé également en Angleterre et dans d'autres États de common law. Il ne s'agit pas d'une pratique uniforme, dans chaque État elle a des caractéristiques différentes. Par exemple, aux États-Unis prévoient de mesures de couvre-feu, des tests réguliers de consommation de drogue, le contrôle des connexions internet, etc. Voir J. PRADEL, *Droit pénal comparé*, Dalloz, 4e édition, 2016, pp. 612-623.

[1016] Le sursis est une pratique sui est née en Belgique par la loi Le Jeune du 31 mars 1888 et qui a été reprise en France par la loi Béranger du 26 mars 1891. Il s'agit d'un sursis à l'exécution de la peine prononcé par les juges. Voir : J. PRADEL, *Droit pénal comparé*, Dalloz, 4e édition, 2016, pp. 612-623 et E. BONIS et V. PELTIER, *Droit de la peine*, 3e édition, LexisNexis, 2011, pp. 309-353.

[1017] J. PRADEL, *Droit pénal comparé*, Dalloz, 4e édition, 2016, pp. 585-586.

[1018] Cette distinction est opérée en Espagne, aux Pays-Bas, en Pologne par exemple. Voir J. PRADEL, *Droit pénal comparé*, Dalloz, 4e édition, 2016, p. 584.

[1019] J. PRADEL, *Droit pénal comparé*, Dalloz, 4e édition, 2016, p. 584.

peines principales, qui confèrent « sa qualification à l'infraction qu'elles répriment »[1020] et qui peuvent être prononcées seules, les peines complémentaires qui existent seulement si une peine principale est prononcée et les peines accessoires. Dans d'autres, cette trilogie est remplacée par d'autres peines, par exemple, l'Espagne distingue les peines en : graves (« penas graves »), moins graves (« penas menos graves »), et lègeres (« penas leves »)[1021]. Ou encore, en France, par exemple, les peines accessoires n'existent pas.

D'abord, pour les personnes physiques, les peines principales peuvent être peuvent être peines de réclusion, des amendes mais également des travaux d'intérêt général. Ces derniers ont comme objectif de faire réaliser à la personne condamnée une activité qui puisse profiter à la société et en assurant sa réintégration en société. Cette peine est considérée une peine autonome dans plusieurs États, par exemple : l'Angleterre, la France, les Pays-Bas, la Belgique, le Luxembourg, l'Espagne et le Portugal[1022]. Certains États ont consacré cette mesure comme une modalité de la probation, comme l'Allemagne, la France et le Canada ou comme alternative à la poursuite comme la Belgique[1023]. Ensuite, les peines complémentaires peuvent être des interdictions à l'exercice d'une profession, le retrait d'un droit, des stages de sensibilisation (par exemple sur les violences sexuelles et sexistes) ou encore un suivi socio-judicaire. Enfin, pour les personnes morales, les peines sont surtout financières, comme des amendes, mais aussi l'interdiction d'exercer des activités arrivant jusqu'à la dissolution.

483. Nous pouvons également souligner la distinction entre les sanctions pénales et civiles. Premièrement, il est nécessaire de mentionner qu'historiquement, pour la théorie classique du droit pénal[1024], la sanction pénale a comme fonction d'« obtenir un effet de motivation sur les délinquants en puissance »[1025], c'est-à-dire un effet préventif. Mais également un effet moral, c'est-à-dire « le pouvoir de la loi d'inculquer ses propres

[1020] E. BONIS et V. PELTIER, *Droit de la peine*, 3e édition, LexisNexis, 2011, p. 63.
[1021] J. PRADEL, *Droit pénal comparé*, Dalloz, 4e édition, 2016, p. 587.
[1022] *Ibid.* pp. 623-627.
[1023] *Ibid.* p. 627.
[1024] Voir des auteurs comme C. BECCARIA ou J. BENTHAM.
[1025] J. ANDENAES, « Les effets de prévention générale du droit pénal », *Archives de politique criminelle*, 1978, n° 3, p. 5.

valeurs aux citoyens »[1026]. Nous pouvons mettre en avant également d'autres fonctions, celle de neutralisation et de réparation. La fonction de neutralisation consiste à « neutraliser » le sujet ayant commis un délit ou un crime pour empêcher qu'il nuise à nouveau. À cette fin, des sanctions privatives de liberté sont adoptées, en particulier l'incarcération, mais aussi la liberté surveillée ou la liberté conditionnelle. La fonction de prévention n'est rien d'autre que la mission de freiner ou d'empêcher un comportement illicite. Cela, avec une finalité consistant à dissuader d'autres personnes à commettre des comportements illicites. Concernant cette fonction dissuasive et d'« intimidation collective », M. Van De Kerchove et d'autres auteurs montrent que son efficacité n'a pas été prouvée au regard des travaux contradictoires et incertains en la matière[1027]. De plus, la sanction pénale peut avoir une fonction réparatrice (ou de reconstruction) qui est essentiellement symbolique car elle relève du registre d'une réparation psychologique[1028] et morale pour la victime. Ce qui est censé « permettre à la victime de dépasser les conséquences psychologiques de l'acte délictueux » [1029]. Cela nous amène à la fonction symbolique de la peine, appelée également « socio-pédagogique »[1030] qui sert à montrer à l'ensemble de la société la validité des normes mais également d'augmenter la confiance dans les institutions. Deuxièmement, la sanction civile se distingue de la pénale parce qu'elle a principalement une fonction de dédommagement, « essentiellement financier » [1031], pour la victime. Cette sanction est prévue en compensation du préjudice matériel mais aussi moral[1032]. Dans les développements qui vont suivre, nous analyserons la sanction d'un côté, comme toute mesure contraignante qui constitue « une réaction du droit à une violation de la

[1026] *Ibid.* p. 5.
[1027] M. VAN DE KERCHOVE, « Les fonctions de la sanction pénale. Entre droit et philosophie », *Informations sociales*, 2005/7 (n° 127) qui cite P. ROBERT, *La peine, quel avenir ? Approche pluridisciplinaire de la peine judiciaire*, Paris, Le Cerf, 1983, pp. 105-106 ; G. KELLENS, *La mesure de la peine*, Liège, Collection scientifique de la Faculté de droit de Liège, 1982, p. 194 ; A. C. BERGHUIS, « La prévention générale : limites et possibilités », *Les objectifs de la sanction pénale. En hommage à Lucien Slachmuylder*, Bruxelles, Bruylant, 1989, p. 93. Voir également A. BARATTA, « Les fonctions instrumentales et les fonctions symboliques du droit pénal », *Déviance et société*, 1991, vol. 15, n° 1, p. 14.
[1028] M.L. CESONI et R. RECHTMAN, « « La réparation psychologique » de la victime : une nouvelle fonction de la peine ? », *Revue de droit pénal et de criminologie*, 2005, 2, pp. 158-178.
[1029] *Ibid.* p. 159.
[1030] M. VAN DE KERCHOVE, « Les fonctions de la sanction pénale. Entre droit et philosophie », *Informations sociales*, 2005/7 (n° 127), p. 22-31
[1031] M.L. CESONI et R. RECHTMAN, « « La réparation psychologique » de la victime : une nouvelle fonction de la peine ? », *Revue de droit pénal et de criminologie*, 2005, 2, p. 168.
[1032] *Ibid.* p. 168.

légalité »[1033] et comme une sanction appliquée par une autorité publique. De l'autre, comme une mesure répressive qui ne se situe pas dans le plan juridique, qui est prononcée par des autorités privées et qui a des effets potentiels à l'égard des droits fondamentaux des utilisateurs.

484. Les sanctions adoptées par autorités contre les infractions en ligne suivent une logique préventive et répressive. À cet égard, il s'agit d'analyser les multiples sanctions prévues pour réprimer les comportements illicites en ligne (**Section I**), puis, d'étudier leur efficacité (**Section II**).

Section I : Des peines multiformes contre les comportements illicites en ligne

485. Lorsque les comportements illicites en ligne sont encadrés par les textes nationaux, les peines encourues sont généralement les mêmes sanctions que celles prévues pour les comportements hors ligne. Cependant, nous assistons à l'apparition de nouvelles sanctions qui ont un effet immédiat sur les contenus illicites publiés et ses utilisateurs.

486. Il s'agira d'analyser les mesures traditionnelles adoptés par les autorités nationales (**§I**) pour ensuite analyser l'apparition des nouvelles sanctions et d'autorités capables de prendre de mesures ayant un impact immédiat contre les utilisateurs et la publication de contenus illicites (**§II**).

I. Des mesures répressives peu dissuasives par les autorités nationales

487. Nous nous concentrons sur la sanction au sens de toute mesure contraignante qui constitue « une réaction du droit à une violation de la légalité »[1034]. En général, concernant les sanctions, les instruments juridiques que nous avons cités à maintes reprises dans ces travaux, comme la Convention du Conseil de l'Europe contre la

[1033] C. CHAINAIS, D. FENOUILLET et G. GUERLIN (dir.), *Les sanctions en droit contemporain, La motivation des sanctions prononcées en justice*, Dalloz, 2013, p. XI.
[1034] *Ibid.*

cybercriminalité ou encore la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, indiquent que la sanction doit être effective, proportionnée et dissuasive[1035].

488. En premier lieu, il s'agit d'étudier les sanctions traditionnelles prévues par les acteurs étatiques (**A**). En second lieu, il s'agit d'analyser leur application à travers un approfondissement sur la jurisprudence française (**B**).

A. Une réponse étatique en demi-teinte

489. Les États membres de l'Union européenne disposent de mesures répressives assez similaires les uns avec les autres. En général, les sanctions prononcées sont des amendes ou bien des peines d'emprisonnement. Les peines varient selon la gravité des actes. Nous allons analyser ces sanctions en prenant des exemples de comportements illicites et des sanctions au sein des États membres de l'Union européenne et au-delà.

490. En particulier, pour fixer un cadre précis et apporter des exemples clairs, nous analyserons les sanctions prévues pour les comportements illicites étudiées précédemment. Dans les développements précédents[1036], nous avions analysé la réponse juridique de certains États aux infractions sexuelles, comme le partage des contenus à caractère sexuel sans le consentement de la victime, le voyeurisme digital, le cyberharcèlement et le discours de haine en ligne. Nous approfondirons cette analyse concernant ces infractions, cependant nous n'étudierons pas sur le voyeurisme digital, en effet, très peu d'États membres de l'Union européenne ont adopté des dispositions pour le réprimer.

[1035] Voir article 45 de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à égard des femmes et la violence domestique, ainsi que l'article 13 de la Convention du Conseil de l'Europe contre la cybercriminalité mais également l'article 13 de la directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie.
[1036] Voir §§ 237-260 de cette thèse.

491. D'abord, concernant le partage de contenus à caractère sexuel sans le consentement de la victime, nous avions analysé les sanctions prévues par le Code pénal italien et le Code pénal français pour conclure que le droit italien prévoit des peines d'emprisonnement plus lourdes (jusqu'à six ans d'emprisonnement contre deux ans en France) et une amende moins importante (jusqu'à 15 000 euros contre 60 000 euros en France). Les autres États membres qui répriment explicitement le partage des contenus à caractère sexuel sans le consentement de la victime sont la France, l'Italie, la Belgique, les Pays-Bas, Malte, l'Espagne, l'Irlande, le Portugal, la Suède et la Pologne[1037]. L'ensemble des États prévoit une peine d'emprisonnement qui n'excède pas les sept ans (Irlande) et, la plupart des États a fixé une peine d'un à deux ans d'emprisonnement[1038]. La peine de prison est ensuite accompagnée, sauf en Belgique, par une amende qui ne dépasse pas les 60 000 euros (France). Ces peines sont légères lorsque nous savons que à la suite du partage de contenus illicites la victime peut subir des conséquences graves sur sa vie professionnelle, par exemple perdre son emploi, et personnelle avec des séquelles psychologiques graves qui nécessitent un suivi médical régulier.

492. Ensuite, concernant le cyberharcèlement, treize États membres de l'Union européenne prévoient des dispositions *ad hoc* dans leur législation. Il s'agit de la Bulgarie, la République Tchèque, l'Allemagne, la Grèce, l'Espagne, la France, l'Italie, la Lituanie, Malte, l'Autriche, la Roumanie, la Slovénie et la Slovaquie[1039]. Les sanctions, sans compter les circonstances aggravantes, prévoient une peine d'emprisonnement qui ne dépasse pas les 5 ans et qui peut s'accompagner d'amendes[1040]. La peine d'emprisonnement plus lourde est prévue en Italie (de 6 mois à 5 ans), en Allemagne et France (jusqu'à 3 ans) et en Slovénie (jusqu'à 2 ans).

[1037] Le cas de la Pologne est particulier car l'article 191 a du Code pénal réprime le fait de fixer et/ou diffuser des images à caractère sexuel prises avec l'utilisation de la violence, la menace illégale ou la tromperie. Dans le cas où les images ont été prises avec le consentement de la victime alors d'autres dispositions plus générales seront appliquées.
[1038] Voir tableau 1 dans les annexes.
[1039] EIGE, *Combating coercive control and psychological violence against women in the EU Member States*, Publications Office of the European Union, 2022, pp. 133-139.
[1040] Voir le tableau 2 dans les annexes.

493. Enfin, concernant le discours de haine en ligne, nous rappelons que, dans ces travaux, nous avons utilisé la définition du Conseil de l'Europe qui le définit comme : « tout type d'expression qui incite à, promeut, diffuse ou justifie la violence, la haine ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes, ou qui les dénigre, en raison de leurs caractéristiques personnelles ou de leur statut réels ou attribués telles que [une prétendue] «race», la couleur, la langue, la religion, la nationalité, l'origine nationale ou ethnique, l'âge, le handicap, le sexe, l'identité de genre et l'orientation sexuelle »[1041]. Ces discours comprennent les appels à la haine et à la violence à l'encontre d'une personne ou d'un groupe de personnes en raison, entre autres, de leur origine, religion ou genre. Cela diffère d'État en État. En effet, certains d'entre eux ne prévoient pas des dispositions pour les discours haineux basés sur le genre, par exemple la Grèce ou l'Italie. Nous rappelons que les discours haineux, notamment ceux motivés par le racisme et la xénophobie, sont sanctionnés par l'article 20 du Pacte international relatif aux droits civils et économiques[1042], mais également par l'article 4 de la Convention internationale sur l'élimination de toutes les formes de discrimination raciale[1043], le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe et, au niveau de l'Union européenne, par la décision cadre du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal[1044]. L'article 3, paragraphe 2, de cette dernière prévoit que chaque État membre doit prendre les mesures nécessaires pour punir avec une peine maximale d'au moins un à trois ans d'emprisonnement les incitations à la haine et à la violence[1045]. Au sein de l'Union européenne, seulement cinq États ont adopté des dispositions sur le discours de haine en ligne qui mentionnent Internet ou plus généralement les technologies de l'information et de la communication. Il s'agit de l'Allemagne, la Croatie, l'Espagne, la Grèce ainsi que

[1041] Voir la recommandation CM/Rec (2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine adoptée par le Comité des Ministres le 20 mai 2022, lors de la 132e Session du Comité des Ministres, point 1 (2).
[1042] Pacte international relatif aux droits civils et politiques, 16 décembre 1966, New-York, Nations Unies.
[1043] Convention internationale sur l'élimination de toutes les formes de discrimination raciale, 7 mars 1966, New-York, Nations Unies.
[1044] Décision-cadre 2008/913/JAI du conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal.
[1045] Article 3, paragraphe 2, de la Décision-cadre 2008/913/JAI du conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal.

la Lettonie[1046]. Ces États prévoient des peines d'emprisonnement qui ne dépassent pas les 5 ans ainsi que des amendes. Les autres États membres qui sanctionnent le discours haineux hors ligne prévoient également ces types de sanction d'un mois à sept ans d'emprisonnement.

494. Il est également intéressant d'analyser ce qui est prévu par la proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique du 8 mars 2022[1047]. Parmi ses dispositions, elle prévoit plusieurs sanctions pour des violences en ligne. En premier lieu, elle prévoit 2 ans d'emprisonnement pour des comportements qui relèvent de la traque furtive en ligne, du cyberharcèlement et de l'incitation à la violence ou à la haine en ligne basée sur le genre[1048]. En deuxième lieu, elle prévoit une peine maximale d'au moins 1 an pour le partage non consenti de matériels intimes ou manipulés[1049]. À cet égard, il est important de mentionner que la définition de « contenu intime » a été jugé trop limitée par certains députés européens qui demandent de l'élargir pour inclure des images de nudité qui n'aient pas de nature sexuelle[1050]. De plus, elle prévoit la possibilité pour les victimes de demander une indemnisation totale pour le préjudice subi qui puisse, entre autres, couvrir les coûts des soins de santé, des services d'aide et de réadaptation ; ainsi que, la perte des revenus issue de l'infraction et de la gestion de ses conséquences[1051]. Certains députés européens demandent d'ajouter à la directive également une obligation pour les États de garantir que la victime ait accès à une assistance juridique gratuite et à un diagnostic spécialisé[1052].

[1046] Voir le Tableau 2 dans les annexes.
[1047] Proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD).
[1048] Article 12, paragraphe 5, de la proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD).
[1049] *Ibid.* article 12, paragraphe 6.
[1050] Parlement européen, *Violences envers les femmes : le sexe sans consentement est un viol, rappellent les députés*, communiqué de presse, 28 juin 2023. Disponible sur : https://www.europarl.europa.eu/news/fr/press-room/20230626IPR00838/violences-envers-les-femmes-le-sexe-sans-consentement-est-un-viol
[1051] *Ibid.* article 26.
[1052] Parlement européen, *Violences envers les femmes : le sexe sans consentement est un viol, rappellent les députés*, communiqué de presse, 28 juin 2023. Disponible sur : https://www.europarl.europa.eu/news/fr/press-room/20230626IPR00838/violences-envers-les-femmes-le-sexe-sans-consentement-est-un-viol

495. Au vu de ces éléments, nous pouvons constater que, d'une part, le plus souvent les mesures répressives constituent des peines d'emprisonnement et des amendes. De l'autre, que les États membres de l'Union européenne, lorsqu'ils prévoient des mesures pour réprimer des violences en ligne, utilisent les mêmes sanctions qui sont prévues pour les infractions hors ligne.

496. Il est intéressant d'analyser comment certaines de ces mesures répressives sont mises en œuvre par les juges nationaux. Pour le faire, nous étudierons la jurisprudence française et nous nous concentrerons sur les trois catégories d'infractions étudiées dans les développements précédents.

B. L'application des mesures répressives par la jurisprudence française

497. Il s'agira d'analyser l'application des normes juridiques en matière de cyberviolences dans le cadre des juridictions françaises. En particulier, nous étudierons certaines affaires concernant les infractions de partage de contenus à caractère sexuel, le cyberharcèlement ainsi que, plus généralement, la haine en ligne.

498. Concernant le partage de contenus à caractère sexuel sans le consentement de la victime, la Cour de cassation française a rendu le 16 mars 2016 un arrêt controversé dans lequel elle jugeait que il n'« 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 »[1053]. Depuis, le législateur a introduit à travers la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique le délit de partage de contenus à caractère sexuel sans le consentement de la victime[1054]. Depuis cette loi, les juges français ont traité plusieurs affaires. Nous en citerons certaines d'entre eux pour donner des exemples de sanctions. Premièrement, le 15 novembre 2016, le tribunal de grande instance de Montpellier[1055] a condamné un homme à 3 ans de prison dont un avec sursis et deux ans de mise à

[1053] Crim. 16 mars 2016, n° 15-82.676
[1054] Article 226-2-1 du Code pénal.
[1055] Tribunal de grande instance de Montpellier, 15 novembre 2016.

l'épreuve ainsi que 10 000 euros d'amende. Cependant, ce dernier n'avait pas seulement partagé une vidéo intime de la victime sur des sites pornographiques mais également essayé de la poignarder. En outre, par son jugement du 20 novembre 2018 le tribunal de grande instance de Bobigny a condamné une femme à une peine de 800 euros de dommages intérêts[1056] pour la diffusion d'images à caractère sexuel sans le consentement de la victime. Enfin, la Cour d'appel de Limoges a condamné plus sévèrement en appel un jeune homme qui avait mis en ligne des vidéos intimes de la victime sans son consentement[1057]. La Cour a condamné le prévenu à verser à la victime 5 000 euros de dommages et intérêts (alors que le tribunal correctionnel l'avait condamné à verser 1 600 euros). Le raisonnement de la Cour est intéressant car le montant des dommages et intérêts a été fixé au regard des conséquences que la diffusion des images avait causé à la victime, notamment la baisse de ses notes scolaires, la dépression et la nécessité de suivre des soins psychologiques. Cela nous montre l'importance de reconnaître les conséquences spécifiques des cyberviolences pour adopter une sanction adaptée. Si les juridictions internes commencent à reconnaître la gravité du partage des contenus illicites sur Internet, les peines sont tout de même très faibles et nous estimons que ne sont pas assez dissuasives pour les autres utilisateurs. De plus, malgré un signal positif envoyé aux victimes, ces peines ne sont pas à la hauteur des conséquences causées.

499. Concernant l'infraction de cyberharcèlement, nous pouvons citer des exemples de la jurisprudence française. Plusieurs cas de cyberharcèlement ont été jugés ces dernières années. L'un des cas les plus emblématiques est celui de la journaliste Nadia Daam menacée, avec sa fille, de mort et de viol sur les réseaux sociaux. Deux de ses harceleurs ont été condamnés : l'un à cinq mois de prison avec sursis et 2500 euros pour préjudice moral pour menace de mort sur elle et menace de viol sur sa fille. Et, deux autres à six mois de prison avec sursis et 2000 euros d'amende pour les mêmes infractions. D'autres décisions similaires ont été rendues concernant le cyberharcèlement d'une jeune femme dont l'agresseur a été condamné à deux ans d'emprisonnement avec sursis ou encore trois hommes et deux femmes qui ont été condamnés à deux mois de prison avec sursis pour avoir cyberharcelé un journaliste français. Cette sanction, rappelle celle du tribunal

[1056] Tribunal de grande instance de Bobigny, Chambre 5 sec 3, 20 novembre 2018.
[1057] Cour d'Appel de Limoges, Ch. corr., arrêt du 20 mai 2022.

correctionnel de Bruxelles qui a condamné un homme pour le cyberharcèlement d'une journaliste à une peine de 10 mois de prison avec un sursis probatoire conditionné par le suivi d'une formation contre les violences faites aux femmes. La peine a également été assortie d'une amende de 3000 euros de dommages et intérêts. Plus lourdes ont été des peines pour un célèbre Youtubeur français qui a été condamné en appel à deux ans de prison, dont deux mois ferme, pour avoir cyberharcelé plusieurs influenceurs[1058]. On peut également ajouter une autre affaire dans laquelle un individu a été condamné à un an d'emprisonnement dont six mois ferme, d'interdiction d'entrer en contact avec la victime pour 3 ans et d'exercer l'activité professionnelle de streamer (profession de la victime) pendant 5 ans. Ce que nous constatons est un manque de mesures éducatives et de sensibilisant les personnes condamnées à la gravité de leurs actes.

500. Concernant la haine en ligne, nous pouvons mentionner une décision sur des appels à la haine en ligne contre la communauté asiatique punis d'une amende et de deux jours de stage de citoyenneté[1059]. Les juridictions françaises avaient également condamné un homme politique pour ne pas avoir retiré promptement de son compte Facebook des propos illicites incitant à la haine publiés par un tiers. Le requérant avait été condamné à payer une amende de 3 000 euros. Après s'être pourvu en cassation sans succès, ce dernier a présenté une demande devant la Cour européenne des droits de l'Homme qui a validé le jugement des juridictions internes en statuant qu'il n'y avait pas eu une violation de l'article 10 de la Convention[1060].

501. En dehors des cours nationales, il est intéressant de citer l'arrêt *Perrin c. Royaume-Uni* de la Cour européenne des droits de l'Homme dans lequel elle estime que pour le partage de contenus obscènes sur Internet une peine d'emprisonnement peut être

---

[1058] Cour d'Appel de Versailles, 28 sept. 2021, n° 634.

[1059] Les stages de citoyenneté ont été instaurés par la loi du 9 mars 2004 et sont une alternative à l'emprisonnement.
Ils ont comme objectif de « permettre aux participants de réfléchir aux conséquences de leur comportement ou de leurs actes délictueux, de les sensibiliser aux risques encourus sur le plan civil et pénal, de les responsabiliser dans leur rôle de citoyen, et de leur faire prendre conscience de leurs droits mais également des obligations qu'implique la vie en société ». Voir Ministère de la justice, 9 avril 2013, disponible sur : http://www.justice.gouv.fr/prison-et-reinsertion-10036/les-stages-de-citoyennete-25274.html

[1060] Cour EDH, 2 septembre 2021, *Sanchez c. France*, req. n° 45581/15, confirmé par Cour EDH, GC, 15 mai 2023, *Sanchez c. France*, req. n° 45581/15.

justifiée. En l'espèce il s'agissait de la publication de contenus à caractère sexuel et obscène sur Internet à des fins commerciales. La Cour souligne qu'« étant donné que le requérant pouvait augmenter ses recettes en faisant figurer des photographies obscènes sur la page de prévisualisation, il était raisonnable de la part des autorités internes de considérer qu'une sanction purement financière n'aurait pas eu un effet dissuasif suffisant ou aurait constitué une peine trop légère »[1061].

502. Après avoir donné des exemples sur l'application des dispositions en vigueur par les juridictions françaises, nous pouvons constater que, d'un côté, les peines d'emprisonnement sont le plus souvent des peines de sursis, de l'autre, que le montant des amendes reste bas comparé au maximum qui peut être requis par le juge. Cela pose la question de savoir si ces peines sont vraiment efficaces et surtout si elles ont un effet dissuasif et réparateur pour la victime.

II. L'apparition des nouvelles sanctions et autorités ad hoc

503. Après avoir étudié les sanctions traditionnelles, il s'agira d'analyser des mesures répressives qui s'adaptent au fonctionnement d'Internet et s'attaquent de façon immédiate aux contenus publiés. Ces mesures, qui peuvent être adoptées par des acteurs publics mais aussi privés, permettent de sanctionner certains comportements illicites en rendant inaccessible une page, un site web ou bien un compte. Cependant, nous verrons qu'elles peuvent également porter atteinte aux droits fondamentaux des utilisateurs, lorsqu'elles sont ordonnées pour des contenus non illicites.

504. Afin d'approfondir ces points, il s'agit, d'un côté, d'étudier les sanctions et mesures répressives adoptées contre des contenus publiés sur Internet (**A**). De l'autre, il s'agit d'analyser l'apparition des nouvelles autorités qui participent à l'adoption et à la mise en œuvre de ces mesures (**B**).

[1061] Cour EDH, 18 octobre 2005, *Perrin c. Royaume Uni,* req. n° 5446/03, point 2.

A. Des sanctions aux effets immédiats sur les contenus illicites en ligne

505. Parmi les sanctions qui s'attaquent directement aux contenus publiés en ligne, il s'agira d'analyser les mesures de blocage et de filtrage (**1**) pour ensuite étudier des mesures qui consistent à invisibiliser les contenus illicites ou à exclure du réseau social la personne les ayant publiés (**2**).

1. Les mesures de blocage et de filtrage

506. Si, dans nos précédentes analyses, nous avons surtout étudié le retrait ou la suppression des contenus illicites, il s'agit ici de se concentrer sur le filtrage et le blocage. À la différence du retrait ou de la suppression, le filtrage est un procédé automatisé qui a pour objectif le blocage d'un ou plusieurs contenus, mais également les sites Internet, pages ou plateformes à travers une phase de filtrage et d'identification préalable du contenu. Quant au blocage, il n'implique pas la phase de filtrage[1062]. Le blocage consiste en la mise en place des mesures « pour empêcher un utilisateur final d'avoir accès à certains contenus »[1063]. En d'autres termes, il s'agit de bloquer l'accès à certains sites Internet, d'exclure certaines pages de la recherche par mots-clés sur les moteurs de recherche mais encore de bloquer l'accès à certains contenus spécifiques.

507. Dans notre analyse nous nous concentrerons sur le blocage des contenus en ligne, des plateformes ainsi que des sites Internet. Ces dernières sont pour la plupart mises en œuvre par les fournisseurs de service d'Internet ou les plateformes de leur propre initiative ou sur incitation des gouvernements nationaux. Certains États ont adopté des

---

[1062] Voir Q. VAN ENIS, « Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 136. Ainsi que les conclusions de l'avocat général M. Cruz Villalón dans le cadre de l'affaire *Scarlet c. Sabam*, aff. C-70/10, présentées le 14 avril 2011, § 48. Disponibles sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62010CC0070&from=EN Pour approfondir, voir C. CALLANAN, M. GERCK E, E. DE MARCO et H. DRIES-ZIEK ENHEINER, *Filtrage d'Internet – Équilibrer les réponses à la cybercriminalité dans une société démocratique*, Rapport en ligne. Disponible sur : http://juriscom.net/documents/lib20100520.pdf

[1063] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », A/HRC/17/27, 16 mai 2011, § 29.

mesures spécifiques pour réglementer le filtrage et le blocage sur Internet[1064]. Par exemple, concernant le blocage de contenus pédopornographiques, l'Espagne et Chypre ont adopté des dispositions qui prévoient la délivrance par des tribunaux nationaux d'ordonnances de blocage[1065] ; en Italie, c'est le procureur qui émet une liste de contenus illicites pour qu'il soit procédé à leur blocage[1066]. Dans d'autres États comme la Fédération de Russie, la Turquie ou bien l'Albanie, c'est une autorité publique qui peut rendre de telles ordonnances[1067].

508. Si ces mesures de blocage et de filtrage permettent d'exclure d'Internet des contenus illicites, comme la pédopornographie, le terrorisme ou l'incitation à la violence ; elles peuvent porter atteinte aux droits des intermédiaires ou des internautes[1068]. D'un côté, les intermédiaires pourraient subir une atteinte à leur liberté d'expression[1069]. À cet égard, la Cour européenne des droits de l'Homme reconnaît ce droit aux éditeurs hors ligne. On pourrait envisager qu'une protection similaire pourrait s'appliquer aux intermédiaires d'Internet[1070]. Et, de l'autre, ils pourraient subir une atteinte à leur liberté d'entreprise. C'est ce qu'estime la Cour de justice de l'Union européenne dans l'arrêt *Scarlet Extended*[1071] qui se prononce sur la licéité d'une injonction prononcée par la Société belge des auteurs, compositeurs et éditeurs à l'encontre d'un fournisseur d'accès à Internet. Cette dernière demandait la mise en place d'un système de filtrage des communications électroniques transitant par son service à l'égard de toute sa

---

[1064] Conseil de l'Europe, *Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet*, février 2017, point 1.2.
[1065] *Ibid.* point 1.2.1.1.
[1066] *Ibid.* point 1.2.1.1.
[1067] *Ibid.* point 1.2.1.1.
[1068] Un examen approfondi de l'atteinte aux droits fondamentaux sera fait dans le chapitre VIII. Voir également Q. VAN ENIS, « Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, pp. 139-146.
[1069] Recommandation CM/Rec (2012) 3 du Comité des ministres aux États membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, adoptée le 4 avril 2012, 1139e réunion des délégués des ministres, § 12.
[1070] Q. VAN ENIS, « Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, pp. 139-140.
[1071] CJUE, *Scarlet Extended*, 24 novembre 2011, C-70/ 10. Voir également D. MELISON, « Arrêt « Scarlet » : le filtrage préventif par les fournisseurs d'accès à internet écarté au nom de l'équilibre entre droit d'auteur et libertés fondamentales », *JDE*, 2012/2, n° 186, p. 43-44.

clientèle, à titre préventif, à ses frais et sans limitation de temps[1072]. La Cour se prononce en faveur du fournisseur d'accès en estimant que la mise en place d'une obligation générale de filtrage porterait atteinte, d'une part, à la liberté d'entreprise[1073], et, de l'autre part, à la liberté d'information et aux droits fondamentaux des clients du fournisseur, en particulier le droit à la protection des leurs données personnelles et leur liberté de recevoir ou de communiquer des informations[1074]. En effet, les autres victimes des mesures de filtrage et de blocage peuvent être les internautes, notamment, d'un côté, les auteurs d'un ou plusieurs contenus bloqués qui se verraient privés de leur droit à la liberté d'expression et, de l'autre, les spectateurs qui seraient privés de leur droit de recevoir des informations.

509. Concernant la qualité de victime, la jurisprudence de la Cour européenne des droits de l'Homme et de la Cour de justice de l'Union européenne est contrastée. D'un côté, la première adopte une approche casuistique[1075]. En effet, dans son arrêt *Akdeniz c. Turquie,* elle considère qu'un utilisateur passif ne peut pas se prétendre victime d'une mesure de blocage sous le fondement de l'article 10 de la Convention de sauvegarde des droits de l'Homme[1076]. Avec cet arrêt, la Cour différencie les utilisateurs passifs des utilisateurs actifs. Ces derniers peuvent se voir reconnaître la qualité de victime et se fonder sur l'article 10 pour demander l'annulation de la mesure de blocage[1077]. De l'autre, la Cour de justice de l'Union européenne ne fait pas cette distinction et reconnaît le droit à l'utilisateur de s'opposer à des mesures de blocage[1078].

510. Concernant le droit à la liberté d'expression et de recevoir des informations, nous pouvons citer plusieurs arrêts rendus le même jour par la Cour européenne des droits de

[1072] CJUE, *Scarlet Extended*, 24 novembre 2011, C-70/ 10, point 28.
[1073] *Ibid.*, point 47.
[1074] *Ibid.*, point 50.
[1075] Cour EDH, 1er décembre 2015, *Cengiz et autres c. Turquie*, requêtes n° 48226/10 et n° 14027/11, § 49.
[1076] Cour EDH, 11 mars 2014, *Akdeniz c. Turquie*, requêtes n° 41139/15 et n° 41146/15, § 71 et 78.
[1077] Cour EDH, 1er décembre 2015, *Cengiz et autres c. Turquie*, requêtes n° 48226/10 et n° 14027/11, §§ 50-53.
[1078] CJUE, 27 mars 2014, *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH et Wega Filmproduktionsgesellschaft mbH*, C-314/12.

l'Homme[1079] qui s'est exprimée quant à l'application d'une loi de la Fédération de Russie qui prévoit les critères et la procédure pour bloquer l'accès à un site Internet. Selon la législation russe c'est le procureur qui peut exiger le blocage d'un site, notamment en raison d'une trouble à l'ordre public. Dans l'ensemble des arrêts, la Cour constate la violation de l'article 10 de la Convention, en particulier, parce que la législation ne prévoit ni une garantie procédurale pour protéger les intermédiaires d'une ingérence arbitraire[1080], ni la nécessité de motiver la décision de blocage au regard des motifs de proportionnalité et nécessité[1081]. La Cour constate également que le procureur avait exigé le blocage des sites en entier sans respecter la loi qui prévoyait de limiter le blocage à l'URL spécifique avec les contenus illicites[1082].

511. En somme, le blocage et le filtrage peuvent être des mesures extrêmes mais très efficaces face à des contenus illicites. Cependant elles peuvent mener à des atteintes importantes aux droits fondamentaux des utilisateurs, c'est pour cela que ces mesures doivent être encadrées et, surtout, ne pas être utilisées pour porter une atteinte volontaire à certaines personnes, comme les journalistes, les opposants politiques ou encore les défenseurs des droits humains.

2. L'invisibilisation et l'exclusion des plateformes

512. Nous pouvons également analyser d'autres mesures qu'on pourrait situer entre la sanction et la modération et qui sont adoptées non seulement par les acteurs judiciaires mais également par les acteurs privés. Nous pouvons mentionner ici le blocage géographique et notamment le blocage des hashtags. En effet, les plateformes ont la capacité de bloquer certains hashtags dans certains États afin de censurer les contenus,

---

[1079] Voir Cour EDH, 23 juin 2020, *OOO Flavius and others c. Russia*, req. n° 12468/15, 23489/15 et 19074/16 ; Cour EDH, 23 juin 2020, *Engels c. Russia*, 23 juin 2020, req. n° 61919/16 ; Cour EDH, 23 juin 2020, *Bulgakov c. Russia*, req. n° 20159/15 et Cour EDH, 23 juin 2020, *Vladimir Kharitonov c. Russia*, req. n° 10795/14.
[1080] Voir par exemple : Cour EDH, 23 juin 2020, *OOO Flavius and others c. Russia*, req. n° 12468/15, §40 ainsi que F. DUBUISSON, et J. PIERET, « Société de l'information, médias et liberté d'expression », *JEDH*, 2021/4-5, p. 418-423.
[1081] Voir : Cour EDH, 23 juin 2020, *OOO Flavius and others c. Russia*, req. n° 12468/15, §41.
[1082] Voir notamment : Cour EDH, 23 juin 2020, *OOO Flavius and others c. Russia*, req. n° 12468/15, §32, ainsi que Cour EDH, 23 juin 2020, *Bulgakov c. Russia*, req. n° 20159/15, §34.

notamment à la demande des États ou des gouvernements. Cela a été le cas en France en 2012 pour l'hashtag #unbonjuif avec lequel les utilisateurs relayaient des messages haineux antisémites contre les personnes juives. En France, la plateforme Twitter a bloqué cet hashtag et les contenus publiés avec ce dernier n'étaient plus accessibles pour les utilisateurs avec une adresse IP localisée en France[1083]. Cette invisibilisation est possible également dans d'autres plateformes et vis-à-vis d'autres types de contenus. Par exemple, sur la plateforme YouTube, il est possible de restreindre l'accès à certaines vidéos. Sur Facebook, la visibilité des contenus problématiques qui ne portent pas atteinte aux standards de communauté, comme la désinformation ou le recollage[1084], est également dégradée[1085]. Les deux plateformes offrent également la possibilité aux propriétaires des pages ou des chaînes de masquer les commentaires de certains utilisateurs. L'invisibilisation des contenus est une forme de régulation mais également de sanction pour les utilisateurs qui en sont la cible et qui, le plus souvent, n'en sont pas informés. Ces invisibilisations ont touché des femmes et d'hommes politiques de tous bords mais également des activistes et défenseurs des droits humains[1086]. Cela pose des questions quant à la légitimité des plateformes de choisir ce qui « mérite d'être vu et discuté »[1087], en particulier parce que leurs décisions sont prises sans aucune transparence. Ainsi, ces méthodes sont inquiétantes pour le débat démocratique en ligne. En effet, les plateformes ont un véritable impact politique.

513. L'exclusion des réseaux sociaux consiste en la possibilité pour les plateformes de suspendre et désactiver les comptes des utilisateurs, des pages ou des groupes de façon temporaire ou permanente. Ces suspensions peuvent se faire de trois manières. Premièrement, cela peut avoir lieu entre utilisateurs, c'est-à-dire un utilisateur bloque l'accès à son profil à un autre utilisateur. Deuxièmement, l'utilisateur peut être exclu du

---

[1083] R. BADOUARD, *Les Nouvelles lois du web,* Modération et censure, Éditions du Seuil et La République des Idées, octobre 2020, p. 61.
[1084] Cela fait partie de la stratégie de Facebook "Remove, Reduce, Inform », pour plus d'informations voir : G. ROSEN, *Remove, Reduce, Inform: New Steps to Manage Problematic Content,* META website, 10 avril 2019. Disponible sur : https://about.fb.com/news/2019/04/remove-reduce-inform-new-steps/#reduce
[1085] R. BADOUARD, *Les Nouvelles lois du web,* Modération et censure, Éditions du Seuil et La République des Idées, octobre 2020, p. 62.
[1086] R. BADOUARD, *Shadow ban. L'invisibilisation des contenus en ligne,* Revue Esprit, novembre 2021. Disponible sur : https://esprit.presse.fr/article/romain-badouard/shadow-ban-l-invisibilisation-des-contenus-en-ligne-43629
[1087] *Ibid.*

réseau social par la plateforme elle-même et enfin, cela peut être le fruit d'une loi nationale qui restreint l'accès aux plateformes à certains individus, c'est notamment le cas aux États-Unis pour des personnes ayant déjà été condamnées pour des crimes ou délits de nature sexuelle[1088].

514. Dans le cadre de l'exclusion par les plateformes, ces dernières peuvent décider de désactiver les comptes des utilisateurs lorsqu'ils portent atteinte aux règles et standards de communauté[1089]. Plusieurs exemples peuvent être mentionnés. Le plus emblématique est le bannissement de plusieurs plateformes de l'ancien président des États-Unis, Donald J. Trump[1090]. Ce dernier a été suspendu des plateformes comme Facebook, Twitter et YouTube à la suite de la prise du Capitole à Washington le 6 janvier 2021 par des manifestants qui considéraient la victoire de Joseph R. Biden comme illégitime. Selon les réseaux, les messages publiés par l'ancien président étaient susceptibles d'inciter à la violence et, pour cela, avaient enfreint leurs règles internes. La suspension du compte personnel de Donald Trump semblait être temporaire mais ensuite les plateformes ont décidé de la poursuivre voir même de le bannir définitivement. En effet, les responsables de Twitter ont décidé de le suspendre de façon permanente jusqu'à l'arrivée du nouveau PDG Elon Musk qui a réactivé son compte en novembre 2022. Le réseau Meta a choisi de le suspendre pour deux ans, jusqu'à janvier 2023[1091]. Cette suspension était le résultat non seulement des publications du 6 janvier mais également de plusieurs violations de la part de l'ancien président et de son attitude récidiviste. Il est intéressant de souligner que Facebook, afin d'adopter sa décision concernant le blocage, a demandé des recommandations à son Conseil de Surveillance de Facebook (Oversight Board), autorité indépendante que nous allons étudier dans les développements qui suivrons. Nous pouvons également citer d'autres suspensions de personnalités célèbres,

---

[1088] Voir : E. CELESTE, Digital punishment: social media exclusion and the constitutionalising role of national courts, *International Review of Law, Computers & Technology*, 35:2, 2021, pp. 164-166.
[1089] Voir par exemple la politique de Twitter. Disponible ici : https://help.twitter.com/fr/managing-your-account/suspended-twitter- Ainsi que la politique de Meta (Facebook et Instagram) concernant la suspension des comptes des utilisateurs. Disponible ici : https://transparency.fb.com/fr-fr/enforcement/taking-action/disabling-accounts/ Et de la suppression des pages et des groupes. Disponible ici : https://transparency.fb.com/fr-fr/enforcement/taking-action/removing-pages-groups/
[1090] H. DENHAM, *These are the platforms that have banned Trump and his allies*, The Washington Post, janvier 2021. Disponible sur : https://www.washingtonpost.com/technology/2021/01/11/trump-banned-social-media/
[1091] Un examen de la proportionnalité sera proposé dans le chapitre VIII de cette thèse.

comme le chanteur français Booba qui a définitivement été exclu d'Instagram suite à plusieurs atteintes aux règles de la plateforme. Des personnalités non publiques sont également exclues. À titre d'exemple, nous pouvons mentionner plusieurs arrêts des cours allemandes qui ont confirmé la suspension des comptes suite à des publications haineuses. C'était le cas lorsque deux utilisateurs récidivistes ont publié, d'un côté, un post pour demander l'utilisation des canons à eau contre les demandeurs d'asiles[1092] et, de l'autre, une publication qui reprenait le discours de Viktor Orbán, premier ministre hongrois, pour dire que les réfugiés syriens étaient des envahisseurs[1093]. Enfin, pour donner un exemple de la suspension d'une page, nous pouvons mentionner celle de « CasaPound Italia », un parti politique italien d'extrême droite et d'inspiration néo-fasciste dont la page Facebook avait été suspendue pour avoir publié des contenus allant à l'encontre des règles de Meta[1094].

B. Des nouvelles autorités s'ajoutant au processus de sanction

515. Depuis des années, on constate la multiplication d'autorités compétentes en matière de contrôle et de sanction contre les comportements illicites en ligne. Nous avons vu l'apparition des juridictions spécialisées sur les violences en ligne, mais également l'essor des nouvelles autorités au sein des plateformes qui n'ont pas de compétence juridique *stricto sensu* mais qui influencent les décisions concernant le retrait et le blocage des contenus ainsi que des sanctions à l'encontre des utilisateurs des plateformes.

516. En premier lieu concernant les autorités judiciaires, il convient d'analyser la création du pôle national de lutte contre la haine en ligne du tribunal judiciaire de Paris. La création de ce pôle est prévue par la loi du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet[1095] et par le décret du 24 novembre 2020 qui désigne la compétence

[1092] LG Frankfurt/Main, 10.09.2018 - 2–03 O 310/18 2018 cité par E. CELESTE, Digital punishment: social media exclusion and the constitutionalising role of national courts, *International Review of Law, Computers & Technology*, 35:2, 2021, p. 166.
[1093] Voir OLG München, 17.07.2018 - 18 W 858/18 cité par E. CELESTE, Digital punishment: social media exclusion and the constitutionalising role of national courts, *International Review of Law, Computers & Technology*, 35:2, 2021, p. 166.
[1094] F. Z. GIUSTINIANI, I limiti alla libertà di espressione nell'agorà politica virtuale e la cyberviolenza comme nuova forma di violenza domestica, *Nomos*, 1-2020.
[1095] Article 10 de la loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

tribunal judiciaire de Paris[1096]. Ce nouveau pôle qui, depuis son entrée en fonction le 4 janvier 2021, a été saisi de plus de 140 dossiers, centralise le traitement des affaires plus complexes en matière de haine en ligne et vient en soutien aux autres juridictions sur ces questions[1097]. Il est compétent selon la complexité de la procédure, due, entre autres, à la technicité de l'enquête et à la multiplicité des acteurs, mais également au trouble à l'ordre public résultant de l'infraction, par exemple lors d'affaires médiatiques[1098]. De plus, ce pôle est l'interlocuteur judiciaire exclusif de la Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) ainsi que des représentants des plateformes en ligne[1099]. Si cette création est saluée par la majeur partie des spécialistes, certains, comme l'avocat Eric Morain, plaident pour la « création de juridictions interrégionales spécialisées sur le numérique »[1100] ou, comme l'avocat Philippe Coen, pour la nécessité de travailler plus sur la prévention et la formation[1101].

517. En second lieu, nous pouvons traiter de l'essor d'autorités privées, comme le Conseil de Surveillance de Facebook (Oversight Board). Ce dernier a vu le jour en septembre 2019 et se compose au maximum de 40 membres dont certains ont été sélectionnés par Meta et d'autres par les membres du Conseil eux-mêmes. Aujourd'hui, le Conseil compte 23 membres provenant du monde entier et avec des profils très différents (chercheurs, professeurs, directeurs d'ONG, avocats ou encore écrivains). Ce dernier a comme mission de « protéger la liberté d'expression en prenant des décisions indépendantes et fondées sur des principes concernant des contenus importants et en émettant des avis consultatifs sur les politiques de contenu de Facebook »[1102]. Il s'agit d'une autorité indépendante avec un budget propre de 130 millions de dollars pour six

---

[1096] Voir décret n°2020-1444 du 24 novembre 2020.
[1097] Pour plus d'informations, voir : Ministère de la justice, Lutte contre la haine en ligne, Un an au service de la justice, 28 juin 2021. Disponible sur : http://www.justice.gouv.fr/le-garde-des-sceaux-10016/archives-2021-eric-dupond-moretti-13017/lutte-contre-la-haine-en-ligne-34445.html
[1098] Création d'un pôle national dédié à la lutte contre la haine en ligne au tribunal judiciaire de Paris, Lexis Veille, 30 novembre 2020. Disponible sur : https://www.lexisveille.fr/creation-dun-pole-national-dedie-la-lutte-contre-la-haine-en-ligne-au-tribunal-judiciaire-de-paris
[1099] G. THIERRY, « Le nouveau pôle spécialisé contre la haine en ligne, une structure très attendue », *DALLOZ Actualité*, 3 février 2021. Disponible sur : https://www.dalloz-actualite.fr/flash/nouveau-pole-specialise-contre-haine-en-ligne-une-structure-tres-attendue#.Yv5PaexBzyh
[1100] *Ibid.*
[1101] *Ibid.*
[1102] Conseil de surveillance, Introduction, *Oversight Board Bylaws*, janvier 2022, p. 5. Disponible sur : https://about.fb.com/wp-content/uploads/2020/01/Bylaws_v6.pdf Traduction de l'autrice.

ans. Le Conseil est compétent pour examiner, d'un côté, les décisions des utilisateurs qui sont en désaccord avec les décisions de Meta et ont épuisé les voies de recours auprès de ce dernier, et de l'autre, celles qui lui seront soumises par Meta[1103]. De plus, à partir d'avril 2021, le mandat du Conseil a été élargi aux demandes des utilisateurs concernant l'effacement des contenus qui n'ont pas été supprimés par Facebook et Instagram[1104]. Le Conseil peut également émettre des « policy advisory statements » (« déclarations politiques consultatives » en français) sur les politiques de la plateforme. Selon la Charte établissant le Conseil, les décisions prises par ce dernier sont contraignantes pour Meta à condition qu'elles n'enfreignent pas la loi. Cependant, les déclarations politiques consultatives émises par le Conseil seront considérées comme des recommandations. Ainsi, il est prévu que le Conseil ait la possibilité d'amender la Charte. Cependant, toute modification doit se faire avec l'accord de Meta, ce qui restreint grandement la liberté et l'indépendance de l'institution[1105].

518. Certains auteurs critiquent l'instauration de cette institution ou certains aspects de ce Conseil. C'est le cas de l'organisation Article 19 qui, malgré la composition internationale du Conseil, émet des réserves concernant « la compréhension de la complexité des contextes locaux et des dimensions sociales, politiques, historiques, culturelles et linguistiques […] pour prendre des décisions éclairées sur la modération des contenus »[1106]. D'autres se questionnent sur la véritable indépendance de l'institution, compte tenu du fait que certains membres du Conseil sont élus par Meta et que la Charte stipule que « le Conseil examinera et se prononcera sur le contenu conformément aux politiques de contenu et aux valeurs de Facebook »[1107]. En effet, cela

[1103] Conseil de surveillance, *Oversight Board Bylaws*, janvier 2022, Article 1, section 3, p. 12.
[1104] Voir : Conseil de surveillance, *Le Conseil de surveillance accepte les appels des utilisateurs au sujet de contenu qu'ils aimeraient voir supprimé de Facebook et Instagram*, avril 2021. Disponible sur : https://oversightboard.com/news/267806285017646-the-oversight-board-is-accepting-user-appeals-to-remove-content-from-facebook-and-instagram/
[1105] Article 5, section 1 du *Oversight Board Bylaws*, janvier 2022, p. 29. Voir également K. KLONICK, The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression, *Yale Law Journal*, Vol. 129, No. 2418, 2020, p. 2435.
[1106] Voir : Article 19, *Facebook: New oversight board is not sufficient to safeguard freedom of expression online*, 18 September 2019. Disponible sur : https://www.article19.org/resources/facebook-new-overs ight-board-is-not-sufficient- to-safeguard-freedom-of-expression-online/
[1107] Article 1, section 3 du du *Oversight Board Bylaws*, janvier 2022, p. 12.

pourrait compromettre le traitement des contenus et la crédibilité du Conseil[1108]. Pour d'autres encore, le problème n'est pas dans la modération mais dans le modèle économique des plateformes[1109]. À cet égard, les actions du Conseil sans un changement de modèle économique ne porteront pas à des grands résultats. Enfin, pour Christophe Deloire, secrétaire général de Reporters Sans Frontières, la création de ces types d'institution « est symptomatique de la carence régulatrice des États démocratiques »[1110]. Pour lui, les compétences du Conseil sont très limitées, en particulier du fait qu'il ne s'intéresse pas aux mécanismes algorithmiques de la plateforme qui sont à la base de l'amplification ou l'invisibilisation de certains contenus et de fait, la clé pour la modération des contenus. À cet égard, un groupe d'experts réunit par le Forum de l'information et la démocratie, lancé par Reporters Sans Frontières, conseille une refonte de la gouvernance d'Internet pour améliorer le régime de responsabilité[1111]. Ils préconisent, au niveau national, la création d'une autorité régulatrice indépendante, d'un mécanisme de signalement de comportements et contenus illicites ainsi que l'accès à un système judiciaire indépendant avec des institutions spécialisés (parquet et magistrats)[1112]. Au niveau international, ils recommandent la création d'un organisme transnational qui aurait trois mandats : la régulation, le règlement des conflits et la conduite des enquêtes. Cet organisme transnational devrait être composé par des représentants des plateformes, de la société civile, des États ainsi que des organisations internationales concernées[1113].

519. Malgré les critiques, il faut souligner que le Conseil crée par Meta a, depuis le début de ses activités en octobre 2020, augmenté fortement son activité d'année en année.

[1108] M. LATONERO, Can Facebook's Oversight Board Win People's Trust?, *Harvard Business Review*, 29 janvier 2020. Disponible sur : https://hbr.org/2020/01/can-facebooks-oversight-board-win-peoples-trust
[1109] Voir : D. GHOSH, Facebook's Oversight Board Is Not Enough, *Harvard Business Review*, 16 octobre 2019. Disponible sur : https://hbr.org/2019/10/facebooks-oversight-board-is-not-enough
Voir également les propos de Joe Westby dans M. LATONERO, Can Facebook's Oversight Board Win People's Trust?, *Harvard Business Review*, 29 janvier 2020. Disponible sur : https://hbr.org/2020/01/can-facebooks-oversight-board-win-peoples-trust
[1110] RSF, *L'« oversight board » de Facebook est une solution à très court terme, mais il faut vite passer à autre chose*, 7 juin 2021. Disponible sur : https://rsf.org/fr/l-oversight-board-de-facebook-est-une-solution-%C3%A0-tr%C3%A8s-court-terme-mais-il-faut-vite-passer-%C3%A0
[1111] Forum on Information and Democracy, *Accountability regimes for social networks and their users*, Chapter 4: Governance, Policy framework, September 2022, pp. 34-42.
[1112] *Ibid.* pp. 35-38.
[1113] *Ibid.* pp. 38-42.

Depuis cette date jusqu'à mars 2022, le Conseil a reçu 1,6 millions de cas. De janvier à mars 2022, les utilisateurs ont soumis environ 480 000 cas[1114]. Au total, le Conseil a émis 36 décisions[1115] sur une variété des sujets : discours de haine, apologie du terrorisme mais également nudité et contenus violents. Malgré certaines limites, il est intéressant de souligner que cette autorité est l'une des seules qui a poussé la plateforme Meta à être plus transparente, on pense notamment à la décision de la suspension du compte de Donald Trump[1116]. De plus, le Conseil continue de se mobiliser et de demander des comptes face aux lacunes en matière de transparence, notamment après les révélations de Frances Haugen[1117] et à la modération des contenus des personnalités célèbres[1118].

[1114] Conseil de surveillance, *Oversight Board publishes transparency report for first quarter of 2022*, août 2022. Disponible sur : https://oversightboard.com/news/572895201133203-oversight-board-publishes-transparency-report-for-first-quarter-of-2022/
[1115] L'ensemble des décisions du Conseil est disponible sur : https://www.oversightboard.com/decision/, consulté le 22 avril 2023.
[1116] V. NDIOR, « Le Conseil de surveillance de Facebook et la protection des libertés », *RDLF 2022*, chron. n°23.
[1117] Voir chapitre V de cette thèse.
[1118] Conseil de surveillance, *To treat users fairly, Facebook must commit to transparency*, Septembre 2021. Disponible sur : https://www.oversightboard.com/news/3056753157930994-to-treat-users-fairly-facebook-must-commit-to-transparency/

Section II : Des mesures répressives inadéquates pour la réparation au préjudice subi

520. Nous avons étudié plusieurs typologies de sanction et leur mise en œuvre. Le constat que nous faisons est que les mesures existantes ne prennent pas assez en compte la dimension « cyber » et notamment les conséquences des cyberviolences. À cet égard, il s'agit d'étudier quels types d'actions devraient être menées par les États et les acteurs privés pour améliorer les mesures répressives.

521. Nous constatons que, malgré la prise de conscience des acteurs étatiques et privés du besoin d'adopter des sanctions efficaces contre les cyberviolences, les conséquences de ces dernières sont rarement prises en compte. Il serait nécessaire d'adopter des mesures répressives qui prennent réellement en compte les conséquences des comportements illicites en ligne pour réparer le préjudice subi (**§I**), ainsi que des sanctions préventives axées sur l'éducation (**§II**).

I. La nécessaire adoption de sanctions prenant en compte les conséquences des cyberviolences

« On a parlé du niveau de violence que ça a pu atteindre, mais je voudrais parler de la durée. Ça a duré extrêmement longtemps. Peut-être que ça dure encore, mais je ne peux pas le savoir, parce que j'ai quitté les réseaux sociaux, alors que c'était un outil de travail pour moi. […] Je n'ai pas pu dormir chez moi après qu'on a donné des coups dans ma porte en pleine nuit. Il fallait que je mente à ma fille. Je ne pouvais pas lui dire que quelqu'un menaçait de violer sa mère avec des tessons de bouteille devant elle. […] Ma vie a changé de manière très claire. On peut couper Twitter, mais on ne peut pas arrêter de se déplacer dans la rue. On se dit que ces gens-là prennent le métro. Qu'ils peuvent croiser notre chemin. On est vulnérable partout. Partout, partout. Et parfois, on reçoit une notification, qui vous remet dans la boucle » - Nadia Daam[1119].

[1119] E. COSTA, Au procès des cyberharceleurs de Nadia Daam, les remords peu convaincants des prévenus, SLATE, 4 juillet 2018. Disponible sur : https://www.slate.fr/story/164132/societe-medias-proces-nadia-daam-journaliste-harcelement-en-ligne-menaces-mort-forum-jeuxvideo

522. Comme pour les comportements illicites hors ligne, les cyberviolences ont des conséquences sur la vie des victimes. Aux conséquences graves découlant des infractions hors ligne, s'ajoutent des conséquences propres à la dimension « cyber »[1120].

523. En premier lieu, les comportements illicites en ligne ont des conséquences directes sur le comportement des victimes. En particulier, elles peuvent causer un état de stress, d'isolement, des problèmes d'assiduité et de concentration à l'école ou au travail. En deuxième lieu, elles causent un sentiment de tristesse, d'énervement, de paranoïa ou bien d'insécurité. En troisième lieu, elles ont un impact sur la santé mentale, psychologique et physique des victimes. Elles mènent à une perte de l'estime de soi, à des symptômes de dépression et elles peuvent conduire jusqu'à des idées suicidaires ou au suicide[1121]. Enfin, elles ont également un impact social, notamment sur la réputation de la victime[1122]. Par exemple, lors de la publication d'images à caractère sexuel sans le consentement, la victime vit dans un état de peur et d'angoisse que ces images continuent de circuler dans le même réseau social ou dans d'autres plateformes. Sa réputation peut être compromise et elle pourrait subir des conséquences négatives à l'école ou au travail, dont le licenciement[1123]. Ainsi, les raids numériques ou le cyberharcèlement peuvent avoir des conséquences sur la confiance en soi des victimes et leur l'utilisation d'Internet.

[1120] Voir le Chapitre I de cette thèse.

[1121] Voir notamment T. BERAN and Q. LI, « The relationship between bullying and cyberbullying », *The Journal of Student Wellbeing*, 1(2), 2007. Voir également K. J. MITCHELL, M. YBARRA, and D. FINKELHOR, « The relative importance of online victimization in understanding depression, delinquency, and substance use », *Child maltreatment*, 12(4), 3, 2007 ; M. YBARRA and K. J. MITCHELL, « Prevalence and frequency of Internet harassment instigation: Implications for adolescent health. Journal of Adolescent Health », 41, 2007 ; Ö. ERDUR-BAKER, « Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools ». *New media & society*, 12(1), 2010 ; Y. KATSUMATA, T. MATSUMOTO, M. KITANI, and T. TAKESHIMA, « Electronic media use and suicidal ideation in Japanese adolescents », *Psychiatry and Clinical Neurosciences*, *62*(6), 2008 ; S. HINDUJA and J.W PATCHIN, « Bullying, cyberbullying, and suicide », *Archives of suicide research*, 14(3), 2, 2010.

[1122] A. DIALLO, *A Guide for Women and Girls to Prevent and Respond to cyberviolence*, UN WOMEN, novembre 2021, p. 4. Voir également A. VAN DER WILK, *Protecting women and girls from violence in the digital age*, The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, Council of Europe, December 2021, p. 7.

[1123] En Italie, la directrice d'une école ayant licencié une professeure qui avait été victime de partage de contenus à caractère sexuel sans le consentement à été condamné à 12 mois de prison avec sursis et également un parent de l'école qui avait rediffusé les photos à d'autres parents de l'école. Voir, *Maestra vittima di revenge porn licenziata: condannate la preside e la madre di un'alunna a Torino*, il Fatto Quotidiano, 19 février 2021. Disponible sur : https://www.ilfattoquotidiano.it/2021/02/19/revenge-porn-maestra-licenziata-condannate-la-preside-e-la-madre-di-unalunna-a-torino/6106956/

Plusieurs études le prouvent, notamment une enquête menée par Plan international auprès des 14 000 filles âgées de 15 à 25 ans dans 22 États du monde. Cette dernière montre que les 42 % des filles interrogées déclarent que le cyberharcèlement subi diminue leur estime de soi et qu'il leur crée un stress mental et émotionnel[1124]. Cela les mène également à quitter les réseaux et de fait à s'auto-censurer par peur d'être à nouveau attaquées en ligne. Le même sort est destiné aux défenseurs des droits humains ainsi qu'aux journalistes, en particulier les femmes, comme le démontre une enquête menée par l'UNESCO qui montre que près de trois femmes journalistes interrogées sur quatre sont victimes de violences en ligne[1125]. La participation à la vie politique et au débat public est également affaiblie par les attaques répétées à l'encontre des femmes[1126], mais également d'autres groupes à cause de leur appartenance à une ethnie, à une religion ou bien à cause de leur identité de genre ou orientation sexuelle.

524. Comme le note le Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO) dans les États où il existe une législation sur les cyberviolences, « la sanction des abus et des dommages causés par la violence en ligne ou au moyen de la technologie se concentrent souvent sur la protection de la sécurité, de la réputation ou des biens des victimes »[1127]. Il ajoute que « de nombreuses lois nationales ne prennent pas en considération les autres conséquences importantes des violences en ligne, telles que les préjudices sociaux, économiques, psychologiques et en matière de participation »[1128].

525. En effet, les sanctions adoptées par les États et les plateformes devraient être effectives et permettre aux victimes d'obtenir une réparation adéquate. Comme le souligne le plan d'action de Rabat « les États devraient garantir que les personnes ayant été victimes d'un préjudice réel résultant d'incitation à la haine puissent bénéficier d'un

---

[1124] Plan international, *Libres d'être en ligne*, La situation des filles dans le monde, 2020, p. 28. Disponible en ligne sur : https://plan-international.org/uploads/2022/02/sotwgr2020-commsreport-fr.pdf
[1125] J. POSETTI, N. SHABBIR et autres, *The Chilling: Global trends in online violence against women journalists*, UNESCO, 2021.
[1126] GREVIO, Recommandation générale n°1 sur la dimension numérique de la violence à l'égard des femmes adoptée le 20 octobre 2021, point 13.
[1127] *Ibid*. point 16.
[1128] *Ibid*. point 16.

recours effectif, y compris d'un recours civil ou non judiciaire, pour des réparations »[1129]. Cela devrait valoir pour une infraction liée à la haine en ligne mais également aux autres contenus illicites dont sont exposés les utilisateurs.

526. Ainsi, les recommandations du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, M. Frank La Rue, formulées en 2012 sont malheureusement encore d'actualité. Il envisageait que les réparations soient « suffisantes, rapides et proportionnées à la gravité de l'expression » et il prévoyait, entre autres, des mesures capables de restaurer la réputation de la victime[1130].

527. C'est pour cela que les sanctions devraient prendre en compte les conséquences sur les victimes, comme la nécessité de suivre des soins psychologiques, le manque à gagner dû au stress et à l'angoisse ou encore la détérioration des notes scolaires. Rarement, comme nous l'avons vu dans les exemples des jurisprudences dans les juridictions françaises, ces conséquences sont prises en compte. Et si elles le sont, les peines, notamment les dommages et intérêts, sont dérisoires et ne permettent pas aux victimes de pallier à leurs besoins. De plus, quid de la peur de voir les contenus réapparaître en ligne ? Ou bien de l'inefficacité des contenus désindexés[1131] qui peuvent porter atteinte à la réputation d'un individu pendant des années.

528. Cela nous amène également à parler du caractère préventif de la sanction, notamment de ses effets sur la récidive.

[1129] Plan d'action de Rabat sur l'interdiction de tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence, Conclusions et recommandations issues des quatre ateliers d'experts organisés par le Haut-Commissariat des Nations Unies pour les droits de l'Homme en 2011 et adoptés par les experts à Rabat, Maroc le 5 octobre 2012, point 33. Disponible sur : https://www.ohchr.org/sites/default/files/Rabat_draft_outcome_FR.pdf Voir rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, point 55.

[1130] Voir le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/67/357 du 7 septembre 2012, point 48.

[1131] Voir §§ 45-61 de cette thèse.

II. La nécessaire adoption des mesures répressives préventives

529. Le Groupe sur la cyberviolence du Conseil de l'Europe affirme que « en ce qui concerne la détermination de la peine, […] les pays ne punissent pas toujours la cyberviolence dans une mesure qui soit adaptée au préjudice causé »[1132]. Pour y remédier, plusieurs mesures pourraient être adoptées par les juridictions internes. D'abord, il faudrait que le droit pénal des États contienne des dispositions qui définissent et sanctionnent clairement les comportements illicites en ligne dirigés contre l'ensemble de la population, en particulier, les personnes plus vulnérables et exposées à la haine en ligne. Ensuite, il faudrait que le droit civil et administratif soit adapté lorsque les comportements illicites ne relèvent pas de la sphère pénale. Enfin, il serait nécessaire de systématiser l'accompagnement de sanctions telles l'emprisonnement ou les amendes par le suivi de sensibilisations et des formations sur les cyberviolences et, en particulier, sur les comportements illicites tenus sur Internet. À l'image des formations sur les violences faites aux femmes auprès des hommes auteurs des violences conjugales, il serait souhaitable de prévoir des formations sur la haine en ligne et sur ses conséquences pour que la sanction ait une fonction pédagogique.

530. Les acteurs privés ont également un rôle à jouer dans la répression préventive et symbolique. En effet, les plateformes pourraient prévoir des mesures qui permettraient aux utilisateurs d'avoir une réparation complémentaire à celle des voies judiciaires classiques et qui n'est pas toujours adaptée aux conséquences de la sphère « cyber ». Les plateformes « doivent concevoir des produits de qualité, qui protègent l'autonomie des utilisateurs, leur sécurité et leur droit à la liberté d'expression afin de compenser les incidences de violations passées »[1133]. Par exemple, elles peuvent envisager que, pour réhabiliter un utilisateur suspendu à cause d'un comportement illicite, il ait l'obligation

---

[1132] Conseil de l'Europe, *Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet*, février 2017, p. 38.
[1133] Voir le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019, point 54.

de présenter ses excuses à la victime[1134] et passer une formation créée par la plateforme sur la haine en ligne ou bien, sur un sujet spécifique selon l'infraction commise.

531. De plus, lorsque des contenus sont offensants et préjudiciables mais ne sont pas considérés, par les droits nationaux ou les standards de communautés des plateformes, d'une gravité telle à justifier le retrait, il serait nécessaire de prévoir des mesures alternatives. Par exemple, celles qui sont conseillées par le Comité des ministres du Conseil de l'Europe aux États membres : « des contre-discours et autres contre-mesures ; des mesures favorisant le dialogue et la compréhension interculturels, également par le biais des médias et des réseaux sociaux ; et des activités pertinentes d'éducation, de partage d'informations et de sensibilisation »[1135].

532. Cependant, les sanctions prévues par la loi, bien qu'elles puissent avoir une fonction préventive, ne suffisent pas. Comme l'avait souligné en 2012, M. Frank La Rue rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression « les codes pénaux ne suffisent toutefois pas à résoudre à eux seuls les problèmes de société soulevés par l'incitation à la haine. Bien que l'interdiction légale et la possibilité d'engager des poursuites soient essentielles dans certains cas, il importe […] aussi de disposer d'un ensemble de moyens plus efficaces, c'est-à-dire de mesures positives à même de traiter les causes profondes de la haine sous ses différentes formes, dont des programmes sociaux de lutte contre les inégalités et la discrimination structurelle qui doivent s'adresser au plus grand nombre, associées à des prescriptions et dispositifs créatifs visant à promouvoir une culture de paix et de tolérance à tous les niveaux »[1136].

[1134] *Ibid.* point 54.
[1135] Recommandation CM/Rec (2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine adoptée par le Comité des Ministres le 20 mai 2022, lors de la 132e Session du Comité des Ministres, point 3 (b).
[1136]Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/67/357 du 7 septembre 2012.

Conclusion du Chapitre VII

533. Les sanctions juridiques prévues contre les individus pour la publication de contenus illicites en ligne ne semblent pas encore reconnaître les spécificités et les conséquences des violences en ligne. En effet, les sanctions adoptées par les autorités nationales sont souvent les mêmes que celles utilisées pour les comportements illicites hors ligne. De plus, les mesures prises par les réseaux sociaux ont l'avantage d'avoir un effet immédiat et efficace pour le retrait des contenus illicites, mais si elles ne sont pas bien encadrées elles peuvent porter atteinte aux droits fondamentaux des utilisateurs. Enfin, la question de la pédagogie et de l'éducation se pose lorsque les contenus illicites sont retirés sans que des mesures éducatives soient prévues.

Chapitre VIII : La recherche d'une sanction proportionnée et respectueuse des droits fondamentaux

534. Comme affirmé par les traités du Conseil de l'Europe, les sanctions doivent être « effectives, proportionnées et dissuasives »[1137]. Pour cela, la proportionnalité est une caractéristique clé des mesures répressives adoptées par les autorités nationales. Cela est confirmé également par la Charte des droits fondamentaux de l'Union européenne qui rappelle que « toute limitation de l'exercice des droits et libertés […] doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. *Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui* »[1138].

535. Face à la nécessité d'adopter et de mettre en œuvre des mesures répressives proportionnées, il s'agira d'étudier cette dimension à travers le blocage et le filtrage (**Section I**). Pour ensuite, s'intéresser à la proportionnalité à travers la mise en balance des droits et libertés fondamentaux dans l'adoption des sanctions (**Section II**).

[1137] Voir par exemple l'article 13 de la Convention du Conseil de l'Europe sur la cybercriminalité STCE n° 185, Budapest, 23 novembre 2001 ; l'article 45 de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, STCE n° 210, Istanbul, 11 mai 2011 ; ainsi que l'article 27 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, STCE n° 201, Lanzarote, 25 octobre 2007.

[1138] Article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, 18 décembre 2000. Italique par l'autrice.

Section I : Vers une sanction proportionnée et respectueuse des droits fondamentaux

536. Dans les développements précédents, nous avons étudié le caractère adéquat et préventif des sanctions. Il s'agit maintenant de s'intéresser à leur proportionnalité. Nous nous concentrerons sur l'atteinte causée par les mesures de filtrage et blocage et sur la jurisprudence européenne (**§I**). En particulier, nous nous pencherons sur l'application de la proportionnalité dans la mise en œuvre de ces mesures (**§II**).

I. Le cas du blocage et du filtrage, des mesures portant atteinte aux libertés fondamentales

537. Dans les développements précédents, nous avions analysé le fonctionnement des mesures de filtrage et de blocage. Ces mesures peuvent porter atteinte aux droits fondamentaux des utilisateurs, comme cela est le cas pour le retrait des contenus non illicites.

538. Le blocage et le filtrage peuvent être dirigés vers des contenus identifiés, une page web, un profil dans les réseaux sociaux ou plus généralement vers un site Internet. Ces mesures peuvent être prises par des plateformes ou par des fournisseurs de moteurs de recherche à la demande de pouvoirs publics ou des personnes physiques pour respecter des obligations légales mais également par leur propre initiative[1139]. À titre d'exemple, le blocage d'un site Internet équivaudrait à la fermeture d'un journal, ce qui représente pour la Cour européenne des droits de l'Homme une ingérence préventive disproportionnée[1140]. Ces mesures peuvent porter atteinte à plusieurs droits, entre autres, à la liberté d'expression.

539. D'abord, les mesures de blocage et filtrages peuvent toucher les intermédiaires de service lorsque le blocage empêche leurs utilisateurs de répandre leurs contenus. Un parallèle peut être fait avec la presse écrite, en effet, la Cour européenne des droits de

[1139] Voir recommandation CM/Rec (2012) 3 du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, adoptée par le Comité des Ministres le 4 avril 2012, lors de la 1139e réunion des Délégués des Ministres, point 14.
[1140] Cour EDH (2e sect.), 20 octobre 2009, *Ürper et autres c. Turquie*, req n° 14526/07, §§ 39-45.

l'Homme avait reconnu que les éditeurs participaient pleinement à la liberté d'expression des auteurs et « disposaient ainsi d'un *locus standi* leur permettant d'alléguer devant la Cour de Strasbourg une violation de ce droit »[1141]. Ensuite, ces mesures peuvent porter atteinte aux droits des utilisateurs en leur qualité d'auteur ou de propriétaire des contenus ou du site, ce qui a été reconnu par la Cour européenne des droits de l'Homme comme un « effet collatéral important »[1142]. Plusieurs cas d'ordonnances de blocage et de filtrage ont montré l'ampleur des atteintes aux libertés et aux droits fondamentaux des utilisateurs.

Nous pouvons parler des blocages des sites Internet ordonnés par les États. Ces mesures sont souvent utilisées comme des armes politiques pour censurer les opposants politiques et pour réprimer la population. Plusieurs organisations non gouvernementales alertent sur le blocage massif de sites portant atteinte aux droits humains des utilisateurs. Entre autres, Reporters sans frontières a révélé le blocage par le gouvernement du Népal de plusieurs sites d'informations[1143]. Mais également la Chine qui, grâce à ses fournisseurs d'Internet nationaux, peut bloquer et filtrer une très grande partie de sites et des contenus sur la politique interne et externe[1144]. Nous pouvons également citer d'autres États asiatiques, comme le Vietnam[1145] et le Myanmar[1146], ainsi que du continent africain, notamment lors de moments politiques importants, comme des élections ou lors de mouvements contestataires. Le Yémen, par exemple, a bloqué temporairement des sites politiques lors des élections de 2006, le Bahreïn a fait la même chose pour les élections

[1141] Q. VAN ENIS, « Chapitre 4. - Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 139.
[1142] Cour EDH (2e sect.), 18 décembre 2012, *Ahmet Yildirim c. Turquie*, req n° 3111/10, § 66.
[1143] Reporters sans frontières, *Énième blocage d'un site Internet d'informations*, Actualité, 20 janvier 2016. Disponible sur : https://rsf.org/fr/eni%C3%A8me-blocage-dun-site-internet-dinformations
[1144] Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », A/HRC/17/27, 16 mai 2011, § 29 qui cite Center for Democracy and Technology, « Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age," version 0.5 - Discussion draft », avril 2011, p. 48 qui renvoie vers un rapport très complet sur Internet et le blocage en Chine, disponible sur : http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf
[1145] Voir §425 de cette thèse et, en particulier, le rapport de Amnesty International, *Let us breathe! Censorship and criminalization of online expression in Viet Nam*, 2020.
[1146] Voir OpenNet Initiative, *Asia overview*, rapport en ligne, 2009, voir entre autres p. 226 et 230. Disponible sur : http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-asia.pdf

parlementaires[1147] ou encore l'Ouganda[1148]. Certains États ne se limitent pas au blocage de quelques sites ou pages mais privent les utilisateurs de l'accès total à Internet. En effet, d'autres manières de bloquer l'accès aux réseaux sociaux et plus généralement à Internet existent, par exemple : les mesures de bridage d'Internet ou les coupures. Des telles mesures ont été adoptées par les autorités turques qui ont limité la bande passante d'Internet, ce qui rend les médias sociaux et les autres sources de communication en ligne inaccessibles[1149]. La coalition #KeepItOn a signalé que, entre 2016 et 2021, 931 coupures d'accès à Internet ont été adoptées dans 74 États[1150]. Ces coupures portent atteinte aux droits humains des utilisateurs et les empêchent de participer activement à la vie politique de l'État, d'organiser des manifestations, de s'informer ou tout simplement d'échanger. Ces mesures sont souvent justifiées par les autorités pour défendre la sécurité nationale mais également comme un rempart contre les discours de haine et la désinformation. Toutefois, comme le souligne le rapport du Haut-Commissariat des Nations unies aux droits de l'Homme qui reprend l'observation générale n° 37 du Comité des droits de l'Homme « on ne saurait invoquer la sécurité nationale pour justifier une action lorsque ce sont précisément des atteintes aux droits de l'Homme qui sont à l'origine de la détérioration de la sécurité nationale »[1151].

540. Nous pouvons ensuite analyser le blocage des comptes personnels, comme celui de l'ancien président Donald J. Trump dont nous avions parlé précédemment[1152]. Le Conseil de surveillance de Meta avait établi que les messages publiés par M. Trump avaient créé

[1147] Voir : OpenNet Initiative, *Internet Filtering in the Middle East and North Africa*, rapport en ligne, 2009, p. 6. Disponible sur : https://opennet.net/sites/opennet.net/files/ONI_MENA_2009.pdf

[1148] Voir : Amnesty International, *Ouganda. Les autorités doivent lever le blocage des réseaux sociaux sur fond de répression à la veille des élections*, 13 janvier 2021. Disponible sur : https://www.amnesty.org/fr/latest/press-release/2021/01/uganda-authorities-must-lift-social-media-block-amid-crackdown-ahead-of-election/

[1149] Voir : N. MUIZNIZKS, « Le blocage arbitraire d'Internet porte atteinte à la liberté d'expression », *Le carnet des droits de l'Homme*, Commissaire aux droits de l'Homme, Conseil de l'Europe, 26 septembre 2017. Disponible sur : https://www.coe.int/fr/web/commissioner/-/arbitrary-internet-blocking-jeopardises-freedom-of-expression#:~:text=Le%20blocage%20de%20contenus%20sur,des%20droits%20de%20l'homme

[1150] Conseil des droits de l'Homme, Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, A/HRC/50/55, cinquantième session, 13 mai 2022, point 19.

[1151] *Ibid.* point 42.

[1152] Voir §514 de cette thèse.

un « environnement dans lequel un risque sérieux de violence était possible »[1153], pour cela il avait statué que la suspension temporaire de l'ancien président ordonné par Meta était justifiée. Toutefois, il souligne que Meta n'était pas autorisé à suspendre le compte *sine die.* En effet, cela était contraire aux règles de l'entreprise qui prévoient : la suppression du contenu de l'infraction, une période de suspension sur un délai précis ou bien la désactivation permanente. Le Conseil a estimé que la décision prise par le réseau social de suspendre le compte le 6 et le 7 janvier sans spécifier la durée du blocage était « vague et arbitraire »[1154]. Pour le faire, il a analysé la responsabilité de Meta vis-à-vis des dispositions protégeant les droits humains. Ces dernières étaient inscrites dans des instruments internationaux qui n'étaient pas contraignants pour le réseau social mais que Meta s'était engagé à respecter[1155]. Le Conseil s'est penché, en particulier, sur les articles 19 et 20 du Pacte relatif aux droits civils et politiques. Après la décision du Conseil de surveillance, Meta a ordonné de suspendre le compte de D. Trump pendant deux ans. Alors que Twitter avait opté pour le blocage définitif du compte[1156] avant de faire un rétropédalage avec l'arrivée du nouveau propriétaire Elon Musk.

541. Ces décisions posent la question de savoir si ce type de blocage est proportionné vis-à-vis des atteintes qu'il peut provoquer au regard de Trump lui-même mais aussi de ses followers. En effet, bannir M. Trump des réseaux sociaux porterait atteinte à son droit à la liberté d'expression et aux droits d'accès à l'information aux personnes qui le suivent (qu'ils soient d'accord avec ses idées, ou pas). Pour le Conseil de surveillance de Meta, le blocage temporaire était proportionné alors que celui *sine die* aurait été une sanction arbitraire et non proportionnée. C'est aussi la position exprimée par certains auteurs, comme E. Celeste qui considère que Trump devrait avoir une seconde chance de retrouver l'accès à ses réseaux sociaux si son comportement ne viole pas à nouveau les règles de la plateforme ou les lois nationales[1157].

[1153] Conseil de surveillance, décision sur le cas 2021-001-FB-FBR, FB-691QAMHJ, 5 mai 2021. Disponible sur : https://oversightboard.com/decision/FB-691QAMHJ/
[1154] *Ibid.*
[1155] Voir la Corporate Human Rights Policy de Meta, disponible sur : https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf
[1156] Twitter, Permanent suspension of @realDonaldTrump, 8 janvier 2021. Disponible sur : https://blog.twitter.com/en_us/topics/company/2020/suspension
[1157] Voir : E. CELESTE, « Trump's social media ban: Reviewing the constitutionality of permanent digital punishment », *Digital Society Blog*, Alexander Von Humboldt, Institut für Internet und Gesellschaft, 17 mars

II. La nécessaire proportionnalité des mesures de blocage et filtrage

542. Comme l'a observé la Cour européenne des droits de l'Homme, les mesures de blocage ne sont pas *a priori* contraires à la Convention européenne des droits de l'Homme, cependant « elles doivent s'inscrire dans un cadre légal particulièrement strict quant à la délimitation de l'interdiction et efficace quant au contrôle juridictionnel contre les éventuels abus »[1158].

543. La recommandation du Comité des ministres du Conseil de l'Europe a spécifié également que « les entités publiques de tous les niveaux […] qui introduisent des filtres ou les utilisent dans leurs prestations de services devraient veiller au plein respect de la liberté d'expression et d'information, du droit de chacun à la vie privée et au respect de la correspondance de chaque utilisateur »[1159]. De plus, en 2011, le rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression Frank la Rue avait énuméré les informations qui pouvaient faire l'objet de restrictions, c'est-à-dire : la pédopornographie, le discours de haine, la diffamation, l'incitation à commettre un génocide ou encore l'apologie de la haine ethnique[1160]. C'est d'ailleurs ce qui est prévu dans la législation nationale de la majeure partie des États européens. En effet, les États prévoient des mesures de blocage contre l'exploitation sexuelle des enfants[1161] mais également contre les contenus terroristes, d'incitation à la haine ou la diffamation.

544. Face aux droits fondamentaux qu'une telle mesure pourrait limiter et léser, il est nécessaire de se prévaloir des textes internationaux qui protègent les individus des

---

2021. Disponible sur : https://www.hiig.de/en/trumps-social-media-ban-reviewing-the-constitutionality-of-capital-digital-punishment/

[1158] Cour EDH (2e sect.), 18 décembre 2012, *Ahmet Yildirim c. Turquie*, req n° 3111/10, § 64.

[1159] Recommandation CM/Rec (2008)6 du Comité des Ministres aux États membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, adoptée par le Comité des Ministres le 26 mars 2008 lors de la 1022e réunion des Délégués des Ministres, point III.

[1160] Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/17/27, 16 mai 2011, § 25.

[1161] Voir par exemple en Allemagne, Royaume-Uni, Suisse ou France.

atteintes à leurs droits et libertés, comme la liberté d'expression ou encore d'accès à l'information. Pour cela, face aux garanties assurées par la Convention européenne des droits de l'Homme, la Convention du Conseil de l'Europe contre la cybercriminalité, mais aussi le Pacte international relatif aux droits civils et politiques et la Charte des droits fondamentaux de l'Union européenne[1162], il faut veiller à ce que les mesures de blocage et de filtrage soient proportionnelles. À cet égard, nous analyserons la jurisprudence européenne sur le blocage sur Internet et plus particulièrement la nécessité d'adopter des mesures proportionnelles pour ne pas porter atteinte aux droits fondamentaux des utilisateurs ou des propriétaires des sites ou des contenus. Pour qu'une mesure restreignant les droits et libertés fondamentales soit proportionnée, les cours européennes ont établi, sous influence allemande[1163], qu'elle doit être appropriée, nécessaire et proportionnée *stricto sensu*[1164]. En d'autres termes, la mesure doit, premièrement, être adaptée pour atteindre le but légitime poursuivi, deuxièmement, ne pas aller au-delà de ce qui est exigé pour réaliser l'objectif et enfin, respecter le rapport entre le préjudice et le bénéfice engendrée par la mesure[1165].

545. La Cour européenne des droits de l'Homme s'est clairement exprimée à plusieurs reprises sur l'illégalité des mesures de blocage prises par des autorités publiques pour affirmer qu'« il y a incompatibilité avec l'état de droit si le cadre juridique n'établit pas de garanties susceptibles de protéger les individus contre les effets excessifs et arbitraires des mesures de blocage »[1166]. La Cour continue en disant que « lorsque des circonstances exceptionnelles justifient le blocage d'un contenu illégal, l'organisme public qui ordonne

---

[1162] Voir : P. WACHSMANN, Commentaire de l'article 11 liberté d'expression et d'information in F. PICOD, C. RIZCALLAH, S. VAN DROOGHENBROECK, Charte des droits fondamentaux de l'Union européenne, Commentaire article par article, 3eme édition, 2023, pp. 291-312.
[1163] La proportionnalité a été citée pour la première fois dans le Code de la Prusse de 1794 et a été repris par la jurisprudence dans l'arrêt de la Cour administrative suprême de Prusse, 14 juin 1882, *Kreuzberg.*
[1164] S. VAN DROOGHENBROECK, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme – Prendre l'idée simple au sérieux*, Bruxelles, Bruylant, 2001, pp. 31 à 38.
[1165] Voir par exemple Q. VAN ENIS, « Chapitre 4. - Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 154. Ainsi que, N. DE BACKER, « Le principe de proportionnalité à l'épreuve de la liberté d'expression numérique », *JEDH*, 2019/4, p. 244. Ainsi que, F. SUDRE, L. MILANO, B. PASTRE-BELDA, A. SCHAHMANECHE, *Droit européen et international des droits de l'homme*, 16eme édition, PUF, 2023.
[1166] Cour EDH, 23 juin 2020, *Vladimir Kaharitonov c. Russie*, n° 10795/14, §46. Traduction libre de l'autrice de la version officielle en anglais.

le blocage doit s'assurer que la mesure vise strictement le contenu illégal et n'a pas d'effets arbitraires ou excessifs, indépendamment de la manière dont elle est mise en œuvre. *Toute mesure de blocage indiscriminée qui interfère avec des contenus ou des sites web licites en tant qu'effet collatéral d'une mesure visant des contenus ou des sites web illicites constitue une ingérence arbitraire dans les droits des propriétaires de ces sites web.* »[1167].

546. Ainsi, la mesure de blocage et de filtrage ne doit pas être trop générale. En effet, les mesures d'ordre général ont tendance à porter atteinte aux droits fondamentaux des individus. À cet égard, il est intéressant de mentionner l'observation générale n° 34 du Comité des droits de l'Homme sur l'article 19 du Pacte international relatif aux droits civils et politiques protégeant la liberté d'opinion et la liberté d'expression. Cette dernière souligne que « les restrictions licites [imposées au fonctionnement des sites Web, des blogs et de tout autre système de diffusion de l'information par le biais de l'Internet, de moyens électroniques ou autres, y compris les systèmes d'appui connexes à ces moyens de communication] *devraient d'une manière générale viser un contenu spécifique ; les interdictions générales de fonctionnement frappant certains sites et systèmes ne sont pas compatibles avec le paragraphe 3* [de l'article 19 du Pacte] »[1168]. En effet, le caractère général de la mesure, même si légitime, peut affecter considérablement les droits des internautes[1169], notamment leur droit de recevoir des informations. La Cour de justice de l'Union européenne dans l'affaire *Scarlet c. Sabam* avait été appelée à répondre à une question préjudicielle sur la mise en place par un fournisseur d'accès à Internet d'un filtrage des contenus. Dans son examen, la Cour a souligné le danger de mettre un place un système trop général qui « risquerait de ne pas suffisamment distinguer entre un contenu illicite et un contenu licite, de sorte que son

[1167] *Ibid.* §46. Italique de l'autrice.
[1168] Comité des droits de l'Homme, observation générale n° 34 sur l'art. 19 du Pacte international relatif aux droits civils et politiques protégeant la liberté d'opinion et liberté d'expression, CCPR/C/GC/34, 12 septembre 2011, § 43. Texte en italique par l'autrice. Voir également Q. VAN ENIS, « Chapitre 4. - Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 156.
[1169] Cour EDH (2e sect.), 18 décembre 2012, *Ahmet Yildirim c. Turquie*, req n° 3111/10, § 66.

déploiement pourrait avoir pour effet d'entraîner le blocage de communications à contenu licite »[1170].

547. Il vaut mieux que le blocage soit adopté pour un contenu spécifique et identifié. Comme le souligne la Cour de justice de l'Union européenne dans un arrêt sur le droit d'auteur. Dans son arrêt, elle ouvre la possibilité aux fournisseurs d'accès d'établir la mesure de blocage la plus adéquate et affirme que « les mesures […] adoptées par le fournisseur d'accès à Internet doivent être *strictement ciblées* »[1171].

548. Le rapporteur Frank la Rue est plus radical et estime que « même dans les cas où des justifications sont fournies, les mesures de blocage constituent un moyen inutile ou disproportionné d'atteindre le but visé puisqu'elles ne sont pas suffisamment ciblées et rendent un large éventail de contenus inaccessibles et ce, au-delà de ce qui a été jugé illégal »[1172]. En effet, sans rentrer dans les détails techniques des systèmes de filtrage et de blocage[1173], ils n'existent pas des systèmes qui puissent garantir le respect absolu des droits fondamentaux. Ainsi, le respect de la légalité et de la proportionnalité des décisions est vital pour que l'ingérence ne porte pas atteinte aux droits et libertés des utilisateurs et des propriétaires des sites ou pages bloquées ou filtrées. Pour cela, il est intéressant de mettre en avant les critères minimaux pour qu'une législation sur le blocage soit compatible avec la Convention européenne des droits de l'Homme, exposés très clairement par le juge Pinto de Albuquerque dans son opinion concordante à l'arrêt *Ahmet Yildirim c. Turquie*[1174]. Ce dernier énumère onze critères, parmi lesquels, le fait de donner une définition des catégories des personnes et institutions qui pourraient faire l'objet d'un blocage ainsi que des catégories d'ordonnances de blocage. De plus, la

---

[1170] CJUE (3eme chambre), *Scarlet c. Sabam*, 24 novembre 2011, C-70/ 10, § 52. Voir également CJUE (3eme chambre), *Samab c. Netlog*, 16 février 2012, C-360/10, § 50.
[1171] CJUE (4eme chambre), *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH et Wega Filmproduktionsgesellschaft mbH*, 27 mars 2014, C-314/12, § 56.
[1172] Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », A/HRC/17/27, 16 mai 2011, § 31.
[1173] Pour approfondir voir : C. CALLANAN, M. GERCKE, E. DE MARCO et H. DRIES-ZIEK ENHEINER, *Filtrage d'Internet – Équilibrer les réponses à la cybercriminalité dans une société démocratique*, Rapport en ligne, 2010, en particulier la p. 22. Disponible sur : http://juriscom.net/documents/lib20100520.pdf
[1174] Cour EDH (2e sect.), 18 décembre 2012, *Ahmet Yildirim c. Turquie*, req n° 3111/10, § 66.

nécessité de donner des détails sur la portée territoriale et la durée du blocage et les critères qui peuvent justifier le blocage, au sens de l'article 10, paragraphe 2, de la Convention. Mais également, il souligne le besoin d'une procédure de recours de nature judiciaire contre le blocage. En effet, il est nécessaire que les mesures de blocage soient accompagnées par des mesures qui garantissent effectivement à l'éditeur ou au propriétaire d'un site de signaler tout abus et mauvais usage du blocage. Nous pouvons également ajouter plus généralement que les entreprises ainsi que les États adoptant des mesures de blocage devraient se conformer aux droits fondamentaux protégés par les instruments européens et internationaux. Et, se tourner, entre autres, vers les principes directeurs des Nations Unies relatifs aux entreprises et aux droits humains.

549. Enfin, dans le choix des sanctions le risque de porter atteinte aux droits fondamentaux s'accompagne de la mise en balance à faire entre les droits et libertés fondamentaux concurrents.

Section II : La difficile mise en balance des droits et libertés fondamentaux

550. La question du filtrage et du blocage et la nécessité de trouver une sanction proportionnée, nous amènent à traiter la question de la mise en balance des droits fondamentaux.

551. En effet, l'espace offert en ligne fait jouir les utilisateurs de plusieurs droits fondamentaux qui, toutefois, se trouvent en concurrence. Nous analyserons la mise en balance de certains de ces droits du point de vue de la liberté d'expression, liberté qui se trouve au cœur de l'espace « cyber ». En effet, les technologies de l'information et de la communication « offrent à tous des possibilités sans précédent de jouir de la liberté d'expression », cependant « elles remettent aussi gravement en question cette liberté, par exemple en cas de censure par l'État ou le secteur privé »[1175].

552. À cet égard, il s'agira d'étudier la tension qui existe entre cette liberté et les autres droits fondamentaux (**§I**) et d'approfondir ces spécificités sur Internet pour assurer que son étendue et ses limites soient proportionnelles (**§II**).

I. La forte tension entre la liberté d'expression et les autres droits fondamentaux

553. D'un côté, nous étudierons l'étendue de la liberté d'expression (**A**) pour ensuite analyser son corollaire : le droit de recevoir des informations (**B**).

A. L'étendue du droit à la liberté d'expression sur Internet

554. Internet, comme le rappelle la Cour européenne des droits de l'Homme, est devenu « l'un des principaux moyens d'exercice par les individus de leur droit à la liberté

[1175] Déclaration du Comité des ministres sur le droit de l'Homme et l'état de droit dans la société de l'information, CM (2005)56 final, 13 mai 2005 cité par F. DUBUISSON et I. RORIVE, « La liberté d'expression à l'épreuve d'Internet », in *Entre ombres et lumières : cinquante ans d'application de la Convention européenne des droits de l'homme en Belgique*, Centre de droit public de l'Université libre de Bruxelles, Bruxelles, Bruylant, 2008, p. 362.

d'expression et d'information » [1176], mais également le lieu où on « trouve des outils essentiels de participation aux activités et débats relatifs à des questions politiques ou d'intérêt public »[1177]. Au vu de la multiplicité des droits fondamentaux concurrents dans la sphère numérique, les juridictions sont amenées à les mettre en balance les unes avec les autres. Le droit par excellence de la sphère numérique est celui à la liberté d'expression, compte tenu de l'espace grandissant offert aux utilisateurs pour publier des écrits, des photos, des vidéos ou encore des fichiers audios. Ce droit est protégé par plusieurs textes internationaux[1178] et, comme le souligne le Comité des ministres du Conseil de l'Europe, « la liberté d'expression […] doit être respectée dans un environnement numérique tout comme dans un environnement non numérique »[1179]. La Cour européenne des droits de l'Homme s'est exprimée à plusieurs reprises sur l'étendue de ce droit en statuant qu'il s'applique non seulement aux « « 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 fraction quelconque de la population » [1180]. Cette liberté constitue l'un des fondements essentiels de la société démocratique et « l'une des conditions primordiales de son progrès et de l'épanouissement de chacun »[1181].

[1176] Cour EDH (2e sect.), 18 décembre 2012, *Ahmet Yildirim c. Turquie*, req n° 3111/10, § 54.
[1177] *Ibid.* § 54.
[1178] Entre autres, l'article 10 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, Rome, 4 novembre 1950 ; l'article 11 de la Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, 18 décembre 2000 ; l'article 19 du Pacte international relatif aux droits civils et politiques, 16 décembre 1966, New York, Nations unies qui reprend l'article 19 de la Déclaration universelle des droits de l'Homme, adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948 à Paris.
[1179] Déclaration sur les droits de l'Homme et l'état de droit dans la société de l'information, adoptée par le Comité des ministres le 13 mai 2005 lors de la 926e réunion des délégués des ministres, cité par Q. VAN ENIS, « Chapitre 4. - Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in de C. TERWANGNE et Q. VAN ENIS (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 148.
[1180] Cour EDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, req. n° 5493/72, §49. Voir également Comité des droits de l'homme, Observation générale n° 34, 12 septembre 2011, CCPR/C.GC.34, par. 11.
[1181] Cour EDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, req. n° 5493/72, §49. Voir également C. RUET, « Chapitre 5. - Liberté d'expression et lutte contre le discours de haine sur Internet » in C. DE TERWANGNE, et Q. VAN ENIS (dir.*), L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019, p. 173. Voir également, F. SUDRE, L. MILANO, B. PASTRE-BELDA, A. SCHAHMANECHE, *Droit européen et international des droits de l'homme*, 16eme édition, PUF, 2023.

555. Cependant, tout n'est pas permis sur Internet et la liberté d'expression a des limites. Nous les étudierons en analysant la jurisprudence de la Cour européenne des droits de l'Homme qui est très riche et claire en la matière, malgré la difficulté de trouver la bonne balance entre les droits et libertés fondamentaux des utilisateurs. Cette étude permet également d'analyser indirectement les décisions des juridictions nationales au sujet de la liberté d'expression sur Internet. La Cour, lorsqu'elle est saisie, apprécie la légalité et la proportionnalité des restrictions émises par les autorités nationales. Elle s'assure notamment de la proportionnalité des mesures qui limitent la liberté d'expression. Dans sa jurisprudence, elle affirme que l'exercice de la liberté d'expression peut être restreint par des « formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique »[1182].

556. D'abord, la liberté d'expression trouve ses limites dans le discours de haine. Comme précisé par le Plan de Rabat[1183] « toute manifestation d'expression identifiée comme étant un « discors de haine » peut être limitée conformément aux articles 18 et 19 du Pacte [international relatif aux droits civils et politiques] »[1184]. Dans l'arrêt *Sanchez c. France,* la Cour européenne des droits de l'Homme rappelle « qu'en principe on peut juger nécessaire, dans les sociétés démocratiques, de sanctionner, voire de prévenir, toutes les formes d'expression qui propagent, encouragent, promeuvent ou justifient la haine fondée sur l'intolérance »[1185]. En effet, le discours de haine ne bénéficie pas de la protection de l'article 10 de la Convention[1186]. Entre autres, les discours niant l'existence de faits historiques clairement établis, comme l'Holocauste, ne sont pas protégés par la Convention. C'est ce qui ressort de la jurisprudence de la Cour européenne des droits de l'Homme et notamment de l'affaire *Garaudy c. France* où elle

---

[1182] Article 10, paragraphe 2, Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, Rome, 4 novembre 1950.
[1183] Plan d'action de Rabat sur l'interdiction de tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence. Conclusions et recommandations issues des quatre ateliers d'experts organisés par le HCDH en 2011 et adoptés par les experts à Rabat, Maroc le 5 octobre 2012.
[1184] *Ibid.* point 14.
[1185] Cour EDH, 2 septembre 2021, *Sanchez c. France,* req. n° 45581/15, § 85, confirmé par Cour EDH, GC, 15 mai 2023, *Sanchez c. France,* req. n° 45581/15. Voir également Cour EDH, 6 octobre 2006, *Erbakan c. Turquie*, req. n° 59405/00, §56.
[1186] Cour EDH, 4 décembre 2003, *Gündüz c. Turquie*, req. n° 35071/97, § 41, voir également Cour EDH, GC, 23 septembre 1994, *Jersild c. Danemark*, req. n° 15890/89, § 35.

rappelle que « ne fait aucun doute qu'à l'égal de tout autre propos dirigé contre les valeurs qui sous-tendent la Convention, la justification d'une politique pronazie ne saurait bénéficier de la protection de l'article 10 » et qu'il existe « une catégorie [de] faits historiques clairement établis - tels que l'Holocauste - dont la négation ou la révision se verrait soustraite par l'article 17 [interdiction de l'abus de droit] à la protection de l'article 10 »[1187]. Elle estime également que « la contestation de crimes contre l'humanité apparaît comme l'une des formes les plus aiguës de diffamation raciale envers les Juifs et d'incitation à la haine à leur égard »[1188]. Dans une autre affaire dans laquelle les tribunaux suisses avaient sanctionné le président du parti de travailleurs de Turquie pour avoir nié à l'occasion de plusieurs conférences l'existence du génocide arménien[1189], elle ne revient pas sur ces précédentes décisions[1190] mais précise indirectement que le cas du génocide arménien se distingue de l'holocauste pour l'absence d'une « décision judiciaire internationale (le jugement de Nuremberg) ayant établi les faits concernés et leur ayant appliqué une certaine qualification juridique »[1191]. Cela amène la Cour à établir un nouveau critère vis-à-vis de ces faits historiques qui est celui d'une décision judiciaire internationale.

557. Concernant les faits historiques, nous pouvons également rappeler que l'observation générale n° 34 du Comité des droits de l'Homme affirme que « les lois qui criminalisent l'expression d'opinions concernant des faits historiques sont incompatibles avec les obligations que le Pacte [international relatif aux droits civils et politiques] impose aux États parties en ce qui concerne le respect de la liberté d'opinion et de la liberté d'expression. Le Pacte ne permet pas les interdictions générales de l'expression d'une opinion erronée ou d'une interprétation incorrecte d'événements du passé »[1192]. Le Comité prévoit également que « les interdictions de manifestations de manque de respect à l'égard d'une religion ou d'un autre système de croyance, y compris les lois sur le

[1187] Cour EDH, 24 juin 2003, *Garaudy c. France*, req n° 65831/01. Ainsi que Cour EDH, 23 septembre 1998, *Lehideux et Isorni c. France*, req. n° 24662/94, § 47 et §53.
[1188] Cour EDH, 24 juin 2003, *Garaudy c. France*, req n° 65831/01.
[1189] Cour EDH (2e sect.), 19 décembre 2013, *Perinçek c. Suisse*, req. n° 27510/08.
[1190] Cour EDH, 4 décembre 2003, *Gündüz c. Turquie*, req. n° 35071/97 ; Cour EDH, GC, 23 septembre 1994, *Jersild c. Danemark*, req. n° 15890/89.
[1191] F. DUBUISSON, « Société de l'information, médias et liberté d'expression », *Journal européen des droits de l'homme*, 2014/3, p. 370.
[1192] Comité des droits de l'Homme, Observation générale n° 34, 12 septembre 2011, CCPR/C.GC.34, § 49.

blasphème, sont incompatibles avec le Pacte [international relatif aux droits civils et politiques] » et il continue en disant que « il ne serait pas acceptable que ces lois établissent une discrimination en faveur ou à l'encontre d'une ou de certaines religions ou d'un ou de certains systèmes de croyance ou de leurs adeptes, ou des croyants par rapport aux non-croyants. Il ne serait pas non plus acceptable que ces interdictions servent à empêcher ou à réprimer la critique des dirigeants religieux ou le commentaire de la doctrine religieuse et des dogmes d'une foi »[1193].

En 2017, le Comité des droits de l'Homme s'est exprimé concernant une demande portant sur des propos considérés par les demandeurs comme injurieux, incitant à la discrimination, à la haine et à la violence à raison de leur race ou de leur religion. En l'espèce, des centaines de personnes et d'organisations avaient porté plainte auprès de la police néerlandaise contre M. Geert Wilders, député et fondateur du Parti pour la liberté, un parti politique d'extrême droite, pour des propos qu'il avait tenu à plusieurs reprises en public, en particulier dans des articles de presse et en ligne. Il s'était exprimé en tenant, entre autres, les propos suivants : « Un jeune Marocain sur cinq a un casier judiciaire. Leur comportement découle de leur religion et de leur culture », « Ces Marocains sont vraiment violents » ou encore : « On en a assez. On ferme les frontières, on ne laisse plus entrer d'islamiques aux Pays-Bas ». Appelé à répondre au délit d'injure et d'incitation à la haine et à la discrimination par la Cour d'appel d'Amsterdam, le défendeur a été relâché et les demandes des organisations et des demandeurs jugées irrecevables. Le Comité par les constations adoptées le 29 mars 2017 a estimé que l'État partie avait pris « les mesures nécessaires et proportionnées visant à « interdire » les déclarations formulées en violation du paragraphe 2 de l'article 20 et à garantir le droit des auteurs à un recours utile en vue de les protéger contre les conséquences de telles déclarations »[1194].

Ce que nous trouvons intéressant à mettre en avant dans cette affaire, ce sont les opinions de Sarah Cleveland et Mauro Politi ainsi que celle du Prof. Olivier de Frouville. Dans leur opinion concordante Sarah Cleveland et Mauro Politi estiment que l'« article 20(2)

[1193] *Ibid.* § 48.
[1194] Comité des droits de l'Homme, Constatations adoptées par le Comité au titre de l'article 5 (par. 4) du Protocole facultatif, concernant la communication n° 2124/2011, CCPR/C/117/D/2124/2011, 29 mars 2017.

does not require legal prohibition of all « advocacy of national, racial or religious hatred," but only of such advocacy that also "constitutes incitement to discrimination, hostility or violence »[1195]. C'est-à-dire que l'appel à la haine nationale, raciale ou religieuse ne suffit pas. Il doit également avoir l'intention d'inciter à la discrimination, à l'hostilité ou à la violence ne suffit pas pour porter atteinte à la liberté d'expression. Nous partageons leur affirmation précisant qu'avoir des standards restrictifs pour l'imposition de sanctions pénales à ce sujet est approprié, car comme souligné par les Nations unies et d'autres organisations internationales « [i]n many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues. Hate speech and similar laws ironically are often employed to suppress the very minorities they purportedly are designed to protect »[1196]. Cependant, nous soutenons l'argumentaire soutenu par Olivier de Frouville qui ne rejoint pas les conclusions du Comité et celles de Mme Cleveland et M. Politi. En effet, selon le Prof. De Frouville, le Comité a exercé seulement un contrôle formel qui ne permet pas de déterminer si le jugement a violé le paragraphe 2 de l'article 20. Selon lui, l'analyse des propos du défendeur à la lecture de la jurisprudence du Comité des droits de l'Homme, du Comité pour l'élimination de la discrimination raciale mais aussi de la Cour européenne des droits humains aurait dû conduite le Comité à statuer que non seulement les propos relevaient de l'article 20, paragraphe 2 mais également que le Tribunal néerlandais avait fait une évaluation erronée[1197]. En effet, comme Olivier de Frouville, nous estimons que les propos tenus par M. Geert Wilders n'étaient pas dirigés contre l'Islam en tant que religion mais contre les musulmans ainsi que toute personne considérée comme non occidentale. Selon de Frouville, le Comité

[1195] Voir Comité des droits de l'Homme, Constatations adoptées par le Comité au titre de l'article 5 (par. 4) du Protocole facultatif, concernant la communication no 2124/2011, CCPR/C/117/D/2124/2011, 29 mars 2017, annexe IV, point 4. Traduction de l'autrice : « L'article 20, paragraphe 2, n'exige pas l'interdiction légale de tout « appel à la haine nationale, raciale ou religieuse », mais seulement de tout appel qui constitue également « une incitation à la discrimination, à l'hostilité ou à la violence » ».

[1196] Voir Comité des droits de l'Homme, Constatations adoptées par le Comité au titre de l'article 5 (par. 4) du Protocole facultatif, concernant la communication no 2124/2011, CCPR/C/117/D/2124/2011, 29 mars 2017, annexe IV, point 8. Traduction de l'autrice : « Dans de nombreux pays, les puissants abusent de règles trop larges dans ce domaine pour limiter les voix non traditionnelles, dissidentes, critiques ou minoritaires, ou les discussions sur des questions sociales difficiles. Ironiquement, les lois sur les discours haineux et autres lois similaires sont souvent utilisées pour supprimer les minorités mêmes qu'elles sont censées protéger ».

[1197] Voir : Comité des droits de l'Homme, Constatations adoptées par le Comité au titre de l'article 5 (par. 4) du Protocole facultatif, concernant la communication no 2124/2011, CCPR/C/117/D/2124/2011, 29 mars 2017, annexe VII, point 12.

aurait dû s'interroger sur la justification de l'acquittement et son caractère appropriée et proportionné. À cet égard, il conclut que le Comité aurait dû conclure que l'acquittement ne pouvait pas être considéré approprié vis-à-vis de la protection du droit de toute personne d'être protégé contre les appels à la haine et l'incitation à la discrimination. Hélas, ce cas d'espèce de 2017, 5 ans plus tard est d'actualité lorsque l'on pense à des propos tenus par des représentants de l'extrême droite pendant la campagne présidentielle française de 2021 ou dans d'autres États comme l'Autriche et l'Italie[1198].

558. La liberté d'expression peut être limitée par le droit à la vie privée. À cet égard, la Cour européenne des droits de l'Homme a, depuis plusieurs années, défini des critères pour statuer sur la mise en balance entre le droit à la vie privée et la liberté d'expression. Elle énumère six critères : la contribution à un débat d'intérêt général, la notoriété de la personne visée et l'objet du reportage, le comportement antérieur de la personne concernée ; ainsi que le mode d'obtention des informations et leur véracité, le contenu, la forme et les répercussions de la publication et la gravité de la sanction imposée[1199]. Cependant, des restrictions à la liberté d'expression ne doivent pas, en principe, être adoptées concernant le débat politique « dans lequel la liberté d'expression revêt la plus haute importance »[1200] et les questions d'intérêt général[1201]. Cela est valable sauf si certaines limites sont atteintes, comme les discours de haine, le respect de la réputation ou des droits d'autrui. Il faut rappeler que, comme l'a spécifié la Cour européenne des droits de l'Homme dans sa jurisprudence, « lorsqu'elle est appelée à se prononcer sur un conflit entre deux droits également protégés par la Convention, la Cour doit effectuer une mise en balance des intérêts en jeu. L'issue de la requête ne saurait en principe varier selon qu'elle a été portée devant elle, sous l'angle de l'article 8 de la Convention, par la personne faisant l'objet de la publication ou, sous l'angle de l'article 10, par son auteur.

[1198] Nous pensons notamment à des propos d'Eric Zemmour candidat à l'élection présidentielle française de 2021, Andreas Mölzer, député européen autrichien ou Francesco Lollobrigida, ministre de l'agriculture italien, qu'en 2023 parle de remplacement ethnique des italiens par les migrants.
[1199] Cour EDH, GC, 7 février 2012, *Axel Springer AG c. Allemagne*, req. n° 39954/08, §§ 89-95. Voir également Cour EDH, GC, 10 novembre 2015, *Couderc et Hachette Filipacchi Associés c. France*, req. n° 40454/07, §93.
[1200] Cour EDH, 11 avril 2006, *Brasilier c. France*, req n° 71343/01, § 41.
[1201] Cour EDH, GC, 8 juillet 1999, *Sürek c. Turquie*, req n° 26682/95, §61.

En effet, ces droits méritent a priori *un égal respect.* […] Dès lors, *la marge d'appréciation devrait en principe être la même dans les deux cas* »[1202].

559. Cela nous amène à parler du droit de recevoir des informations qui est le corollaire de la liberté d'expression et qui se trouve souvent mis à mal par la mise en balance avec d'autres droits fondamentaux.

B. Le droit de recevoir des informations, un droit relatif corollaire de la liberté d'expression

560. Le droit de recevoir des informations est le corollaire de la liberté d'expression et est protégé par les mêmes instruments juridiques. Le professeur Q. Van Enis le définit comme le « parent pauvre de la liberté d'expression »[1203] pour sa vulnérabilité lorsqu'il est mis en balance avec d'autres droits et libertés[1204]. En témoigne la jurisprudence de la Cour de justice de l'Union européenne. D'abord, nous pouvons citer l'affaire *Google Spain et Google Inc c/AEPD*[1205] dans laquelle la Cour a estimé que « le *droit* à la protection de la vie privée et le *droit* à la protection des données à caractère personnel « prévalent en principe » non seulement sur *l'intérêt* économique de l'exploitant du service de référencement, mais également sur *l'intérêt* du public à accéder […] à une information […] »[1206]. Ensuite, dans d'autres affaires la Cour justifie la restriction au droit de recevoir des informations par la présence d'autres moyens de communication qui permettent à l'individu de contourner certaines limitations. Cela a été le cas, par exemple, pour l'interdiction d'une campagne d'affichage d'une association dans le domaine public qui a été considéré conforme à la Convention européenne des droits de l'Homme parce que d'autres moyens de communication, entre autres Internet, étaient disponibles pour

---

[1202] Cour EDH, 30 août 2016, *Medipress-Sociedade Jornalistica Lda c. Portugal*, req n° 55442/12, § 38. Italique de l'autrice.
[1203] Q. VAN ENIS, « Le droit de recevoir des informations ou des idées par le biais de l'internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen *?* », *Journal européen des droits de l'homme*, 2015/2, 175.
[1204] *Ibid*. p. 175.
[1205] CJUE, GC, 13 mai 2014, *Google Spain et Google Inc c/AEPD*, aff. C 131/12.
[1206] Q. VAN ENIS, « Le droit de recevoir des informations ou des idées par le biais de l'internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen *?* », *Journal européen des droits de l'homme*, 2015/2, p. 175.

continuer à diffuser leurs idées[1207]. De plus, la Cour a estimé qu'une restriction vis-à-vis de la publication de publicités payantes dans des médias traditionnels, comme la radio et la télévision, était justifiée parce que d'autres moyens de communication étaient accessibles[1208]. La Cour rappelle que « [the] access to alternative media is key to the proportionality of a restriction on access to other potentially useful media »[1209]. Nous soutenons la position de certains auteurs selon lesquels cet argument de la disponibilité de moyens alternatifs de communication est dangereux « dans la mesure où il présuppose que ces moyens sont et resteront accessibles et qu'ils présentent une efficacité comparable »[1210]. Ainsi, cela pourrait peut-être amener à légitimer le blocage de sites et de pages web lorsque les contenus de ces derniers seraient disponibles ailleurs[1211].

561. D'autres arrêts montrent une application extensive du droit de recevoir des informations. Cela est le cas dans l'arrêt *Cengiz et autres c. Turquie.* Face au blocage du site YouTube à trois universitaires, la Cour européenne des droits de l'Homme a statué la violation de l'article 10 car ces derniers avaient été privés de leur droit de recevoir des informations[1212]. De plus, la Cour européenne des droits de l'Homme s'est exprimée à plusieurs reprises sur le droit d'accès à l'information pour les détenus. Si elle considère que l'article 10 ne peut pas être interprété comme imposant une obligation générale de fournir aux détenus un accès à Internet ou à des sites spécifiques[1213], elle conclut, à plusieurs reprises, à la violation de l'article 10 par les autorités étatiques. En particulier, lors du refus aux détenus d'accéder à des sites contenant des informations juridiques[1214] et éducatives[1215].

[1207] Cour EDH, GC, *Mouvement raëlien suisse c. Suisse*, 13 juillet 2012, req. n° 16354/06, § 75.
[1208] Cour EDH, GC, *Animal Defenders International c. Royaume-Uni*, 22 avril 2012, req n° 48876/08.
[1209] *Ibid.* § 124. Traduction de l'autrice : « l'accès aux médias alternatifs est un élément clé de la proportionnalité d'une restriction de l'accès à d'autres médias potentiellement utiles ».
[1210] Voir E. MONTERO et Q. VAN ENIS, « Les gestionnaires de forums et portails d'actualités cueillis à froid par la Cour de Strasbourg ? », *RTDH*, 27e année, n° 108, 1er octobre 2016, p. 974.
[1211] Q. VAN ENIS, « Le droit de recevoir des informations ou des idées par le biais de l'internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen ? », *Journal européen des droits de l'homme*, 2015/2, 184.
[1212] Cour EDH, 1 décembre 2015, *Cengiz et autres c. Turquie*, req n° 48226/10 et 14027/11.
[1213] Cour EDH, 19 janvier 2016, *Kalda c. Estonie*, req. N° 17429/10, § 45 ainsi que Cour EDH, 17 janvier 2017, *Jankovskis c. Lituanie*, req n° 21575/08, § 55.
[1214] Cour EDH, 19 janvier 2016, *Kalda c. Estonie*, req. N° 17429/10 ; ainsi que, Cour EDH, 9 février 2021, *Ramazan Demir c. Turquie*, req n° 68550/17.
[1215] Cour EDH, 17 janvier 2017, *Jankovskis c. Lituanie*, req n° 21575/08.

562. Le droit de recevoir des informations a vu sa notion s'élargir à travers l'interprétation large de la Cour européenne des droits de l'Homme. Cette dernière englobe à ce droit celui d'accéder à l'information[1216]. La Cour a énuméré quatre critères pour savoir dans quelle mesure un refus d'accès à l'information constitue une atteinte au droit à la liberté d'expression. Selon elle, il s'agit d'évaluer l'objet de la demande d'information, la nature de l'information recherchée, le rôle de celui qui cherche l'information et si l'information demandée est prête et disponible[1217]. La Cour reconnaît également un droit pour les individus d'accéder à des informations détenues par l'État[1218]. Ces critères n'ont pas été formulés dans des affaires qui concernaient un accès à l'information en ligne, mais ils pourraient être transposés à Internet.

II. Les spécificités de la liberté d'expression sur Internet

563. La liberté d'expression et le droit de recevoir des informations sont des droits de plus en plus concurrencés sur Internet par d'autres droits fondamentaux. Cependant, un principe est clair, celui de limiter la liberté d'expression à condition que la mesure soit proportionnée au but légitime au sens de du paragraphe 2 de l'article 10 de la Convention des droits de l'Homme. Cependant, ce droit peut trouver une plus forte protection dans certaines situations (**A**) qui sont tout de même limitées (**B**).

A. Une protection accrue de la liberté d'expression au profit de l'intérêt général

564. Comme nous l'avons vu dans les développements précédents, la liberté d'expression est faiblement restreinte lorsqu'il s'agit de discours politiques ou des questions d'intérêt général. Par conséquent, cette liberté est hautement protégée sur Internet pour les individus qui contribuent aux questions d'intérêt général. Cela est notamment le cas pour

---

[1216] Cour EDH, 10 juillet 2006, *Sdružení Jihočeské Matky c. la République tchèque*, req. n° 19101/03, Cour EDH, 14 avril 2009, *Társaság a Szabadságjogokért c. Hongrie*, req. n° 37374/05, § 35 ainsi que Cour EDH, GC, 8 novembre 2016, *Magyar Helsinki Bizottsàg c. Hongrie*, req. n° 18030/11, § 149.
[1217] Cour EDH, 26 mars 2020, *Centre for democracy and the rule of law c. Ukraine*, req n° 100090/16, § 82.
[1218] Cour EDH, GC, 8 novembre 2016, *Magyar Helsinki Bizottsàg c. Hongrie*, req. n° 18030/11, § 156. Voir également F. DUBUISSON et J. PIERET, « Chronique. Société de l'information, médias et liberté d'expression », *JEDH*, 2017/3, p. 293.

les journalistes. En effet, la Cour européenne a reconnu explicitement leurs droits dans sa jurisprudence.

565. Premièrement, à travers son arrêt *Comité de rédaction Pravoye Delo et Shtekel c. Ukraine*, elle affirme, pour la première fois, que le droit national doit prévoir une protection adéquate de la liberté d'expression sur Internet des journalistes sur le fondement de l'article 10 de la Convention[1219]. Cette protection a été étendue aux reportages politiques ou d'investigations des journalistes auxquels la Cour attribue un haut niveau de protection[1220]. Ensuite, l'article 10 de la Convention protège les journalistes[1221], et, en général, tout individu qui s'engage dans un débat public d'intérêt général « de recourir à une certaine dose d'exagération, voire de provocation, c'est-à-dire d'être quelque peu immodéré dans ses propos »[1222] sans dépasser certaines limites quant au respect des droits d'autrui.

566. Ensuite, la Cour s'est exprimée à plusieurs reprises sur la proportionnalité des sanctions adoptées au niveau national contre les journalistes. Selon elle, certaines sanctions peuvent dissuader ces derniers à contribuer au débat d'intérêt général. La Cour affirme que les autorités nationales doivent s'abstenir de prendre des sanctions qui risquent de « dissuader les journalistes de contribuer à la discussion publique de questions qui intéressent la vie de la collectivité »[1223]. D'abord, elle estime que les condamnations à une peine d'emprisonnement pour avoir commis une infraction de presse ne sont pas compatibles avec la liberté d'expression des journalistes, sauf s'il y a une atteinte grave aux droits fondamentaux. En effet, la menace d'une peine de prison, selon la Cour, a des effets dissuasifs significatifs[1224]. À cet égard, le Conseil de l'Europe demande aux États d'abolir toute législation, encore en vigueur, qui prévoit une peine

---

[1219] Cour EDH, 5 mai 2011, *Comité de rédaction Pravoye Delo et Shtekel c. Ukraine*, req. n°33014/05.
[1220] Cour EDH, 10 mai 2011, *Mosley c. Royaume-Uni*, req n° 48009/08, § 129.
[1221] Voir notamment Cour EDH, 23 juin 2015, *Niskasaari et Otavamedia Oy c. Finlande*, req. n°32297/10 où la Cour a reconnu que « la limite de la critique admissible est large si les commentaires émanent de professionnels des médias bien connus du public qui polémiquent entre eux sur un sujet d'intérêt général » voir Conseil de l'Europe / Cour européenne des droits de l'Homme, *Internet :la jurisprudence de la Cour européenne des droits de l'Homme*, 2011, mise à jour en juin 2015, p. 21.
[1222] Cour EDH, 16 juillet 2009, *Willem c. France*, no 10883/05, § 33 ; voir également Cour EDH, 7 novembre 2006, *Mamere c. France*, req. n° 12697/03, § 25.
[1223] Cour EDH, 8 juillet 1986, *Lingers c. Autriche*, req n° 9815/82, § 44.
[1224] Cour EDH, 24 septembre 2013, *Belpietro c. Italie*, req. n° 43612/10, §61. Italique de l'autrice.

d'emprisonnement pour des infractions de diffamation[1225]. Ensuite, la Cour se prononce également sur la détention provisoire d'un journaliste d'investigation. Elle affirme qu'en le privant de sa liberté « pendant si longtemps sans motifs pertinents ou suffisants, les autorités judiciaires ont exercé un *effet dissuasif sur la volonté du requérant de s'exprimer sur des sujets relevant de l'intérêt public* »[1226]. De plus, elle ajoute qu'une telle mesure « est susceptible de créer un *climat d'autocensure* pour lui et pour tous les journalistes d'investigation envisageant d'effectuer des recherches et de faire des commentaires sur le comportement et agissements des organes étatiques »[1227]. Enfin, la Cour va plus loin en se montrant contraire à d'autres sanctions plus faibles. En effet, elle considère également que des sanctions civiles, « bien que légères »[1228] peuvent également provoquer un effet dissuasif et porter atteinte à la liberté d'expression.

567. Deuxièmement, la Cour européenne des droits de l'Homme reconnaît un degré renforcé de protection de la liberté d'expression pour les propos qui relèvent de l'expression politique et militante[1229]. Elle précise que la liberté d'expression est précieuse pour chacun mais tout particulièrement pour les élus du peuple qui représentent leurs électeurs, partagent leurs préoccupations et défendent leurs intérêts[1230]. De plus, dans son arrêt *Renaud c. France,* la Cour avait été saisie par un membre d'une association alléguant la violation de son droit à la liberté d'expression du fait de sa condamnation pour diffamation et injure publiques sur Internet envers un citoyen chargé d'un mandat public. La Cour constate que les propos du requérant sont d'une certaine virulence et elle retient qu'ils s'inscrivent dans un débat d'intérêt général. En effet, elle affirme que « même s'ils ne s'inscrivent pas dans le cadre de la liberté d'expression d'un membre de l'opposition à proprement parler, ces propos relèvent de l'expression de l'organe représentant d'une association portant les revendications émises par ses membres sur un

[1225] Voir la résolution 1577 (2007) de l'Assemblée Parlementaire du Conseil de l'Europe, *Vers la dépénalisation de la diffamation*, adoptée par l'Assemblée le 4 octobre 2007, 34e séance. Voir également résolution 2035 (2015) de l'Assemblée Parlementaire du Conseil de l'Europe, *La protection de la sécurité des journalistes et de la liberté des médias en Europe*, adoptée par l'Assemblée le 29 janvier 2015 (8e séance).
[1226] Cour EDH, 8 juillet 2014, *Nedim Şener c. Turquie*, req. n° 38270/11, § 122.
[1227] *Ibid.* § 122. Italique de l'autrice.
[1228] Cour EDH, GC, 7 février 2012, *Axel Springer AG c. Allemagne,* req. n° 39954/08, § 109.
[1229] Cour EDH, 25 février 2010, *Renaud c. France*, req. n° 13290/07, § 33.
[1230] Cour EDH, 16 juillet 2009, *Willem c. France*, req. n° 10883/05, § 32.

sujet d'intérêt général dans le cadre de la mise en cause d'une politique municipale »[1231]. La Cour rappelle également que « l'intérêt plus général d'assurer le libre jeu du débat politique […] se trouve au cœur même de la notion de société démocratique qui domine la Convention tout entière »[1232]. Enfin, elle considère que la condamnation du requérant viole l'article 10 de la Convention. En effet, elle « ne représentait pas un moyen raisonnablement proportionné à la poursuite du but légitime visé, compte tenu de l'intérêt de la société démocratique à assurer et à maintenir la liberté d'expression »[1233].

La Cour de justice de l'Union européenne va également dans le même sens pour les fonctionnaires et agents de l'Union européenne. Elle précise que la liberté d'expression de ces derniers « comprend celle d'exprimer, verbalement ou par écrit, des opinions discordantes ou minoritaires par rapport à celles défendues par l'institution qui les emploie »[1234]. Elle confère également une « liberté maximale »[1235] aux parlementaires européennes qui serait limitée seulement face à une entrave au fonctionnement de l'institution parlementaire.

568. Troisièmement, elle s'exprime également sur la protection des professionnels du droit, en particulier lorsqu'il s'agit de participer au débat public. À cet égard, la Cour européenne des droits de l'Homme a pu conclure que la révocation d'une magistrate qui critique dans plusieurs médias nationaux une réforme de la justice porte atteinte à sa liberté d'expression[1236].

569. Enfin, la Cour a pu se pencher sur les propos qui relèvent de la critique ou de la satire. Dans son arrêt *Eon c. France,* la Cour affirme que la satire « peut jouer un rôle très important dans le libre débat des questions d'intérêt général sans lequel il n'est pas de société démocratique »[1237]. Pour cela, elle considère que la sanction pour un individu

---

[1231] Cour EDH, 25 février 2010, *Renaud c. France*, req. n° 13290/07, § 40.
[1232] *Ibid*. §41.
[1233] *Ibid*. §43.
[1234] CJUE, 6 mars 2001, *Connolly*, aff. C-274/99.
[1235] P. WACHSMANN, Commentaire de l'article 11 liberté d'expression et d'information in F. PICOD, C. RIZCALLAH, S. VAN DROOGHENBROECK, Charte des droits fondamentaux de l'Union européenne, Commentaire article par article, 3eme edition, 2023, p. 299.
[1236] Cour EDH, 5 mai 2020, arrêt *Kövesi c. Romania*, req n° 3594/19.
[1237] Cour EDH, 13 mars 2013, *Eon c. France,* req. n° 26118/10, § 61.

ayant tenu une pancarte satirique pendant la visite officielle du président de la République française était disproportionnée et portait atteinte à sa liberté d'expression. Ces deux derniers arrêts ne concernent pas Internet, cependant nous pouvons penser que ces principes sont transposables à des propos satiriques tenus sur Internet.

570. Toutefois, cette extension à la liberté d'expression trouve également des limites.

B. Les limites à l'extension de la liberté d'expression sur Internet

571. Nous avons vu précédemment que lorsqu'il s'agit de participer au débat d'intérêt général, la liberté d'expression est étendue, notamment pour certains individus.

572. Premièrement, face à l'élargissement de la liberté d'expression des journalistes, « chiens de garde de la démocratie »[1238], la Cour a également renforcé leurs « devoirs et responsabilités »[1239] pour éviter les abus. D'abord, comme nous l'avons relevé dans le paragraphe précèdent, la diffusion de discours de haine et d'appel à la violence n'est pas protégé par la liberté d'expression. Cela vaut également pour la publication de fausses informations[1240]. Ensuite, la Cour souligne l'importance de la déontologie. En effet, elle affirme que « dans un monde dans lequel l'individu est confronté à un immense flux d'informations, circulant sur des supports traditionnels ou électroniques et impliquant un nombre d'auteurs toujours croissant, le contrôle du respect de la *déontologie journalistique* revêt une importance accrue »[1241]. Enfin, elle affirme qu'en ligne, comme hors ligne, « la presse est tenue au respect de ses *devoirs et responsabilités* dans l'exercice de sa liberté d'expression »[1242] et elle ajoute que « la protection que l'article 10 offre aux journalistes est subordonnée à la condition qu'ils agissent de *bonne foi* de manière à fournir des informations exactes et dignes de crédit dans le respect des

[1238] Voir notamment Cour EDH, 27 mars 1996, *Goodwin c. Royaume-Uni*, req. n° 17488/90, §39.

[1239] Cour EDH, 22 octobre 2009, *Europapress Holding D.O.O c. Croatie*, req. n°25333/06, § 58.
[1240] Cour EDH, 3 juin 2014, *Schuman c. Pologne*, req n°52517/13.
[1241] Cour EDH, 10 décembre 2007, *Stoll c. Suisse*, req. n° 69698/01, § 104. Italique de l'autrice.
[1242] Cour EDH, 10 mars 2009, *Times Newspaper c. Royaume-Un*i, req. n° 3002/03 et n° 23676/03, § 42. Italique de l'autrice.

principes d'un journalisme responsable »[1243]. Les journalistes ont le devoir de fournir des informations exactes et fiables et, surtout, fondées sur une base factuelle. Cela vaut non seulement lorsqu'ils s'expriment dans le journal qu'il les emploie mais également en dehors de ce cadre, notamment dans un forum sur Internet[1244].

573. Deuxièmement, la Cour s'est également prononcée sur la proportionnalité des sanctions pour les autres catégories de personnes pour lesquelles elle a reconnu une liberté d'expression étendue, comme les exposants politiques ou les lanceurs d'alerte. En premier lieu, sur les femmes et les hommes politiques, elle précise que lorsque la liberté d'expression des élus du peuple est remise en question, elle se livre à un contrôle plus strict. Ainsi, elle souligne que les propos tenus dans un débat d'intérêt général ne doivent pas dépasser le respect des droits d'autrui. La Cour relève également que, comme les journalistes, les hommes et femmes politiques ont des devoirs et des responsabilités. De plus, ils se doivent « de conserver une certaine neutralité et dispose d'un devoir de réserve dans ses actes lorsque ceux-ci engagent la collectivité territoriale qu'il représente dans son ensemble »[1245]. Notamment, lorsque les propos s'inscrivent dans une « démarche discriminatoires »[1246]. La Cour a confirmé ces propos également dans l'affaire *Feret c. Belgique* où elle affirme que « les partis politiques ont le droit de défendre leurs opinions en public, même si certaines d'entre elles heurtent, choquent ou inquiètent une partie de la population. […] Toutefois, ils doivent éviter de le faire en préconisant la discrimination raciale et en recourant à des propos ou des attitudes vexatoires ou humiliantes, car un tel comportement risque de susciter parmi le public des réactions incompatibles avec un climat social serein et de saper la confiance dans les institutions démocratiques »[1247]. Pareillement, lorsqu'il s'agit d'attaques personnelles qui ne respectent pas « les règles du combat intellectuel des idées »[1248]. En second lieu,

[1243] Ibid. §42.
[1244] Voir Cour EDH, 22 avril 2010, *Fatullayev c. Azerbadjian*, req n° 40984/07, § 94.
[1245] Cour EDH, 16 juillet 2009, *Willem c. France*, req. n° 10883/05, § 37.
[1246] *Ibid.* §38.
[1247] Cour EDH, 16 juillet 2009, *Feret c. Belgique*, req. N° 15615/07, § 77.
[1248] Cour EDH, 16 janvier 2014, *Tierbefreier E.V. c. Allemagne*, req. n° 45192/09, § 56.

la Cour précise également que les lanceurs d'alerte sont soumis à des limites dans leur liberté d'expression. Ces derniers doivent agir avec vigilance et modération[1249].

[1249] Conseil de l'Europe / Cour européenne des droits de l'Homme, *Internet : la jurisprudence de la Cour européenne des droits de l'Homme*, 2011, mise à jour en juin 2015, p. 27.

Conclusion du Chapitre VIII

574. Les sanctions contre les comportements illicites en ligne doivent être dissuasives, cependant elles doivent être proportionnelles et respectueuses des droits fondamentaux. Les mesures de blocage et de filtrage, par exemple, utilisées comme mesures dissuasives contre la publication des contenus sur Internet peuvent représenter une atteinte forte aux droits des utilisateurs. De plus, ces mécanismes sont souvent utilisés de façon impropre pour faire taire les défenseurs des droit humains et les opposants politiques. Ces mesures montrent la tension qui existe entre les différents droits fondamentaux sur Internet, d'une part, il y a la volonté de modérer les contenus illicites et, de l'autre, la nécessité de protéger certaines libertés comme la liberté d'expression et de recevoir des informations. La liberté d'expression est omniprésente en ligne et voit sa protection accrue au profit de l'intérêt général même si des limites s'appliquent, en particulier lorsqu'on est face à des propos haineux ou portant atteinte à la vie privée.

CONCLUSION DU TITRE II

575. Des sanctions inadaptées - Nous avons vu que les cyberviolences ont des caractéristiques propres qui devraient être prises en compte pour leur qualification juridique. Le même principe devrait également être appliqué pour leur régime. Aujourd'hui, la réponse étatique est nuancée. En effet, nous constatons que les mesures répressives prévues ne sont pas assez dissuasives. De plus, avec l'apparition de nouveaux acteurs non juridiques capables d'émettre des sanctions, nous avons observé que certaines mesures adoptées peuvent, au contraire, porter atteinte aux droits fondamentaux des utilisateurs.

576. La nécessité d'adopter des mesures répressives dissuasives - Ce que nous recommandons aux acteurs « traditionnels » et aux acteurs privés est d'adopter des sanctions dissuasives mais respectueuses de droits fondamentaux des utilisateurs. Ainsi, nous observons la nécessité de prendre en compte les conséquences spécifiques des cyberviolences que nous ne constatons pas hors ligne. En effet, les comportements illicites en ligne ont des effets nuisibles sur les victimes qui perdurent dans le temps à cause de l'impossible maîtrise de la durée et des lieux de diffusion des contenus illicites.

Conclusion de la Partie II

577. Les effets mitigés des mesures de prévention et de sanction – Plusieurs mesures préventives sont adoptées aujourd'hui par les acteurs traditionnels. Il s'agit le plus souvent d'actions de sensibilisation et de formation. Bien qu'essentielles, aujourd'hui très peu d'études analytiques sont menés pour mesurer leur efficacité sur les utilisateurs qui nous permettraient d'améliorer leurs effets. De plus, peu d'attention est portée au public adulte. En effet, aujourd'hui les mesures adoptées sont souvent à destination des mineurs ou des fonctionnaires spécialisés. De plus, les efforts des plateformes sont encore modérés et dictés par leurs modèles économiques qui profitent des réactions colériques et des effets de buzz lors de la publication de contenus polémiques. Ainsi, certaines plateformes, ont également adopté des mesures préventives allant à l'encontre des droits fondamentaux des utilisateurs pour répondre aux exigences de certains États non démocratiques.

Quant aux sanctions, elles ne sont pas encore assez dissuasives pour éviter les comportements illicites et leur amplification. De surcroît, les mesures existantes ne prennent pas en compte les spécificités des cyberviolences et leurs conséquences sur les victimes. Enfin, certaines d'entre elles ne sont pas proportionnées et portent atteinte aux droits et libertés fondamentales des utilisateurs.

578. Des améliorations nécessaires pour mitiger l'exécution et l'amplification des comportements illicites – Afin de mieux répondre à ce phénomène, des sanctions adaptées aux spécificités des cyberviolences doivent être adoptées. En particulier, des sanctions avec une logique préventive éduquant les utilisateurs à une meilleure utilisation d'Internet mais également avec un effet dissuasif pour éviter le déferlement de la violence sur les réseaux sociaux. Les acteurs traditionnels et les plateformes doivent également veiller à la proportionnalité des mesures répressives. En effet, sur Internet, les droits fondamentaux des utilisateurs sont souvent mis sous tension, en témoigne la balance à faire entre la liberté d'expression et le droit à la vie privée, ou les restrictions

au droit de recevoir des informations, souvent relégué à « parent pauvre »[1250] de la liberté d'expression.

[1250] Q. VAN ENIS, « Le droit de recevoir des informations ou des idées par le biais de l'internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen ? », *Journal européen des droits de l'homme*, 2015/2, 175.

Conclusions générales

579. Des instruments juridiques existants - À travers l'analyse des spécificités des cyberviolences, leur qualification et leur régime, nous avons pu approfondir l'étude de ce phénomène d'un point de vue juridique en regardant aux droits nationaux, au droit européen et international. Notre sujet, d'une extrême actualité et en perpétuelle évolution, nous a mené à nous intéresser également à la jurisprudence et aux faits divers de plusieurs États. Au vu de ces analyses, nous pouvons soulever deux constats : premièrement qu'une définition de cyberviolences universellement acceptée par le droit international ou par le droit de l'Union européenne n'existe pas. Deuxièmement que des dispositions juridiques ont été adoptées contre les cyberviolences au sein de l'Union européenne et de certains États du Conseil de l'Europe. Depuis la fin de 2018, nous avons enregistré des évolutions législatives importantes qui ont inscrit à l'ordre du jour le sujet de cyberviolences. Plusieurs États de l'Union européenne ont adopté des dispositions *ad hoc* contre le partage de contenus à caractère sexuel contre le consentement de la personne, le raid numérique, le voyeurisme digital, d'autres, au contraire, n'ont pas fait évoluer leurs dispositions nationales et se sont contentés de répondre à ce phénomène avec des dispositions déjà existantes. En droit de l'Union européenne, nous avons assisté à l'adoption du Digital Services Act, alors qu'au niveau international aucun texte contraignant a été adopté et seuls des accords multilatéraux ou des engagements de principe ont été signés.

580. La nécessité d'adopter une définition et des règles minimales contre les cyberviolences – Si des dispositions juridiques existent, les utilisateurs continuent de faire face à des atteintes à leurs droits fondamentaux lors de l'utilisation d'Internet et des réseaux sociaux. L'absence d'une définition universellement reconnue a plusieurs conséquences qui exposent les individus à des risques. Laisser aux États le soin de décider s'ils doivent ou non prendre des mesures et de ne pas collecter de données pour mesurer l'ampleur du phénomène porte atteinte aux droits fondamentaux des personnes en ligne. S'accorder sur une définition et des règles minimales permettrait de rendre plus

uniforme la lutte contre les cyberviolences et garantirait une protection minimale aux utilisateurs dans tous les États.

581. **Le besoin d'investir et perfectionner les mesures de prévention –** Alors que nous nous demandions tout au long de ces années si nos travaux n'allaient pas devenir obsolètes au moment de leur publication compte tenu des développements des nouvelles technologies, nous sommes convaincus que cela n'est pas le cas. En effet, le constat que nous faisons aujourd'hui en 2023 est que, malgré des évolutions positives, la prévention et la sanction des cyberviolences n'est toujours pas à la hauteur. Les mesures de prévention n'ont pas encore reçu une attention adéquate de la part des pouvoirs publics et des plateformes qui dédient très peu d'efforts financiers pour mettre en œuvre des mesures. Les initiatives d'éducation et de sensibilisation sont souvent tournées vers les mineurs et non pas vers les adultes, qui sont tout autant touchés par les violences en ligne. Les mesures de modération préventives mise en place par les entreprises privées sont très peu financées et la logique commerciale prime encore sur celle de la protection des utilisateurs. Si la société civile se distingue par des initiatives innovantes, elle est encore très peu soutenue financièrement et ses efforts ne sont pas suffisants face à l'ampleur international des cyberviolences.

582. **Des sanctions inadaptées et insuffisamment dissuasives –** Les sanctions en vigueur aujourd'hui au sein de l'Union européenne semblent ne pas prendre en compte les conséquences des comportements illicites, laissant les victimes dans des situations de détresse psychologique et matérielle, tandis que les auteurs ne reçoivent pas de véritable sensibilisation pour les dissuader de réitérer les violences à l'avenir. Dans le respect des droits fondamentaux des usagers et de la proportionnalité, les sanctions devraient prendre en compte les effets nuisibles sur les victimes et avoir une fonction dissuasive et éducative pour les agresseurs.

583. **Un sujet en perpétuelle évolution -** Les épisodes de violences se multiplient partout dans le monde et de nouvelles formes de violence se développent avec les avancées de l'intelligence artificielle. Nous avons pu le constater tout au long de notre recherche. En effet, année après année les agresseurs trouvaient de nouvelles manières d'agir :

« ficha », « deepfakes » ou encore « Zoom bombing », il est nécessaire d'alerter sans cesse sur les nouveaux risques d'Internet et prévenir toute nouvelle forme de cyberviolences à travers un engagement de la communauté internationale. En effet, dans ce contexte, nous sommes convaincus que seule une réponse européenne et internationale sera efficace pour mitiger le phénomène, pour prévenir les formes actuelles et nouvelles de cyberviolences et pour sanctionner à la hauteur les responsables.

Annexes

Tableau 1

Partage non consenti des contenus à caractère sexuel[1251]			
État	**Définition**	**Sanction**	**Disposition**
Italie	Sauf si l'acte constitue une infraction plus grave, quiconque, après les avoir réalisés ou pris, envoie, livre, remet, publie ou diffuse des images ou des vidéos sexuellement explicites, destiné à rester privé, sans le consentement des personnes représentées, sera puni d'un emprisonnement d'un à six ans et d'une amende allant de 5 000 à 15 000 euros.	Un an et six ans d'emprisonnement et une amende de 5 000 à 15 0000 euros	Article 612 ter du Code pénal
France	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, avec le consentement exprès ou	Deux ans d'emprisonnement et à 60 000 € d'amende	Article 226-2-1 du Code pénal

[1251] Traductions en anglais et en français de l'autrice.

	présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1.		
Belgique		*Peine d'emprisonnement de six mois à cinq ans*	Article 371/1, §1er du Code pénal
Pays-Bas	The following shall be punished by a term of imprisonment not exceeding one year or a fine of the fourth category: a. a person who intentionally and unlawfully creates an image of a person of a sexual nature; b. a person who has access to an image as referred to under a, while he knows or should reasonably suspect that it was obtained through or as a result of an act made punishable under a.	Peine d'emprisonnement d'un an ou amende de 22 500 euros	Article 139h(1)(a) et (b) Code pénal
	2 The following shall be punished by a term of imprisonment not exceeding two years or a fine of the fourth category: a. a person who makes public an image as referred to in the first paragraph, under a, while he knows or should reasonably suspect that it was obtained through or as a result of an act made punishable in the first paragraph, under a;	Une peine d'emprisonnement n'excédant pas deux ans ou une amende de 22 500 euros	Article 139h(2)(a) et (b) Code pénal

	b. a person who discloses an image of a person of a sexual nature, knowing that such disclosure may be detrimental to that person.		
Espagne	A prison sentence of three months to one year or a fine of six to twelve months shall be imposed on anyone who, without the authorisation of the person concerned, disseminates, discloses or transfers to third parties images or audiovisual recordings of that person obtained with their consent in a home or any other place out of the reach of the eyes of third parties, when the disclosure seriously undermines the personal privacy of that person.	Une peine d'emprisonnement de trois mois à un an ou une amende de six à douze mois	Article 197(7) du Code pénal
Malta	Whosoever, with an intent to cause distress, emotional harm or harm of any nature, discloses a private sexual photograph or film without the consent of the person or persons displayed or depicted in such photograph or film shall on conviction be liable to imprisonment for a term of up to two years or to a fine (multa) of not less than three thousand euro (€,3000) and not more than five thousand euro (€5,000), or to both such imprisonment and fine. (2) A person shall not be guilty of an offence under this article if: (a) he has disclosed the sexual photograph or film solely to the person or	Une peine d'emprisonnement pouvant aller jusqu'à deux ans ou d'une amende de de trois mille euros (3 000 €) au minimum et de cinq mille euros (5 000 €) au maximum.	Article 208 E du Code pénal

	persons displayed or depicted in such photograph or film; or (b) the disclosure was necessary for the purpose of preventing, detecting or investigating a crime; or (c) to the extent that it is reasonably required, the disclosure is authorised by a court or tribunal in the course of judicial proceedings: Provided that where authorisation is so granted by a court or tribunal, the sexual photograph or film shall, without delay, be sealed by the registrar or deputy registrar of that court or tribunal and shall only be accessible by the parties to the suit or to their authorised legal representatives. (3) When the offence provided for in this article is committed as a means or in the context of blackmail the punishment shall be increased by one degree.		
Irlande	Distributing, publishing or threatening to distribute or publish intimate image without consent with intent to cause harm or being reckless as to whether harm is caused 2. (1) A person who distributes, publishes or threatens to distribute or publish an intimate image of another person— (a) without that other person's consent, and (b) with intent to cause harm to, or being reckless as to whether or not harm is caused to, the other person, is guilty of an offence. (2) For the purposes of subsection (1), a person causes	Jusqu'à 12 ou 7 ans d'emprisonnement et/ou 5 000 euros d'amende mois	Article 2 et 3 du "Harassment, harmful communications and related offences act 2020"

	harm to another person where— (a) he or she, by his or her acts, intentionally or recklessly seriously interferes with the other person's peace and privacy or causes alarm or distress to the other person, and (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm or distress to the other person. (3) A person who is guilty of an offence under this section is liable — (a) on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months, or both, or (b) on conviction on indictment to a fine or imprisonment for a term not exceeding seven years, or both. Recording, distributing or publishing intimate image without consent 3. (1) Subject to subsection (2), a person is guilty of an offence where— (a) he or she records, distributes or publishes an intimate image of another person without that other person's consent, and (b) that recording, distribution or publication, as the case may be, seriously interferes with that other person's peace and privacy or causes alarm, distress or harm to that other person. (2) Subsection (1) shall not apply to a person who distributes or publishes an intimate image for the purpose of the prevention, investigation or prosecution of an offence under this section. (3) A person who is guilty of an offence		

	under this section is liable on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months, or both.		
Portugal	Whoever creates, maintains or uses an automated file of individually identifiable data referring to political, religious or philosophical beliefs, party or trade union affiliation, private life, or ethnic origin, is punished with imprisonment for up to two years or with penalty of fine up to 240 days.	Une peine d'emprisonnement allant jusqu'à deux ans ou d'une peine d'amende allant jusqu'à 240 jours.	Article 193 du Code pénal
Suède	A person who intrudes into the private life of another person by disseminating: 1. an image of or other information about a person's sexual life; 2. an image of or other information about a person's state of health; 3. an image of or other information about a person being subjected to an offence that includes an attack on their person, liberty or peace; 4. an image of a person in a very vulnerable situation; or 5. an image of a person's wholly or partially naked body, is, if the dissemination is liable to result in serious damage to the person whom the image or information concerns, guilty of unlawful breach of privacy and is sentenced to a fine or imprisonment for at most two years.	Une amende ou une peine de prison de deux ans au maximum.	Section 6 (c) chapitre 4 du Code pénal

Pologne	Whoever preserves the image of a naked person or person during sexual activity, using violence against him/her for this purpose, an unlawful threat or deception, or the image of a naked person or person during sexual activity, disseminates without his/her consent, is punishable by imprisonment from 3 months to 5 years.	Peine d'emprisonnement de 3 mois à 5 ans.	Article 191 (a) du Code pénal

Tableau 2

Haine en ligne[1252]			
État	**Définition**	**Sanction**	**Disposition**
Allemagne	(1) Whosoever, in a manner capable of disturbing the public peace 1. incites hatred against segments of the population or calls for violent or arbitrary measures against them; or 2. assaults the human dignity of others by insulting, maliciously maligning, or defaming segments of the population, shall be liable to imprisonment from three months to five years. (2) Whosoever 1. with respect to written materials (section 11(3)) which incite hatred against segments of the population or a national, racial or religious group, or one characterised by its ethnic customs, which call for violent or arbitrary measures against them, or which assault the human dignity of others by	De trois mois à 5 ans d'emprisonnement et amende	Section 130 du Code pénal

[1252] Traductions en anglais de l'autrice.

	insulting, maliciously maligning or defaming segments of the population or a previously indicated group (a) disseminates such written materials; (b) publicly displays, posts, presents, or otherwise makes them accessible; (c) offers, supplies or makes them accessible to a person under eighteen years; or (d) produces, obtains, supplies, stocks, offers, announces, commends, undertakes to import or export them, in order to use them or copies obtained from them within the meaning of Nos (a) to (c) or facilitate such use by another; or 2. disseminates a presentation of the content indicated in No 1 above *by radio, media services, or telecommunication services shall be liable to imprisonment not exceeding three years or a fine*. (3) Whosoever publicly or in a meeting approves of, denies or downplays an act committed under the rule of National Socialism of the kind indicated in section 6 (1) of the Code of International Criminal Law, in a manner capable of disturbing the public peace shall be liable to imprisonment not exceeding five years or a fine. (4) Whosoever publicly or in a meeting disturbs the public peace in a manner that violates the dignity of the victims by approving of, glorifying, or justifying National Socialist rule of arbitrary force shall		

	be liable to imprisonment not exceeding three years or a fine.		
Croatie	(1) Anyone who by press, radio, TV, *computer system or network*, on public gathering or in any other way, publicly incites or makes available to the public leaflets, pictures or other material that incites to violence or hatred directed towards a group of people or a member of a group on the grounds of race, religion, national or ethnic belonging, origin, skin colour, gender, sexual orientation, gender identity, disability or any other characteristics, will be punished up to three years of prison. (2) Whoever organizes or leads a group of three or more persons for perpetrating acts from paragraph (1) of this article, will be punished from six months up to five years of prison. (3) Whoever participates in the join activity stated in the paragraph (2) of this article, will be punished up to one year of prison. (4) Anyone who publicly approves, incites or considerably lessens criminal act of genocide, crime of aggression, crime against humanity or war crime directed towards a group of people or a member of a group on the grounds of race, religion, national or ethnic belonging, origin, skin colour and in a way that is suitable for incitement to violence and hatred against such group or a member of	De 6 mois à 5 ans d'emprison nement	Article 325 Code pénal

	a group, will be punished as stated in the paragraph (1) of this article. (5) For the attempt stated in paragraphs (1) and (4) of this article, perpetrators will be punished.		
Espagne	Article 510. 1. Seront punis d'une peine d'emprisonnement de un à quatre ans et d'une amende de six à douze mois : (a) Ceux qui, publiquement, encouragent, promeuvent ou incitent, directement ou indirectement, à la haine, à l'hostilité, à la discrimination ou à la violence à l'égard d'un groupe, d'une partie d'un groupe ou d'une personne déterminée en raison de leur appartenance à ce groupe, pour des motifs racistes, antisémites ou autres liés à l'idéologie, à la religion ou aux convictions, à la situation familiale, à l'appartenance à une ethnie, une race ou une nation, à l'origine nationale, au sexe, à l'orientation ou à l'identité sexuelle, en raison du sexe, d'une maladie ou d'un handicap. b) Ceux qui produisent, élaborent, possèdent en vue de les distribuer, donnent accès à des tiers, distribuent, diffusent ou vendent des écrits ou tout autre type de matériel ou de média qui, par leur contenu, sont propres à encourager, promouvoir ou inciter, directement ou indirectement, à la haine, à l'hostilité, à la discrimination ou à la violence contre un groupe, une partie d'un groupe, ou contre une personne déterminée en raison de son	De 6 mois à 4 ans d'emprisonnement et d'une amende de 6 à 12 mois	Article 510 du Code pénal

	appartenance à un tel groupe, pour des motifs racistes, antisémites ou autres liés à l'idéologie, à la religion ou aux convictions, à la situation familiale, à l'appartenance à une ethnie, une race ou une nation, à l'origine nationale, au sexe, à l'orientation ou à l'identité sexuelle, au genre, à la maladie ou au handicap. (c) nier publiquement, banaliser gravement ou glorifier les crimes de génocide, les crimes contre l'humanité ou les crimes contre les personnes et les biens protégés en cas de conflit armé, ou glorifier les auteurs de ces crimes, lorsqu'ils sont commis contre un groupe ou une partie d'un groupe, ou contre une personne déterminée en raison de son appartenance, pour des motifs racistes, antisémite ou pour d'autres raisons liées à l'idéologie, à la religion ou aux convictions, à la situation familiale ou à l'appartenance à une ethnie, une race ou une nation, à l'origine nationale, au sexe, à l'orientation ou à l'identité sexuelle, au genre, à la maladie ou au handicap, lorsque cela favorise ou encourage un climat de violence, d'hostilité, de haine ou de discrimination à leur égard. 2. Seront punis d'un emprisonnement de six mois à deux ans et d'une amende de six à douze mois : a) Ceux qui portent atteinte à la dignité des personnes par des actions qui impliquent l'humiliation, le mépris ou le discrédit de l'un des groupes visés à la section		

	précédente, ou d'une partie d'entre eux, ou d'une personne déterminée en raison de son appartenance à ces groupes pour des motifs racistes, antisémites ou autres liés à l'idéologie, à la religion ou aux convictions, à la situation familiale, à l'appartenance de ses membres à une ethnie, une race ou une nation, à son origine nationale, à son sexe, à son orientation ou son identité sexuelle, pour des raisons de sexe, de maladie ou de handicap, ou produire, élaborer, posséder dans le but de distribuer, donner accès à des tiers, distribuer, diffuser ou vendre des écrits ou tout autre type de matériel ou média qui, de par leur contenu, sont aptes à porter atteinte à la dignité des personnes en représentant une humiliation grave, un mépris ou un discrédit de l'un des groupes susmentionnés, d'une partie d'entre eux, ou de toute personne spécifique en raison de son appartenance à ceux-ci. b) Ceux qui glorifient ou justifient, par tout moyen d'expression ou de diffusion publique, les crimes qui ont été commis contre un groupe, une partie d'un groupe ou une personne déterminée en raison de son appartenance à ce groupe pour des motifs racistes, antisémites ou autres liés à l'idéologie, à la religion ou aux convictions, à la situation familiale, à l'appartenance à une ethnie, une race ou une nation, à l'origine nationale, au sexe, à l'orientation ou à l'identité sexuelle, au genre, à la maladie ou		

	au handicap, ou ceux qui ont participé à leur exécution. Les infractions sont punies d'un à quatre ans d'emprisonnement et d'une amende de six à douze mois lorsqu'elles favorisent ou encouragent un climat de violence, d'hostilité, de haine ou de discrimination à l'égard des groupes susmentionnés. *3. Les peines prévues aux paragraphes précédents sont appliquées dans leur moitié supérieure lorsque les actes ont été réalisés par un moyen de communication sociale, par Internet ou par l'utilisation des technologies de l'information, de telle sorte qu'ils sont accessibles à un grand nombre de personnes.* 4. Lorsque les faits, compte tenu de leurs circonstances, sont de nature à troubler la paix publique ou à créer un grave sentiment d'insécurité ou de crainte parmi les membres du groupe, la peine est prononcée dans la moitié supérieure de la peine, qui peut être portée au degré supérieur. 5) Dans tous les cas, la peine d'interdiction spéciale est également prononcée pour les activités d'éducation, d'enseignement, de sport et de loisirs pour une durée de trois à dix ans supérieure à la durée de la peine privative de liberté prononcée dans le jugement, compte tenu de la gravité de l'infraction, du nombre d'infractions commises et de la situation du délinquant. Le juge ou le tribunal ordonne la destruction, l'effacement ou la mise hors		

	d'usage des livres, des dossiers, des documents, des articles et de tout type de support objet du délit visé aux articles précédents ou au moyen duquel il a été commis. Lorsque l'infraction a été commise au moyen des technologies de l'information et de la communication, la suppression des contenus est ordonnée. *Dans les cas où, par le biais d'un portail d'accès à Internet ou d'un service de la société de l'information, les contenus visés au paragraphe précédent sont diffusés de manière exclusive ou prédominante, il est procédé au blocage de l'accès ou à l'interruption de sa diffusion.*		
Grèce	1. Whoever intentionally, publicly, orally or through the press, *through the Internet or in any other means or manner*, incites, provokes, incites or incites acts or actions that can cause discrimination, hatred or violence against a person or group of persons, who are identified on the basis of race, color, religion, descent, national or ethnic origin, sexual orientation, gender identity, gender characteristics or disability, in a manner that endangers public order or poses a threat to the life, liberty or physical integrity of the aforementioned persons, shall be punished by imprisonment of three (3) months to three (3) years and a fine of five to twenty thousand (5,000 - 20,000) euros.	De 3 mois à 3 ans d'emprison nement et d'une amende de 5 000 à 20 000 euros.	Article 1 de la loi 927/1979, Official Gazette A΄139/28.6.1979, 2014

Lettonie	Section 150. Incitement of Social Hatred and Enmity (1) For a person who commits an act oriented towards inciting hatred or enmity depending on the gender, age, disability of a person or any other characteristics, if substantial harm has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine. (2) For the criminal offence provided for in Paragraph one of this Section, if it has been committed by a public official or a responsible employee of an undertaking (company) or organisation, or a group of persons, or *if it committed using an automated data processing system*, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine. (3) For the act provided for in Paragraph one of this Section, if it is related to violence or threats or if it is committed by an organised group, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine.	Trois ans d'emprison nement, ou un travail d'intérêt général, ou une amende	Article 150 du Code pénal

Bibliographie

Nous avons retenu une bibliographie présentant nos sources à la fois de manière thématique et alphabétique.

OUVRAGES GENERAUX

Nouvelles technologies

ATTIA J. J., VERBIEST T., *Un nouvel Internet est-il possible ?,* 1ère édition, Bruylant, 2020.

BADOUARD R., *Les Nouvelles lois du web,* Modération et censure, Éditions du Seuil et La République des Idées, octobre 2020.

BEELEN A., CHARLIER C., VIGNERON J., *Guide pratique des plateformes,* 20 legal designs commentés, 1ère édition, Larcier, 2021.

BENYEKHLEF K., TRUDEL P., *État de droit et virtualité*, Les éditions Thémis, 2009.

BRUNS A., *Are filter Bubbles real?,* Polity, 2019.

BURGESS A., W., BAKER T., *Cyberstalking,* J.C.W. Boon & L, 2002.

CACHARD O., *La régulation internationale du marché electronique*, LGDJ, Tome 365.

CASTETS-RENARD C., *Droit du marché unique numérique et intelligence artificielle,* 1ère édition, Bruylant, 2020.

DE FELCOURT G., *L'usurpation d'identité ou l'art de la fraude sur les données personnelles,* CNRS éditions, 2014.

ERNOTTE F., *Droits des réseaux sociaux,* 1ère édition, Larcier, 2021.

EYNARD J. (dir), *L'identité numérique*, 1ère édition, Larcier, 2020.

FAUCHOUX V., DÉPREZ P. et al., *Le droit de l'Internet,* LexisNexis, 3ème édition, 2017.

FÉRAL-SCHUHL C., *Cyberdroit - Le droit à l'épreuve de l'Internet 2020-2021,* 8ème édition, 02/2020.

FITTON L., GRUEN M., POSTON L., *Twitter for dummies*, Hoboken, NJ: John Wiley & Sons, 2009.

FLORE D., FRANSSEN V., *Société numérique et droit pénal*, Belgique, France, Europe, 1ère édition, Bruylant, 2019.

HECKER M., *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015.

JONGEN F., STROWEL A., *Droit des médias et de la communication*, Presse, audiovisuel et Internet, 1ère édition, Larcier, 2017.

KITTICHAISAREE K., *Public International Law of Cyberspace*, Springer, 2018.

KEMPF O., *Introduction à la cyberstratégie*, Economica, 2ème édition, 2015.

LEPAGE A., *Libertés et droits fondamentaux à l'épreuve d'Internet*, Dalloz, 12eme édition, 2006.

OWEN T., NOBLE W., SPEED F. C., *New Perspectives on Cybercrime*, Springer International Publishing AG, 1ère edition, 2017.

PARISER E., *The Filter Bubble: What The Internet Is Hiding From You*, Penguin, 2012.

POULLET Y., *Vie privée, liberté d'expression et démocratie dans la société numérique*, 1ère édition, Larcier, 2020.

QUÉMÉNER M., *Le droit face à la disruption numérique*, Gualino, 1ère édition, 2018.

REED C., MURRAY A., *Rethinking the jurisprudence of cyberspace*, Rethinking Law series, Edward Elgar, 2018.

SALVADORI I., *L'adescamento di minori: il contrasto al child-grooming tra incriminazione di atti preparatori ed esigenze di garanzia*, Giappichelli, 2018.

SUMMERS S., SCHWARZENEGGER C., EGE G., YOUNG F., *The Emergence of EU Criminal Law. Cyber Crime and the Regulation of the Information Society*, Oxford, Hart Publishing, 2014.

SVANTESSON D. J. B., *Private international law and the internet*, 2nd edition, Wolters Kluwer, 2012.

SYNODINOU T.E, *EU Internet law - regulation and enforcement*, Springer, 1st edition ed. 2017, 9 novembre 2017.

VAN CLEYNENBREUGEL P., *Plateformes en ligne et droit de l'Union européenne, Un cadre juridique aux multiples visages*, 1ère édition, Bruylant, 2020.

VENTRE D., *Cyberespace et acteurs du cyberconflits*, Lavoisier, 2011.

Droit international

ASCENSIO H., DECAUX E., PELLET A., *Droit international pénal*, 2ème édition, Éditions Pédone, 2012.

BERGHUIS A. C., « La prévention générale : limites et possibilités », *Les objectifs de la sanction pénale. En hommage à Lucien Slachmuylder*, Bruylant, 1989.

BONIS E., PELTIER V., *Droit de la peine*, 3ème édition, LexisNexis, 2011.

BUREAU D., MUIR WATT H., *Droit international privé*, Tome I, partie générale, 4ème édition, 2017.

BURGORGUE LARSEN L., *La vulnérabilité saisie par les juges en Europe*, Cahiers européens, Pedone, 2014.

CAPPADORO H., *Le sens de la peine*, Bibliothèques de droit, L'Harmattan, 2018.

CARREAU D., MARRELLA F., *Droit international public*, 12ème édition, Éditions Pédone, 2018.

CHAINAIS C., FENOUILLET D., GUERLIN G. (dir.), *Les sanctions en droit contemporain, La motivation des sanctions prononcées en justice*, Dalloz, 2013.

COMBACAU J., SUR S., *Droit international public*, LGDJ, 13ème édition, 2019.

DAILLIER P., FORTEAU M., PELLET A., *Droit international public*, L.G.D.J, 8ème édition, 2008.

DECAUX E., DE FROUVILLE O., *Droit international public*, Hypercours Dalloz, 10ème édition, 2016.

DECAUX E., DE FROUVILLE O., *Droit international public*, Hypercours Dalloz, 12ème Edition, 2020.

DELMAS- MARTY M., Le pluralisme ordonné, *Les forces imaginantes du droit (II)*, Seuil, 2006.

DELMAS- MARTY M., *Les forces imaginantes du droit. Le relatif et l'universel*, Seuil, 2004.

DE SCHUTTER O., TRIALLE L., TULKENS F., VAN DROOGHENBROECK S., Droit international des droits humains, Codes essentiels, Larcier, 2019.

FERNANDEZ J., *Droit international pénal*, LGDJ, 2022.

FERNANDEZ J., *Justice pénale internationale*, CNRS, 2016.

HERNANDEZ G., *International law*, Oxford, 2nd edition, 2022.

KELLENS G., *La mesure de la peine,* Liège, Collection scientifique de la Faculté de droit de Liège, 1982.

PRADEL J., *Droit pénal comparé*, Dalloz, 4ème édition, 2016.

REBUT D., *Droit pénal international,* 4ème édition, Dalloz, 2022.

REVET T., Rapport de synthèse, in *La vulnérabilité*, Journée québécoises 2018, Association Henri Capitant, Bruylant, 2020, p. 10.

ROBERT P., *La peine, quel avenir ? Approche pluridisciplinaire de la peine judiciaire*, Le Cerf, 1983.

SUDRE F., *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme*, Droit et justice, Bruylant, 2005.

SUDRE F., MILANO L., PASTRE-BELDA B., SCHAHMANECHE A., *Droit européen et international des droits de l'homme*, 16ème édition, PUF, 2023.

VAN DROOGHENBROECK S., *La proportionnalité dans le droit de la Convention européenne des droits de l'homme – Prendre l'idée simple au sérieux*, Bruylant, 2001.

Droit de l'Union européenne

BARNARD C., PEERS S., *European Union Law*, 4eme edition, Oxford, Oxford University Press, 2023.

BLIN O., *Droit institutionnel, matériel et contentieux de l'Union européenne*, 3ème édition, Bruylant, 2018.

BLANQUET M., *Droit général de l'Union européenne,* Sirey, 11ème édition, 2018.

BLUMANN C., *Droit institutionnel de l'Union européenne*, LexisNexis, 7ème édition, 2023.

BLUMANN C., DUBOUIS L., *Droit institutionnel de l'Union européenne*, LexisNexis, 7ème édition, 2019.

BLUMANN C., DUBOUIS L., *Droit matériel de l'Union européenne*, LGDJ, 8ème édition, 2019.

BRUNESSEN B. (dir.), *La politique européenne du numérique*, 1ère édition, Bruylant, 2022.

HAGUENAU-MOIZARD V. C., GAZIN F., LEBLOIS-HAPPE J., *Les fondements du droit pénal de l'Union européenne*, 1ère édition, Larcier, 2015.

MARTUCCI F., *Droit de l'Union européenne*, Paris, Dalloz, 2017.

PICOD F., *Droit de l'Union européenne des droits de l'homme et des libertés fondamentales*, Jurisclasseur Europe, fascicule 120, 2007.

PICOD F., VAN DROOGHENBROECK S., *Charte des droits fondamentaux de l'Union européenne*, commentaire article par article, Bruylant, 2018.

RIDEAU J., *Droit institutionnel de l'Union européenne*, LGDJ, 6ème édition, 2010.

SIMON D., *Le système juridique communautaire*, PUF, 3ème édition, 2001.

TINIÈRE R., VIAL C. (dir.), *Les dix ans de la Charte des droits fondamentaux de l'Union européenne. Bilan et perspective*s, Bruylant, 2020.

TINIÈRE R., VIAL C. (dir.), *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, Bruylant, 2015.

THESES

BLONDEL M., *La personne vulnérable en droit international*, Thèse de doctorat, Université de Bordeaux, 2015.

CRIQUI-BARHALAIS G., *La protection des libertés individuelles sur le réseau Internet*, Université Paris II Panthéon Assas, Thèse de doctorat, 2018.

DESARA D., *The phenomenon of online live-streaming of child sexuel abuse: challenges and legal responses*, Thèse de doctorat, Alma Mater Studiorum – Università di Bologna, 2019.

DI TANO F., *Hate speech e comportamenti d'odio in rete: un'analisi comparatistica in prospettiva de iure condendo*, Thèse de doctorat, Alma Mater Studiorum – Università di Bologna, 2017.

GUIZIOU-PÉRONNE G., *Les cyberdélits et le droit international privé*, Thèse de doctorat, Université Paris I Panthéon-Sorbonne, 2013.

MARTINEAU A.C, *Une analyse critique du débat sur la fragmentation du droit internationa*l, Thèse, Université Panthéon-Sorbonne - Paris I, 2013.

MERRA L., *Pour une sociologie des médias sociaux. Internet et la révolution médiatique : nouveaux médias et interactions*, Thèse de doctorat, Paris Sorbonne Cité - Paris Descartes, 2013.

MOUNDOUNGA NTSIGOU S., *La fragmentation du droit international public : l'œuvre de codification à la lumière de la fragmentation du droit international*, Thèse de doctorat, Université de Strasbourg, 2013.

QUILTON A., *L'exercice des droits et libertés fondamentaux sur l'Internet*, Thèse de doctorat, Université d'Aix-Marseille, 2014.

SAINT-PAU J-Ch., *L'anonymat et le droit*, Thèse de doctorat, Bordeaux IV, 1998.

ZWOLINSKA M., *Sécurité et libertés fondamentales des communications électroniques en droit français, européen et international*, Thèse de doctorat, Université Nice Sophia Antipolis, 2015.

ACTES DE COLLOQUE

ASSOCIATION HENRI CAPITANT, « La vulnérabilité », Journées québécoises 2018, Bruylant, 2020.

SFDI, *Le standard de due diligence et la responsabilité internationale*, Journée d'études franco-italienne du Mans, Pedone, 2018.

REVUES ET CONTRIBUTIONS A DES OUVRAGES COLLECTIFS

Droit et nouvelles technologies

BANNEUX N., KERZMANN L., « Le mal nommé « harcèlement téléphonique » : chronique des tribulations législatives d'une infraction moderne », *RDTI*, 2009/1, n° 34.

BASECQZ N., *La protection pénale des personnes vulnérables dans l'environnement numérique*, 2018 in JACQUEMIN H., NIHOUL M. (eds), *Vulnérabilités et droits dans l'environnement numérique*, Collection de la Faculté de droit de l'UNamur, Larcier, Bruxelles.

BAUDINO H., « L'anonymat sur le web, un éternel marronnier politique », *L'observatoire*, 20 novembre 2020.

BELLOIR P., « La répression pénale du « phishing » », *Revue Lamy Droit de l'Immatériel*, N° 12, 1er janvier 2006.

BENABOU V-L., « Bannir l'ex-président des Etats-Unis d'un réseau social. So what ? », *Le Club des juristes*, 6 juillet 2021.

BENSOUSSAN A., « L'arsenal législatif existant pour punir les deepfakes », *Lexing*, 14 août 2019.

BOLLÉE S., HAFTEL B., « Les nouveaux (dés)équilibres de la compétence internationale en matière de cyberdélits après l'arrêt eDate Advertising et Martinez », *Recueil Dalloz*, 2012.

BROWN N. I., « Deepfakes and the Weaponization of Information», *Virginia Journal of Law & Technology*, Vol. 23, n° 01, 2020.

CALETTI G. M, « « Revenge porn » e tutela penale, Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane », *Diritto penale contemporaneo*, Rivista trimestrale, 3/2018.

CALLANAN C., GERCKE M., DE MARCO E., DRIES-ZIEK ENHEINER H., « Filtrage d'Internet – Équilibrer les réponses à la cybercriminalité dans une société démocratique », *Juriscom*, 2010.

CAMMILLERI A., « Intelligence artificielle et droit de la cybersécurité dans l'Union européenne », *RDUE*, 2017/4.

CELESTE E., « Digital punishment: social media exclusion and the constitutionalising role of national courts », *International Review of Law, Computers & Technology*, 35:2, 2021.

CELESTE E., « Trump's social media ban: Reviewing the constitutionality of permanent digital punishment », *Digital Society Blog*, Alexander Von Humboldt, Institut für Internet und Gesellschaft, 17 mars 2021.

ÇETINKAYA O., GÜNGÖRDÜ A., « When national laws and international standards are at odds: human rights responsibilities of social media platforms under Turkey's new internet law », *International Bar Association*, 2021.

CITRON D. K., « Sexual Privacy », *128 Yale Law Journal 1870*, 2019.

CITRON D. K., CHESNEY R., « Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security », 107 *California Law Review* 1753, 2019.

DAVIO E., « Anonymat et autonomie identitaire sur Internet », *Droit des technologies de l'information*, sous la direction de Etienne Montero, CRID, Bruyant, 1999.

DE BACKER N., « Le principe de proportionnalité à l'épreuve de la liberté d'expression numérique », *JEDH*, 2019/4.

DE TERWANGNE C., « Internet et la protection de la vie privée et des données à caractère personnel », in VAN ENIS Q. et DE TERWANGNE C., *L'Europe de droits de l'homme à l'heure d'Internet,* Bruyant, 2019.

DI NICOLA A., BARATTO G., MARTINI E., « Surf and Sound: The role of the Internet in people smuggling and human trafficking », *CSD*, Department 'Faculty of Law, University of Trento, March 2017.

DOCKSEY C., « Chapitre 3 - Articles 7 and 8 of the EU Charter: two distinct fundamental rights » in GROSJEAN A. (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1ère édition, Larcier, 2015.

DOCQUIR P.F., « Chapitre 2. - La confrontation entre droits fondamentaux et puissances privées vue à travers le prisme de la liberté d'expression » in VAN ENIS Q. et DE TERWANGNE C. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1ère édition, Bruylant, 2019.

DONEGAN R., « Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis », *Strategic Communication Elon University*, 2010.

DUBUISSON F., « Société de l'information, médias et liberté d'expression », *JEDH*, 2014/3.

DUBUISSON F., PIERET J., « Chronique. Société de l'information, médias et liberté d'expression », *JEDH*, 2017/3.

DUBUISSON F., PIERET J., « Société de l'information, médias et liberté d'expression », *JEDH*, 2021/4-5.

DUBUISSON F., RORIVE I., « La liberté d'expression à l'épreuve d'Internet », in *Entre ombres et lumières : cinquante ans d'application de la Convention européenne des droits de l'homme en Belgique*, Centre de droit public de l'Université libre de Bruxelles, Bruxelles, Bruylant, 2008.

ESTANO N., « Nouvelles technologies et cyberharcèlement : l'exemple du swatting », *Criminologie*, Volume 52, Numéro 2, Automne 2019.

FRANCILLON J., « Le droit pénal face à la cyberdélinquance et à la cybercriminalité », *Revue Le Lamy Droit de l'immatériel*, Nº 81, 1er avril 2012.

GAFFNEY H., « Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review », *Aggression and Violent Behavior*, 2018.

GEORGES F., « Identités virtuelles : Les profils utilisateur du web 2.0 », *Questions théoriques*, 2010.

GIUSTINIANI F. Z., « I limiti alla libertà di espressione nell'agorà politica virtuale e la cyberviolenza comme nuova forma di violenza domestica », *Nomos*, 1-2020.

HENRY N., POWELL A., « Sexual violence in the digital age: The scope and limits of criminal law », *Social & Legal Studies*, 25(4), 2016.

HORSMAN G., « The Challenges Surrounding the Regulation of Anonymous Communication Provision in the United Kingdom », *Computers & Security*, 2015.

JAMES ENZWEILER M., « Swatting Political Discourse: A Domestic Terrorism Threat », *Notre Dame Law Review*, Vol. 90, 2015.

JAQUEMIN Z., Les sanctions civiles comme outils de régulation de l'activité numérique, in CASTETS-RENARD C., NDIOR V., RASS-MASSON L., *Enjeux internationaux des*

activités numériques : Entre logique territoriale des États et puissance des acteurs privés, Larcier, 2020.

JAULT-SESEKE F., « Internet, vecteur d'affinement des règles de compétence juridictionnelle », in *Internet et le droit international*, SFDI, Pedone, 2014.

KLONICK K., The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression, *Yale Law Journal*, Vol. 129, No. 2418, 2020.

LAGRANGE P., « Internet et l'évolution normative du Droit international : d'un Droit international applicable à l'internet à un DI du cyberespace ? », in *Internet et le droit international*, SFDI, Pedone, 2014.

LANDIN A. B., « La lutte contre les contenus haineux sur Internet. L'ex-article premier paragraphe II de la loi Avia à la lumière de la question de la responsabilité », in *Études digitales*, Capitalocène et plateformes, Hommage à Bernard Stiegler, vol. 1, n° 9, 2020.

LAVOIE P-E., FORTIN F., TANGUAY S., « Problèmes relatifs à la définition et à la mesure de la cybercriminalité » in FORTIN F. (dir.) *Cybercriminalité, entre inconduite et crime organisé*, Presses Internationales Polytechniques Polytechnique et Sûreté du Québec, 2013.

LAWSON A., «Automation in moderation: Preserving fundamental rights while moderating online content at scale », *Observer Research Foundation*, 14 avril 2021.

LEISER M., « AstroTurfing,'CyberTurfing' and other online persuasion campaigns », *European Journal of Law and Technology*, vol. 7, n° 1, 2016.

LOUIS-SIDNEY B., « La dimension juridique du cyberespace », *Revue internationale et stratégique*, 2012/3, n° 87, 2012.

MAILHÉ F., « CJUE, 1re ch., 17 juin 2021, Mittelbayerischer Verlag KG c/ SM, aff. C-800/19, ECLI:EU:C:2021:489 », *Jurisprudence de la CJUE 2021*, Décisions et commentaires 2022.

MARTIN D., « Cybercriminalité : l'importance du facteur humain », in La criminalité numérique, *Cahiers de la sécurité* n° 6, INHES octobre-décembre 2008.

MAYER SCHONBERGER V., « The shape of governance: analysing the World of internet regulation », *Virginia Journal of international law*, vol. 43, 2003.

MCHANGAMA J., J. FISS J., « The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship », *Justitia*, novembre 2019.

MOUTOT R., « Lutter contre les contenus illicites et imposer une plus grande transparence aux plateformes : publication du *Digital Services Act* au JOUE », *Dalloz Actualité,* 10 janvier 2023.

MOYSE F., « Chapitre 4 - La protection des données personnelles entre droits de l'homme et droits fondamentaux » in A. GROSJEAN (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, 1ère édition, Larcier, 2015.

MUIZNIZKS N., « Le blocage arbitraire d'Internet porte atteinte à la liberté d'expression », *Le carnet des droits de l'Homme*, Commissaire aux droits de l'Homme, Conseil de l'Europe, 26 septembre 2017.

NDIOR V., « Le Conseil de surveillance de Facebook et la protection des libertés », *RDLF*, chron. n°23, 2022.

NORODOM A.T., « Internet et le droit international : défi ou opportunité ? » in *Internet et le droit international*, Colloque de Rouen, SFDI, Pedone, 2014.

NORODOM A.T., « Le droit international et Internet après l'« affaire Snowden » : La recherche de nouveaux équilibres », in *Annuaire français de droit international*, volume 60, 2014.

NORODOM A.T., « Secret et droit international public : le droit à la vie privée à l'ère numérique », in BLAIZOT-HAZARD C. (dir.), *Les NTIC face aux droits et libertés fondamentaux à travers le prisme du secret*, Institut universitaire Varenne, 2017.

PAILLER L., « Chapitre 1 - La garantie du libre accès au réseau social par la vie privée sociale » in *Les réseaux sociaux sur Internet et le droit au respect de la vie privée*, 1ère édition, Larcier, 2012.

PATRICK J., « La gouvernance de l'Internet du point de vue du droit international public », in *Annuaire français de droit international*, volume 56, 2010.

PEYROU S., « Société de l'information, vie privée et protection des données à caractère personnel : des précisions attendues CJUE Gde ch. 24 septembre 2019, aff. C-507/17, Google LLC - CJUE Gde ch. 24 septembre 2019, aff. C-136/17, GC e.a. - CJUE 1er octobre 2019, aff. C-673/17, Planet49 – CJUE, 3 octobre 2019, aff. C-18/18, Eva Glawischnig-Piesczek c. Facebook Ireland Limited », *RDUE*, 2020/1.

QUEMENER M., « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », *Sécurité et stratégie*, 2011/1 (5), 2011.

RESTA G., « Anonimato, responsabilità, identificazione: prospettive di diritto comparato », *Il diritto dell'informazione et dell'informatica*, Anno XXX, Fasc. 2 -2014.

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, Laterza, 2014.

RONA G., AARONS L., « State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace », 26 octobre 2016, *8 Journal of National Security Law and Policy*, 2016.

RUET C., « Chapitre 5. - Liberté d'expression et lutte contre le discours de haine sur Internet » in VAN ENIS Q. et DE TERWANGNE C. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1e édition, Bruxelles, Bruylant, 2019.

SIRINELLI P., « L'adequation entre le village virtuel et la création normative - Remise en cause du role de l'État ? » in BOELE-WOELKI K. et KESSEDJIAN C., *Internet: Which Court Decides? Which Law Applies?*, 1998.

SUNSTEIN C. R., « Social Norms and Social Roles », *Columbia Law Review*, vol. 96, no. 4, Columbia Law Review Association, Inc., 1996.

TAXIL B., « Internet et l'exercice de droits fondamentaux », in *Internet et le droit international*, Colloque de Rouen, SFDI, Pedone, 2014.

THIERRY G., « Le nouveau pôle spécialisé contre la haine en ligne, une structure très attendue », *DALLOZ Actualité*, 3 février 2021.

TöLLER M., « Revenge porn ou vengeance pornographique », *RDTI*, 2018/71.

TRÉGUER F., « Anonymat et chiffrement, composantes essentielles de la liberté de communication » in VAN ENIS Q. et DE TERWANGNE C. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, Bruylant, 2019.

TRÉGUER F., « Internet dans la jurisprudence de la Cour européenne des Droits de l'Homme », *RDLF*, chron. n°13, 2013.

TURGIS S., « La coexistence d'Internet et des médias traditionnels sous l'angle de la Convention européenne des droits de l'homme », *RTDH*, 2013, nr. 93.

TURGIS S., « La conciliation d'un droit à l'oubli avec les droits fondamentaux consacrés par la CEDH », colloque *Le droit à l'oubli numérique, enjeux et perspectives*, organisé par l'Institut de l'Ouest : Droit et Europe (IODE) le 6 mars 2015.

TURGIS S., *Les droits de l'homme à l'heure d'Internet et du numérique : rupture ou continuité ?*, in in VAN ENIS Q. et DE TERWANGNE C. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1ère édition, Bruylant, 2019.

VALLAT T., *Un tribunal belge reconnait un viol par internet à distance...via une webcam*, Blog de maître Thierry Vallat, 26 septembre 2018.

VAN ENIS Q., « Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression » in VAN ENIS Q. et DE TERWANGNE C. (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, 1ère édition, Bruylant, 2019.

VAN ENIS Q., « Le droit de recevoir des informations ou des idées par le biais de l'internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen *?* », *Journal européen des droits de l'homme*, 2015/2.

VAN LEEUWEN F., « Cyberviolence, domestic abuse and lack of gender sensitive approach - Reflections on Buturuga v. Romania », *Strasbourg Observers*, 11 mars 2020.

Droit international

BELLAMI V., CARAZO-MÉNDEZ W., GRADIN C., « Dénonciation de la Convention d'Istanbul par la Turquie : L'insoluble équilibre entre volonté étatique et garantie des droits des femmes et des filles », *Revue Droits Fondamentaux*, n°19, 2021.

D'URSEL E., « La Convention du Conseil de l'Europe sur la prévention et la lutte contre les violences à l'égard des femmes : une révolution silencieuse ? », *Revue trimestrielle des droits de l'homme*, n° 113/2018, 2018.

DUPUY P. M., « La fragmentation du droit international ou des perceptions qu'on en a ? », *EUI Working Paper*, n° 14.

DURAND-JAMIS B., « Propos introductifs : la polarisation de la notion de fragmentation, entre unité et diversité du droit », *La Revue des droits de l'homme*, 15, 2019.

IZORCHE M-L., « La marge nationale d'appréciation, enjeu de savoir et de pouvoir, ou jeu de construction ? », *Revue de science criminelle et de droit pénal comparé*, nº 1, 2006.

MONTERO E., VAN ENIS Q., « Les gestionnaires de forums et portails d'actualités cueillis à froid par la Cour de Strasbourg ? », *RTDH*, 27e année, n° 108, 1er octobre 2016.

RASPAIL H., « Due Diligence et droits de l'homme », in CASSELLA S. (dir.), *Le standard de due diligence et la responsabilité internationale*, SFDI, Pedone, 2018.

TAMBOU O., « Chapitre 1. - Droit autonome du droit au respect de la vie privée », in *Manuel de droit européen de la protection des données à caractère personnel*, 1ère édition, Bruylant, 2020.

TOUZÉ S., « La notion de prévention en droit international des droits de l'homme », in DECAUX E. et TOUZÉ S., (Dir), *La prévention des violations des droits de l'homme,* Publications de l'Institut international des droits de l'homme n°25, Pedone, 2013.

ZOLLER E., « La Cour suprême des États-Unis et la liberté d'expression », in E. ZOLLER (dir.), *La liberté d'expression aux États-Unis et en Europe*, Dalloz, 2008.

Droit de l'Union européenne

ADALID S., COMBET M., MAZILLE C. et ROCCATI M., « L'Espace de liberté sécurité justice : un droit à géométrie variable ? », *RTDEur.*, 2012/4.

ARROYO ZAPATERO L. et MUÑIOZ DE MORALES ROMERO M., « Droit pénal européen et Traité de Lisbonne : le cas de l'harmonisation autonome (article 83.1 TFUE) », in GIUDICELLI-DELAGE G. et LAZEGES C. (dir.), *Le droit pénal de l'Union européenne au lendemain du traité de Lisbonne*, Société de législation comparée, 2012.

BERGÉ J. S., « La justice saisie par la Cour de Justice : recherche d'une spécificité du droit de l'Union européenne en matière de libre circulation de l'information diffamatoire », in BURGORGUE-LARSEN L. et CALVÈS G., *La diffamation saisie par les juges en Europe sous la direction*, Cahiers européens, Pedone, 2019.

BERNARDI A., *L'harmonisation pénale accessoire*, in GIUDICELLI-DELAGE G. et LAZEGES C. (dir.), *Le droit pénal de l'Union européenne au lendemain du traité de Lisbonne*, Société de législation comparée, 2012.

BLUMANN (Cl.), « Les compétences de l'Union européenne en matière de droits de l'homme », R.A.E. – L.E.A., 2006/1.

CARIAT N., « Article 7 respect de la vie privée et familiale », in PICOD F., RIZCALLAH C., VAN DROOGHENBROECK S., *Charte des droits fondamentaux de l'Union européenne, Commentaire article par article*, 2ème édition, Bruylant, 2020.

DUBOUT E., MARTUCCI F., PICOD F. (dir.), *L'extraterritorialité en droit de l'Union européenne*, Colloques, Bruylant, 2021.

FLORE D., « Contours, limites et perspectives du rapprochement des droits pénaux matériels au sein de l'Union européenne », *Rev. UE*, 2014/582.

MELISON D., « Arrêt « Scarlet » : le filtrage préventif par les fournisseurs d'accès à internet écarté au nom de l'équilibre entre droit d'auteur et libertés fondamentales », *JDE*, 2012/2, n° 186.

PICOD Y., « Préface » in CALMETTE J-F., *Sanctions en droit de la concurrence et concurrence des sanctions*, Mare & Martin, 2017.

TINIÈRE R., Commentaire de l'arrêt Digital Rights Ireland in PICOD F., *Jurisprudence de la CJUE 2014 - Décisions et commentaires*, Collection Droit de l'Union Européenne, Bruylant, 2015.

WACHSMANN P., Commentaire de l'article 11 liberté d'expression et d'information in F. PICOD, C. RIZCALLAH, S. VAN DROOGHENBROECK, Charte des droits fondamentaux de l'Union européenne, Commentaire article par article, 3ème édition, 2023.

Autres thématiques

ANDENAES J., « Les effets de prévention générale du droit pénal », *Archives de politique criminelle*, 1978.

BARATTA A., « Les fonctions instrumentales et les fonctions symboliques du droit pénal », *Déviance et société*, vol. 15, n° 1, 1991.

CESONI M. L., RECHTMAN R., « « La réparation psychologique » de la victime : une nouvelle fonction de la peine ? », *Revue de droit pénal et de criminologie*, 2, 2005.

MICHAUD Y., « Définir la violence ? », *Les cahiers dynamiques*, 2014/2, n°60, 2014.

RODOTÀ S., *Il diritto di avere diritti*, Roma-Bari, Laterza, 2012.

SOULET M.-H., « La vulnérabilité comme catégorie de l'action publique », *Pensée plurielle*, 2005/2, n°10, 2005.

VAN DE KERCHOVE M., « Les fonctions de la sanction pénale. Entre droit et philosophie », *Informations sociales*, 2005/7 (n° 127), 2005.

Articles non juridiques sur les nouvelles technologies

ANCEL M-E., « Un an de droit international privé du commerce électronique », *Communication, commerce électronique,* LexisNexis, n°1, janvier 2021.

AZY B., « Sexuel Harassment on the internet », *Social Science Computer Review*, Vol. 23 No. 1, Spring 2005.

BAKSHY E., MESSING S., ADAMIC L. A., « Exposure to ideologically diverse news and opinion on Facebook », *Science*, Vol 348, Issue 6239, 5 Jun 2015.

BALFE M., GALLAGHER B. et al., « Internet Child Sex Offenders' Concerns about Online Security and their Use of Identity Protection Technologies: A Review », *Child Abuse Review*, 24(6), 2015.

BEAUVISAGE T., BEUSCART J-S. et al., « Le succès sur Internet repose-t-il sur la contagion ? Une analyse des recherches sur la viralité », *Tracés. Revue de Sciences humaines*, 21/2011.

BERAN T., LI Q., « The relationship between bullying and cyberbullying », *The Journal of Student Wellbeing*, 1(2), 2007.

BERGER J.M., MORGAN J., « The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter », *The Brookings Project on US Relations with the Islamic World*, Analysis Paper, n° 20, mars 2015.

BLAYA C., « Le cyberharcèlement chez les jeunes », *Enfance*, 2018/3 n°3, 2018.

BLAYA C., « Les programmes d'intervention contre la cyberviolence et le cyberharcèlement : quels moyens, quelle efficacité ? », *Les dossiers des sciences de l'éducation*, 33, 2015.

BOCIJ P., « Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet », *First monday*, 2003.

BRITT P., DONOVAN J., « Deepfakes and Cheap Fakes, The Manipulation of Audio and Visual Evidence », *Data & Society*, 2019.

BURNS A., « In full view: Involuntary porn and the postfeminist rhetoric of choice », in NALLY C. and SMITH A. (Eds.), *Twenty-first century feminism: Forming and performing femininity*, Basingstoke, UK, Palgrave Macmillan, 2015.

CHU Z., GIANVECCHIO S., WANG H., JAJODIA S., « Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? », *IEEE Transactions on Dependable and Secure Computing*, November 2012.

DEKESEREDY W. S., SCHWARTZ M. D., « Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory », *Sexualization, Media, & Society*, 2016.

DESFORGES A., « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, 2014/1-2, n° 152-153, 2014.

DOUGLAIS D. M., « *Doxing: A Conceptual Analysis* », *Ethics Inf Technol*, 28 june 2016.

ERDUR-BAKER Ö., « Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools », *New media & society*, 12(1), 2010.

FESTINGER L., PEPITONE A., NEWCOMB T., « Some consequences of de-individuation in a group », *The Journal of Abnormal and Social Psychology, 47* (2, Suppl), 1952.

FLETCHER R., KLEIS NIELSEN R., « Automated Serendipity », *Digital Journalism*, 6:8, 976-989, 2018.

GEIGER R. S., « Bot-based collective blocklists in Twitter: the counter public moderation of harassment in a networked public space », *Information, Communication & Society*, 19:6, 787-803, 2016.

GHOSH D., « Facebook's Oversight Board Is Not Enough », *Harvard Business Review*, 16 octobre 2019.

HARKNETT R. J., CALLAGHAN J. P., KAUFFMAN R., « Leaving Deterrence Behind: War-Fighting and National Cybersecurity », *Journal of Homeland Security and Emergency Management*, January 2010.

HAYDÉE P., « De l'idéal virtuel à l'autre réel », *Dialogue*, 2009/4 (n° 186), 2009.

Holocauste : l'UNESCO, le Congrès juif mondial et TikTok partenaires contre le négationnisme, ONU Info, 27 janvier 2022.

KATSUMATA Y., MATSUMOTO T., KITANI M., TAKESHIMA T., « Electronic media use and suicidal ideation in Japanese adolescents », *Psychiatry and Clinical Neurosciences, 62*(6), 2008.

LATONERO M., « Can Facebook's Oversight Board Win People's Trust? », *Harvard Business Review*, 29 janvier 2020.

MCGLYNN C., RACKLEY E., « Not 'revenge porn,' but abuse: Let's call it image-based sexual abuse », *Inherently Human*, 15 février 2016.

MISHNA F., COOK C., SAINI M., WU M.-J., McFADDEN R., « Interventions for children, youth, and parents to prevent and reduce cyber abuse », *Campbell Systematic Reviews*, 2009.

MITCHELL K. J., YBARRA M., FINKELHOR D., « The relative importance of online victimization in understanding depression, delinquency, and substance use », *Child maltreatment*, 12(4), 3, 2007.

MORELLI P., « La viralité entre métaphore communicationnelle et approche esthétique » in *Dialogue des révolutions*, Madarat, n°29-30, 2017.

NECHUSHTAI E., LEWIS S.C., « What kind of news gatekeepers do we want machines to be? Filter bubbles, fragmentation, and the normative dimensions of algorithmic recommendations », *Computers in Human Behavior*, 2018.

NISBETH BRØGGER M., NIELBO K. L., FAGE-BUTLER A., « #detkuhaværetmig How twitter enabled the expression and propagation of solidarity among healthcare professionals », *Conjunctions: transdisciplinary journal of cultural participation*, vol. 8, no. 1.

RATHNAYAKE C., BUENTE W., « Incidental Effects of Automated Retweeting: An Exploratory Network Perspective on Bot Activity During Sri Lanka's Presidential Election in 2015, Bulletin of Science », *Technology & Society*, 1–9, 2017.

SAILLOT I., « Psychopathologie implicite de l'anonymat sur Internet », *Les Cahiers Internationaux de Psychologie Sociale*, *Presses universitaires de Liège*, Numéro 106, 2015/2.

SILVA L., MONDAL M., CORREA D. et al., « Analyzing the Targets of Hate in Online Social Media », *Tenth International AAAI Conference on Web and Social Media*, Vol. 10 No. 1, 2016.

SNYDER P., DOERFLER P., KANICH C., MCCOY D., « Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing, Proceedings of Internet Measurement Conference », *Association for Computing Machinery*, New York, NY, USA, 2017.

SPENCE R., HARRISON A., BRADBURY P., BLEAKLEY P., MARTELLOZZO E., & DEMARCO J., « Content moderators' strategies for coping with the stress of moderating content online », *Journal of Online Trust & Safety*, 2023.

WEISS T., « Japan's 'pro-nuclear civil society': Power in the analysis of social capital and civil society », *Journal of Civil Society*, vol. 15, no 4, 26 septembre 2019.

WU T., « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and Hight Technology*, Vol.2, 2003.

YBARRA M., MITCHELL K. J., « Prevalence and frequency of Internet harassment instigation: Implications for adolescent health », *Journal of Adolescent Health*, 41, 2007.

ZUIDERVEEN BORGESIUS F. J., TRILLING D., MÖLLER J., BODÓ B., DE VREESE C. H., HELBERGER N., « Should we worry about filter bubbles? », *Internet Policy Review*, 5(1), 2016.

DOCUMENTS OFFICIELS

Organisation des Nations Unies

Agences et organes des Nations Unies

Rapports

Declaration of principles, *Building the Information Society: a global challenge in the new Millennium* », Document WSIS-03/GENEVA/DOC/4-E, World Summit on the Information Society organized by the International Telecommunication Union (ITU), 12 December 2003.

DIALLO A., *A Guide for Women and Girls to Prevent and Respond to cyberviolence*, UN WOMEN, novembre 2021.

EUROPOL, *Intelligence Notification: Trafficking in Human Beings and the Internet*, November 2014.

EUROPOL, *Online Jihadist propagande*, 2020 in review, Europol Public Information, 2021.

EUROPOL, *The Internet Organised Crime Threat Assessment (IOCTA)*, 2015.

INTERPOL, *Covid19 - les menaces et les tendances en matière d'exploitation sexuelle des enfants et d'abus pédosexuels*, 7 septembre 2020.

KOSKENNIEMI M., *Rapport préliminaire sur la fragmentation du droit international : difficultés découlant de la diversification et de l'expansion du droit international*, Groupe d'étude sur la fragmentation, Commission du droit international, ILC(CVI)/SG/FIL/CRD.1, 2004.

POSETTI J., ABOULEZ N., BONTCHEVA K. et al., *Violence en ligne à l'égard des femmes journalistes : un aperçu mondial des incidences et impacts*, UNESCO et ICFJ, 2021.

POSETTI J., SHABBIR N. et al., *The Chilling: Global trends in online violence against women journalists*, UNESCO, 2021.

Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), *Malicious Uses and Abuses of Artificial Intelligence*, 2020.

UN Broadband Commission for digital development working group, *Cyberviolence against women and girls, A world-wide wake-up call*, 2015.

UN WOMEN, T*urning Promises Into Action: Gender Equality in the 2030 Agenda for Sustainable Developmen*t. Global Factsheet, 2018.

UNICRI and UNCCT, *Countering terrorism online with artificial intelligence*, An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia, 2021.

UNICRI, *Stop the virus of disinformation*, The risk of malicious use of social media during COVID-19 and the technology options to fight it, November 2020.

UNICRI, UNCCT, *Countering terrorism online with artificial intelligence*, 2021.

UNODC, *Global report on trafficking in persons*, 2020.

UNODC, *The Use of the Internet for Terrorist Purposes*, 2012.

UNODC, *Utilisation de l'Internet à des fins terroristes*, mars 2014.

Assemblée générale et Conseil de sécurité

Rapports

Rapport du Secrétaire général, *S'unir contre le terrorisme : recommandations pour une stratégie antiterroriste mondiale,* Soixantième session, 27 avril 2006.

Conventions et déclarations

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

Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, Rome, 4 novembre 1950.

Convention Internationale sur l'élimination de toutes les formes de discrimination raciale, adoptée par l'Assemblée générale des Nations unies le 21 décembre 1965, entrée en vigueur le 4 janvier 1969.

Pacte international relatif aux droits civils et politiques, 16 décembre 1966, New-York, Nations Unies.

Convention internationale des droits de l'enfant, adoptée par l'Assemblée générale des Nations unies le 20 novembre 1989, entrée en vigueur le 2 septembre 1990.

Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, adoptée par l'Assemblée générale des Nations unies le 15 novembre 2000, entrée en vigueur le 25 décembre 2003.

Résolutions

Résolution 1566(2004) des Nations Unies, adoptée par le Conseil de sécurité à sa 5053e séance le 8 octobre 2004.

Résolution 1963 (2010) Adoptée par le Conseil de sécurité à sa 6459e séance, le 20 décembre 2010, S/RES/1963 (2010).

Assemblée Générale des Nations Unies, Promotion de la Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus : protection des défenseuses des droits de l'homme/défenseurs des droits des femmes, Résolution adoptée par l'Assemblée générale le 18 décembre 2013, Soixante-huitième session, A/RES/68/181.

Résolution 2178 (2014) Adoptée par le Conseil de sécurité à sa 7272e séance, le 24 septembre 2014, S/RES/2178.

Conseil(s) et Comité(s)

Rapports

Conseil des droits de l'Homme, rapport du Rapporteur spécial sur la promotion et la protection des droits de l'Homme et des libertés fondamentales dans la lutte antiterroriste, Commission des Droits de l'Homme, E/CN.4/2006/98 28 décembre 2005

Conseil des droits de l'Homme, rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression », A/HRC/17/27, 16 mai 2011.

Conseil des droits de l'Homme, rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/67/357 du 7 septembre 2012.

Conseil des droits de l'Homme, rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/29/32, 22 mai 2015.

Conseil des droits de l'Homme, rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Conseil des droits de l'Homme, 11 mai 2016, A/HRC/32/38.

Conseil des droits de l'Homme, rapport de la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences concernant la violence en ligne à l'égard des femmes et des filles du point de vue des droits de l'homme, A/HRC/38/47, 18 juin 2018.

Conseil des droits de l'Homme, rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-treizième session, A/73/348 du 29 août 2018.

Rapporteur spécial des Nations Unies pour la promotion et la protection du droit à la liberté d'expression et rapporteuse spéciale sur la promotion et la protection des droits humains et des libertés fondamentales dans la lutte contre le terrorisme, *Amendment to the Criminal Code on Sharing of Abhorrent Violent Content*, 4 avril 2019.

Conseil des droits de l'Homme, rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Promotion et protection du droit à la liberté d'opinion et d'expression, Assemblée Générale des Nations Unies, Soixante-quatorzième session, A/74/486 du 9 octobre 2019.

Conseil des droits de l'homme, Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, A/HRC/50/55, cinquantième session, 13 mai 2022.

Résolutions

Conseil des droits de l'Homme, Liberté d'opinion et d'expression, résolution 12/16, 12 octobre 2009, A/HRC/RES/12/16.

Conseil des droits de l'Homme, *La promotion, la protection et l'exercice des droits de l'homme sur l'Internet,* 29 juillet 2012, A/HRC/20/L.13.

Conseil des droits de l'Homme, La promotion, la protection et l'exercice des droits de l'homme sur Internet, résolution 32/13, 18 juillet 2016, A/HRC/RES/32/13.

Observations générales et recommandations

Comité des droits de l'Homme, observation générale n° 34 sur l'art. 19 du Pacte international relatif aux droits civils et politiques protégeant la liberté d'opinion et liberté d'expression, CCPR/C/GC/34, 12 septembre 2011.

Comité pour l'élimination de la discrimination à l'égard des femmes, Recommandation générale n° 35 sur la violence à l'égard des femmes fondée sur le genre, portant actualisation de la recommandation générale n° 19, 26 juillet 2017, CEDAW/C/GC/35.

Conseil de l'Europe

Rapports

BENEDEK W., KETTEMANN M. C., *Liberté d'expression et Internet*, Conseil de l'Europe, décembre 2014.

Conseil de l'Europe, *Rapport explicative de la Convention sur la cybercriminalité,* 23 novembre 2001.

Conseil de l'Europe, *Rapport explicatif du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques,* 28 janvier 2003.

Conseil de l'Europe, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains,* 16 mai 2005.

Conseil de l'Europe / Cour européenne des droits de l'Homme, *Internet :la jurisprudence de la Cour européenne des droits de l'Homme*, 2011, mise à jour en juin 2015.

Conseil de l'Europe, *Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet*, février 2017.

Conseil de l'Europe, Comité de la Convention sur la cybercriminalité, *Étude cartographique sur la cyberviolence*, 2018.

Conseil de l'Europe, *Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence*, 11 May 2011, Council of Europe Treaty Series - No. 210.

Conseil de l'Europe, *La Convention de Budapest sur la cybercriminalité : avantages et impact concrets*, T-CY (2020)16, 13 juillet 2020.

Conseil de l'Europe, Modération de contenu, *Meilleures pratiques en vue de la mise en place de cadres juridiques et procéduraux efficaces pour les mécanismes d'autorégulation et de corégulation de la modération de contenu*, Note d'orientation, Adoptée par le Comité directeur sur les médias et la société de l'information (CDMSI), Juin 2021.

Conseil de l'Europe, rapport explicatif du protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE 223, 10 octobre 2018.

Council of Europe, Steering Committee for Media and Information Society (CDMSI), Guidance note, Content Moderation, Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, adopted by the at its 19th plenary meeting, 19-21 May 2021.

Direction générale des droits de l'Homme et des affaires juridiques du Conseil de l'Europe, *Traite des êtres humains : recrutement par internet*, L'usage abusif d'Internet pour le recrutement des victimes de la traite des êtres humains, EG-THB-INT (2007) 1, 2007.

KETTEMANN M. C., *Follow-up to the Comparative Study on Blocking Filtering and Take-down of Illegal Internet Content*, Country Report for Germany 2016-2019, Strassburg, Europarat, mai 2019.

SYKITOU A. P., *Traite des êtres humains : recrutement par internet*, pour la Direction générale des droits de l'Homme et des affaires juridiques du Conseil de l'Europe, 2007.

VAN DER WILK A., *Protecting women and girls from violence in the digital age,* The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, Council of Europe, December 2021.

Résolutions

Résolution 1577 (2007) de l'Assemblée Parlementaire du Conseil de l'Europe, *Vers la dépénalisation de la diffamation,* adoptée par l'Assemblée le 4 octobre 2007, 34e séance.

Résolution 2035 (2015) de l'Assemblée Parlementaire du Conseil de l'Europe, *La protection de la sécurité des journalistes et de la liberté des médias en Europe*, adoptée par l'Assemblée le 29 janvier 2015 (8e séance).

Recommnadations et avis

Avis sur l'article 23 de la Convention de Lanzarote et sa note explicative, adopté par le Comité de Lanzarote le 17 juin 2015.

GREVIO, Recommandation générale n°1 sur la dimension numérique de la violence à l'égard des femmes adoptée le 20 octobre 2021.

Recommandation N° R (99) 5 du Comité des ministres du Conseil de l'Europe sur la protection de la vie privée sur Internet, du 23 février 1999.

Recommandation CM/Rec (2012) 3 du Comité des ministres aux États membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, adoptée le 4 avril 2012, 1139e réunion des délégués des ministers.

Recommandation CM/Rec (2008)6 du Comité des Ministres aux États membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, adoptée par le Comité des Ministres le 26 mars 2008 lors de la 1022e réunion des Délégués des Ministes.

Recommandation CM/Rec (2012) 3 du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, adoptée par le Comité des Ministres le 4 avril 2012, lors de la 1139e réunion des Délégués des Ministres.

Recommandation CM/Rec (2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine adoptée par le Comité des Ministres le 20 mai 2022, lors de la 132e Session du Comité des Ministres.

Déclarations et Conventions

Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n°108, Strasbourg, 28 janvier 1981.

Convention du Conseil de l'Europe sur la cybercriminalité, STCE n° 185, Budapest, 23 novembre 2001.

Comité des ministres du Conseil de l'Europe, Déclaration sur la liberté de la communication sur l'Internet, 28 mai 2003, 840e réunion des Délégués des Ministres du Conseil de l'Europe.

Comité des ministres du Conseil de l'Europe, déclaration sur le droit de l'Homme et l'état de droit dans la société de l'information, CM (2005)56 final, 13 mai 2005.

Convention du Conseil de l'Europe pour la prévention du terrorisme, STCE n° 196, Varsovie, 16 mai 2005.

Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains, STCE n° 197, Varsovie, 16 mai 2005.

Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, STCE n° 201, Lanzarote, 25 octobre 2007.

Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, STCE n° 210, Istanbul, 11 mai 2011.

Déclaration sur les droits de l'homme et l'état de droit dans la société de l'information, adoptée par le Comité des ministres le 13 mai 2005 lors de la 926e réunion des délégués des ministres.

Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, STCE n° 189, Strasbourg, 28 janvier 2003.

Union européenne

Traités et Chartes

Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, 18 décembre 2000.

Traité sur le fonctionnement de l'Union européenne, Journal officiel de l'Union européenne, C 326/47, 26 octobre 2012.

Traité sur l'Union européenne, Journal officiel de l'Union européenne, C 326/13, 26 octobre 2012.

Agences européennes

Agence des droits fondamentaux de l'Union européenne, *La violence à l'égard des femmes : une enquête à l'échelle de l'Union européenne,* 5 mars 2014.

EIGE, *Cyberviolence à l'égard des femmes et des filles*, 23 juin 2017.

European Union Agency for Fundamental Rights, *Fundamental Rights Survey*, 2019.

EIGE, *Combating coercive control and psychological violence against women in the EU Member States*, Publications Office of the European Union, 2022.

Commission européenne

Advisory Committee on Equal Opportunities for Women and Men, *Opinion on combatting online violence against women,* 1st April 2020.

DE VIDO S., SOSA L., *Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence,* Directorate-General for Justice and Consumers, European Commission, 2021.

European Commission, *Security Union: Commission welcomes political agreement on removing terrorist content online*, 10 décembre 2020.

FLETCHER R., The truth behind filter bubbles: Bursting some myths, Reuters Institute, 2020.
Ramboll Management Consulting, *Evaluation of the implementation of the Alliance To Better Protect Minors Online,* Final report, European Commission, 2018.

Parlement européen et Conseil

Règlements

Proposition de règlement du Parlement européen et du Conseil, du 15 décembre 2020, relatif à un marché intérieur des services numériques et modifiant la directive 2000/31/CE (« Digital Services Act »).

Règlement 2015/2120 du Parlement européen et du Conseil, du 25 novembre 2015, établissant des mesures relatives à l'accès à un Internet ouvert et aux prix de détail pour les communications à l'intérieur de l'Union européenne

Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Règlement 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, Journal officiel n° L 012 du 16/01/2001.

Règlement 2021/784 du Parlement Européen et du Conseil, du 29 avril 2021, relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

Directives

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»)

Directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique.

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

Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications et modifiant la directive 2002/58/CE.

Directive 2008/115/CE du Parlement européen et du Conseil, du 16 décembre 2008, relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier.

Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants.

Directive 2012/29/UE du Parlement européen et du Conseil, du 25 octobre 2012, établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil.

Directive 2013/33/UE du Parlement européen et du Conseil du 26 juin 2013 établissant des normes pour l'accueil des personnes demandant la protection internationale.

Directive 2013/40/UE du Parlement européen et du Conseil, du 12 août 2013, relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Directive 2017/541 du Parlement européen et du Conseil, du 15 mars 2017, relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil.

Directive 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant 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 (directive « Services de médias audiovisuels »).

Proposition de directive du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 8 mars 2022, COM (2022) 105 final, 2022/0066 (COD).

Décisions

Décision-cadre du Conseil européen du 13 juin 2002 relative à la lutte contre le terrorisme (2002/475/JAI).

Décision de la Commission européenne du 16 juin 2008 relative à la création d'un comité consultatif de l'égalité des chances entre les femmes et les hommes (2008/590/EC).

Décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal.

Rapports

DE STREEL A., et al., *Online Platforms' Moderation of Illegal Content Online,* Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, 652.718, June 2020.

LOMBA N., NAVARRA C., FERNANDES M., *Combating gender-based violence: Cyber violence European added value assessment,* European Parliamentary Research Service (EPRS), European Parliament, March 2021.

SARTOR G., LOREGGIA A., *The impact of algorithms for online content filtering or moderation,* Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament, September 2020.

VAN DER WILK A., *Cyber violence and hate speech online against women*, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, September 2018.

ZILLER J.*, Liberté d'expression, une perspective de droit comparé,* EPRS Service de recherche du Parlement européen, octobre 2019.

Résolutions

Résolution législative du Parlement européen sur la proposition de décision-cadre du Conseil concernant la lutte contre le racisme et la xénophobie (COM (2001) 664 — C5-0689/2001 — 2001/ 0270(CNS)).

Résolution du Parlement européen du 12 septembre 2017 sur la proposition de décision du Conseil portant conclusion, par l'Union européenne, de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (COM (2016) 0109 – 2016/0062 (NLE)).

Résolution du Parlement européen du 14 décembre 2021 contenant des recommandations à la Commission sur la lutte contre la violence fondée sur le genre : cyberviolence, 2020/2035(INL).

Communications officielles

Communication de la Commission au Parlement européen, au Conseil et au Comité des Régions - Vers une politique générale en matière de lutte contre la cybercriminalité, COM/2007/0267.

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions vers une politique de l'Union européenne en matière pénale : assurer une mise en œuvre efficace des politiques de l'Union européenne au moyen du droit pénal, COM/2011/0573.

Autres organisations régionales et internationales

Commission interaméricaine des droits de l'Homme, Freedom of Expression and the Internet, OEA/Ser.L/V/II. CIDH/RELE/INF, 11/13, 31 December, 2013.

Convention interaméricaine sur la prévention, la sanction et l'élimination de la violence contre les femmes, adoptée par l'Assemblée Générale de l'Organisation des États américains le 6 septembre 1994, entrée en vigueur le 3 mai 1995.

GOTTSCHALK F., Cyberbullying: an overview of research and policy in OECD contries, OECD Education Working Papers N° 270, EDU/WKP(2022)8, 24 March 2022.

International Working Group on Data Protection in Telecommunications, *Report and guidance on privacy in social networks services* - « Rome Memorandum », adopté le 4 mars 2008 à Rome.

LLANSÓ E., VAN HOBOKEN J., LEERSSEN P., HARAMBAM J., *Artificial Intelligence, Content Moderation, and Freedom of Expression,* Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 26 February 2020.

OSCE, Bureau du Représentant pour la liberté des médias, *Freedom of Expression on the Internet, Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating states*, 15 décembre 2011.

OSCE, Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools,* mai 2020.

Organisations non gouvernementales internationales et régionales

Rapports

AJDER H., PATRINI G., CAVALLI F., *Automating image abuse, deepfake bots on telegram*, Sensity, octobre 2020.

Amnesty International, *Let us breathe! Censorship and criminalization of online expression in Viet Nam*, 2020.

AVAAZ, *Megaphone for hate - Disinformation and hate speech on Facebook during Assam's citizenship count*, Octobre 2019.

BOUCHE V., *Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking*, THORN, January 2018.

Center for Democracy and Technology, « Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age," version 0.5 - Discussion draft », avril 2011.

ECPAT and THAILAND INSTITUTE OF JUSTICE, *Global initiative to explore the sexual exploitation of boys*, Thailand report, 2021.

ECPAT et INTERPOL, *Towards a global indicator on unidentified victims in child sexual exploitation material*, 2018.

ECPAT INTERNATIONAL, *Online child sexual exploitation*, 2017.

ECPAT INTERNATIONAL, *Violence against children in cyberspace*, 2005.

Groupe de travail « Article 29 » sur la protection des données, avis 5/2009 sur les réseaux sociaux en ligne, 01189/09/FR, WP 163, 12 juin 2009.

Human Rights Watch, *"Video Unavailable" Social Media Platforms Remove Evidence of War Crimes*, 10 September 2020.

Institut du droit international, « Internet et les atteintes à la vie privée : problèmes de conflit de lois et de juridictions », résolution, 8 RES FR, 31 août 2018.

Interagency Working Group, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, ECPAT International and ECPAT Luxembourg*, Luxembourg, 28 January 2016.

JAYME E., SYMEONIDES S. C. (rapp.), « Internet et les atteintes à la vie privée : problèmes de conflits de loi et juridiction », Institut du droit international, 2019.

OpenNet Initiative, *Asia overview*, rapport en ligne, 2009.

OpenNet Initiative, *Internet Filtering in the Middle East and North Africa,* rapport en ligne, 2009.

PARIS C., *Bodyguard Rewind : retour sur l'année 2020,* 1er janvier 2021.

Pew Research Center, *The State of Online Harassment*, Janvier 2021.

Plan international, *Libres d'être en ligne*, La situation des filles dans le monde, 2020

Communications

Amnesty International, *Ouganda. Les autorités doivent lever le blocage des réseaux sociaux sur fond de répression à la veille des élections*, 13 janvier 2021.

Amnesty International, *Pakistan : les défenseurs des droits humains cible d'une campagne de cyberattaques*, 15 mai 2018.

Amnesty International, *Togo: un militant togolais ciblé par un logiciel espion fabriqué en Inde et lié à un groupe de hackers*, 7 octobre 2021.

Article 19, *CJEU judgment in Facebook Ireland case is threat to online free speech*, 3 October 2019.

Reporters sans frontières, *Énième blocage d'un site Internet d'informations*, Actualité, 20 janvier 2016.

Reporters sans frontières, *L'"oversight board" de Facebook est une solution à très court terme, mais il faut vite passer à autre chose*, 7 juin 2021.

Reporters without borders, *Censorship and surveillance of journalists: an unscrupulous business*, 2017.

Autorités et organisations nationales

Allemagne

Communications

ECHIKSON W., KNODT O., « Germany's NetzDG: A key test for combatting online hate », *CEPS Research Reports*, November 2018, No. 2018/09.

Lois et Codes

Bundesrecht konsolidiert, Strafgesetzbuch (Code pénal féderal).

Loi Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG) du 1er septembre 2017.

Australie

Lois et Codes

Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019.

Espagne

Lois et Codes

Ley Constitucional Contra el Odio, por la Convivencia Pacífica y la Tolerancia, Gaceta Oficial N° 41.274, 9 novembre 2017.

États-Unis

Lois et Codes

Communication Decency Act, 1996.

United States Code

France

Autorités publiques

Rapports et avis

Centre Hubertine Auclert, *Cybersexisme : une étude sociologique dans des établissements scolaires franciliens,* 2016.

Centre Hubertine Auclert, *Cyberviolences conjugales, recherche-action menée auprès de femmes victimes de violences conjugales et des professionnel-le-s les accompagnant,* 2018.

CNCDH, Recommandation n°14, *Avis sur la lutte contre les discours de haine en ligne*, 12 février 2015.

CNIL, Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

CNIL, Droit au déréférencement, Les critères communs utilisés pour l'examen des plaintes, 2014.

CNIL, Droit au déréférencement, Les critères communs utilisés pour l'examen des plaintes, 2014.

CNIL, *Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*, Rapport d'activité 2013.

Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, *Numérique et libertés : un nouvel âge démocratique*, Rapp. N°3119 du 8 octobre 2015, recommandation n°76.

Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, *Numérique et libertés : un nouvel âge démocratique*, Rapp. N°3119 du 8 octobre 2015, recommandation n°76.

Conseil d'État, Avis sur la proposition de loi visant à lutter contre les contenus haineux sur Internet, 16 mai 2019.

Conseil d'État, Droit à l'oubli : le Conseil d'État donne le mode d'emploi, 6 décembre 2019.

Conseil d'État, Proposition n°28, *Le numérique et les droits fondamentaux*, Le rapports du Conseil d'État (ancienne collection Étude et documents du Conseil d'État), 9 septembre 2014.

Création d'un pôle national dédié à la lutte contre la haine en ligne au tribunal judiciaire de Paris, Lexis Veille, 30 novembre 2020.

CSA, Questionnaire aux opérateurs de plateformes en ligne soumis au titre III de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. Bilan des mesures de lutte contre la manipulation de l'information sur les plateformes en ligne mises en œuvre en 2020, 2021.

HARFOUSH R., *QAnon, la culture numérique et les élections françaises,* CNAMM, juin 2021.

Haut Conseil à l'Égalité entre les femmes et les hommes, *En finir avec l'impunité des violences faites aux femmes en ligne, : une urgence pour les victimes*, 2017.

IMBERT-QUARETTA M., *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne*, Rapport à Madame la ministre de la culture et de la communication, mai 2014.

Ministère de la justice, Lutte contre la haine en ligne, Un an au service de la justice, 28 juin 2021.

ROBERT M. (dir.), *Protéger les internautes, rapport sur la cybercriminalité, rapp. aux ministres de l'intérieur et de l'Economie, à la garde de Sceau et à la secrétaire d'État chargée du numérique,* juin 2014.

Lois et Codes

Code de l'éducation.

Code des postes et des communications électroniques.

Code pénal français.

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

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

Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes.

Loi 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet.

Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

Décrets

Décret n° 2007-1538 du 26 octobre 2007 relatif aux demandes de mise à disposition de données par voie électronique et modifiant le code de procédure pénale qui prévoit une obligation de communication de données pour certains organismes publics et privés.

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.

Décret n° 2014-1162 du 9 octobre 2014 portant création d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires ».

Décret d'application de la loi du 24 juillet 2015 relative au renseignement.

Société civile

BOUZAR D., CAUPENNE C., VALSAN S., *La métamorphose opérée chez le jeune par les nouveaux discours terroristes*, Centre de prévention des dérives sectaires liées à l'islam, novembre 2014.

Fondation Scelles, *Système prostitutionnel*, Nouveaux défis, nouvelles réponses, 5e rapport mondial, 2019.

Génération numérique, *Les pratiques numériques des jeunes de 11 à 18 ans*, enquête 2021.

HECKER M., *Web social et dijihadisme*, IFRI, Focus stratégique n° 57, juin 2015.

Point de contact, *Rapport annuel 2019*, 2020.

Italie

Communications des autorités publiques

Garante della privacy, *Provvedimento* n° 144 du 24 mars 2016.

Garante per la protezione dei dati personali, *Deep fake: il Garante privacy apre un'istruttoria nei confronti di Telegram per il software che "spoglia" le donne*, 2020.

Lois et Codes

Code pénal

Legge n°39, « Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2001 », 1er mars 2002 publié à la Gazzetta Ufficiale n. 72 du 26 mars 2002.

Legge n° 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, del 29 maggio 2017(17G00085), GU Serie Generale n.127 del 03-06-2017.

Legge n.69, *Tutela delle vittime di violenza domestica e di genere*, 19 luglio 2019 (GU 25.07.2019).

Legge n. 70 del 25 giugno 2020 di conversione del D.L. n. 28/2020, *Misure urgenti in materia di intercettazioni, di ordinamento penitenziario, di giustizia civile, penale, amministrativa e contabile e per l'introduzione del sistema di allerta Covid-19.*

Roumanie

Lois et Codes

Loi n°106 portant modification et complément de la loi n° 217/2003 sur la prévention et la lutte contre la violence domestique.

Royaume-Uni

Lois et Codes

Cambridge Consultants, *Use of AI in online content*, Report produced on behalf of Ofcom, 2019.

Sexual Offences Act, 2003.

Acteurs privés

Advisory Council to Google on the Right to be Forgotten, *Advisory report*, 6 février 2015.

AIDER H., PATRINI G., CAVALLI F., CULLEN L., *The State of Deepfakes: Landscape, Threats, and Impact*, Deeptrace, September 2019.

Conseil de surveillance, décision sur le cas 2021-001-FB-FBR, FB-691QAMHJ, 5 mai 2021.

Conseil de surveillance, Introduction, *Oversight Board Bylaws*, janvier 2022.

Conseil de surveillance, *Oversight Board publishes transparency report for first quarter of 2022*, août 2022.

Conseil de surveillance, *To treat users fairly, Facebook must commit to transparency*, Septembre 2021.

FERRARO M. F., *Deepfake Legislation: A Nationwide Survey—State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media*, WilmerHale, 2019.

TOBIN A., VARNER M., ANGWIN J., Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up, 28 décembre 2017.

Twitter, Permanent suspension of @realDonaldTrump, 8 janvier 2021.

PRESSE

ALLYN B., *Former TikTok moderators sue over emotional toll of 'extremely disturbing' videos*, NPR, 24 mars 2022.

ANTONIUK D., *Ukrainian content moderators among Facebook's lowest paid workers,* The Kyiv post, 25 octobre 2021.

Attentat de Halle en Allemagne : La diffusion en ligne de la vidéo de l'attaque montre la difficulté à stopper les « live », 20 Minutes avec l'AFP, 10 octobre 2019.

BADOUARD R., *Shadow ban. L'invisibilisation des contenus en ligne,* Revue Esprit, novembre 2021.

BERTRAND C., « Tout comprendre au débat sur l'anonymat sur Internet », *Les Echos*, 20 juillet 2020.

BRAUN E., *La viralité d'une fausse vidéo d'Obama met en lumière le phénomène du «deep fake»*, Le Figaro, 20 avril 2018.

BROSSELIN L., *TikTok et l'ONU Femmes lancent un forum de discussion et de sensibilisation sur le cybersexisme*, L'ADN, 17 décembre 2021.

CHAHUNEAU L., *Grossophobie : la Une de Télérama censurée par Facebook et Instagram, les internautes contre-attaquent,* Le Parisien, 7 février 2020.

Courrier international, *Génocide des Rohingyas : le mea culpa de Facebook*, 7 novembre 2018.

CROSSLAND D., *German plan for age filters across web to stop under-18s accessing pornography,* The Times, 22 juillet 2021.

CUSHING E., *How Facebook fails 90 percent of its users,* The Atlantic, 25 octobre 2021.

D'ANASTASIO C., *Children Stream on Twitch—Where Potential Predators Find Them*, WIRED, 2020.

DAGRY M-A., *Vivastreet : une information judiciaire ouverte pour « proxénétisme aggravé »*, AFP agence, 31 mai 2018.

DENHAM H., *These are the platforms that have banned Trump and his allies,* The Washington Post, janvier 2021.

DEVILLIER N., « Pourquoi vos données survivront à la suppression de votre compte Facebook et quels en sont les risques ? », *The Conversation*, 28 mars 2018.

FONTANA S., *Dentro il più grande network italiano di revenge porn, su Telegram*, Wired Italia, 3 avril 2020.

FRANCESCHI-BICCHIERAI L., *Anonymous Hackers Officially Dox Hundreds of Alleged KKK Members*, VICE, 6 novembre 2015.

FRANKS M. A., *How to defeat 'revenge porn': First, recognize it's about privacy, not revenge*, Huffington Post, 22 juin 2015.

GILBERT D., *Les conditions de travail infernales des modérateurs de Facebook,* Vice, 21 janvier 2020.

GRABER J., VELEZ G., *How it Started*, Bluesky blog, 28 février 2022.

GRAND H., *«Deepfake »: une vidéo trafiquée de Nancy Pelosi relayée par des proches de Trump*, Le Figaro, 24 mai 2019.

HT CORRESPONDENT, *You can now deepfake Elon Musk and others in your Zoom meetings*, 18 avril 2020.

HUVELIN G., *Amnesty International dénonce une campagne de phishing sophistiquée visant des défenseurs des droits de l'homme égyptiens*, Numerama, 12 mars 2019.

JACOBY K., *Facebook fed posts with violence and nudity to people with low digital literacy*, USA Today, 23 novembre 2021.

KESVANI H., « Abolishing online anonymity won't tackle the underlying problems of racist abuse », *The Guardian*, 15 juin 2021.

KHOUIEL L., *Quand le revenge porn s'adapte au confinement*, VICE, 8 avril 2020.

LA FRANCE A., *History will not judge us Kindly*, The Atlantic, 25 octobre 2021.

LAUSSON J., *QAnon est désormais systématiquement banni de Facebook, qu'importe ce qui est publié,* Numerama, 7 octobre 2020.

Le Monde, *« Swatting » : vingt ans de prison pour un canular téléphonique ayant mené à la mort d'un homm*e, 1er avril 2019.

LELOUP D., PIQUARD A., « *Facebook ne place pas les profits avant les gens »*, Le Monde, 11 octobre 2021.

LONGO A., *Filtro automatico al porno su Internet, ecco la norma firmata Lega*, La Repubblica, 19 juin 2020.

LYNCH S. N., LAMBERT L., *Sex ads website Backpage shut down by U.S. authorities,* Reuters, 6 avril 2018.

M.C avec l'AFP, « Facebook s'excuse après avoir censuré les seins nus de « La Liberté guidant le peuple » », *20 Minutes,* 19 mars 2018.

NEWTON C., *Half of all Facebook moderators may develop mental health issues,* The Verge, 13 mai 2020.
NEWTON C., *The terror queue*, The Verge, 16 décembre 2019.

PERRIGO B., *Facebook Content Moderators in Kenya to Receive Pay Rise Following TIME Investigation*, Time, 2 mars 2022.

PINNELL O., KELLY J., *Slave markets found on Instagram and other apps*, BBC News Arabic, 31 octobre 2019.

PIQUARD A., *Facebook hors des États-Unis : les failles d'une tour de Babel,* Le Monde, 26 octobre 2021.

PIQUARD A., REYNAUD F., *Des pro-anorexie aux pro-QAnon : Facebook face aux effets de ses recommandations automatiques,* Le Monde, 27 octobre 2021.

RAHMIL D-J., *« Il y a eu un loupé » : pourquoi vous n'auriez jamais dû voir la vidéo de l'attentat de Buffalo*, L'ADN, 16 mai 2022.

ROTH E., *Facebook content moderators protest low wages with mobile billboard*, The Verge, 19 octobre 2021.

SINGH J., CBI *Reportedly Asks Social Media Firms to Use Intrusive PhotoDNA Technology to Track Suspects*, 1 janvier 2019.

SMITH A., « Calls to end social media anonymat give plate-forme more power without actually fixing the problem, experts say », *Indipendent*, 14 juin 2021.

Suède : un homme condamné pour des viols d'enfants à distance, via internet, Le Parisien, 1er décembre 2017.

The Globe and mail, *Cambridge Analytica, AggregateIQ and the Facebook scandal: A guide to who's accused of what*, 5 avril 2018.

The Washington Post, *Transcript of Mark Zuckerberg's Senate hearing*, 11 avril 2018.

Twitter supprime 70 000 comptes liés à la mouvance conspirationniste pro-Trump QAnon, France Info, 12 janvier 2021.

UNTERSINGER M., LELOUP D., « Hollande et le PS s'en prennent de nouveau à « l'anonymat sur Internet » », *Le Monde*, 17 décembre 2013.

UNTERSINGER M., LELOUP D., *Pour modérer 220 millions d'utilisateurs en langue arabe, Facebook n'emploie que 766 modérateurs,* Le Monde, publié le 16 novembre 2021.

UNTERSINGER M., *Modérationdu Web : la justice européenne favorable au filtrage automatique des messages déjà jugés haineux*, *Le Monde*, 3 octobre 2019.

UNTERSINGER M., TUAL M., « Après avoir censuré une photo de la guerre du Vietnam, Facebook fait machine arrière », *Le Monde*, 9 septembre 2016.

USA : Zuckerberg défend la neutralité de Facebook, Le Figaro, 13 mai 2016.

WATERSON J., HERN A., *UK age-verification system for porn delayed by six monthS*, The Guardian, 20 juin 2019.

WATERSON J., *UK drops plans for online pornography age verification system*, The Guardian, 16 octobre 2019.

WHEELER A., *« TikTok we need to talk » : Lizzo slams social media app for body shaming*, The Guardian, 5 mars 2020.

WONG J. C., « Facebook Blocks Pulitzer-Winning Reporter over Malta Government Exposé », *The Guardian*, 19 mai 2017.

ZHONG R., KROLIK A., MOZUR P., BERGMAN R., *Behind China's Twitter Campaign, a Murky Supporting Chorus*, The New York Times, 8 juin 2020.

ZURLONI L., *Uscite le minorenni*, Wired Italia, 23 janvier 2019.

JURISPRUDENCES

Cour européenne des droits de l'Homme

Cour EDH, *Botta c. Italie* du 24 février 1998, 21439/93.

Cour EDH, GC, *Animal Defenders International c. Royaume-Uni*, 22 avril 2012, req n° 48876/08.

Cour EDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, req. n° 5493/72.

Cour EDH, *Klass et autres c. Allemagne* du 6 septembre 1978, req. n° 5029/71.

Cour EDH, *Malone c. Royaume Uni* du 2 août 1984, req. n° 8691/79.

Cour EDH, 8 juillet 1986, *Lingers c. Autriche*, req n° 9815/82.

Cour EDH, 25 mars 1993, *Costello-Roberts c. Royaume-Uni*, req n° 13134/87.

Cour EDH, GC, 23 septembre 1994, *Jersild c. Danemark*, req. n° 15890/89.

Cour EDH, 27 mars 1996, *Goodwin c. Royaume-Uni*, req. n° 17488/90.

Cour EDH, 22 octobre 1996, *Stubbing et autres c. Royaume-Uni*, req. n° 22083/93 et 22095/93.

Cour EDH, 23 septembre 1998, *Lehideux et Isorni c. France*, req. n° 24662/94.

Cour EDH, GC, 8 juillet 1999, *Sürek c. Turquie*, req n° 26682/95.

Cour EDH, 28 mars 2000, *Kilic c. Turquie*, req. n° 22492/93.

Cour EDH, 10 mai 2001, *Z et autre c. Royaume Uni*, req. n° 29392/95.

Cour EDH, GC, 12 décembre 2001, B*ankovi*ć *et autres c. Belgique et autres*, req. n° 52207/99.

Cour EDH, 29 avril 2002, *Pretty c. Royaume Uni*, req. 2346/02.

Cour EDH, 14 mai 2002, *Gentilhomme et autres c. France*, requêtes nos 48205/99, 48207/99 et 48209/99.

Cour EDH, 24 juin 2003, *Garaudy c. France*, req n° 65831/01.

Cour EDH, 10 juillet 2003, *Murphy c. Irlande*, req ° 44179/98.

Cour EDH, 4 décembre 2003, *Gündüz c. Turquie*, req. n° 35071/97.

Cour EDH, 4 décembre 2003, *M.C. c. Bulgarie*, req. n° 39272/98.

Cour EDH, 9 mars 2004, *Glass c. Royaume-Uni*, n^{o} 61827/00.

Cour EDH, 8 juillet 2004, *Ilaşcu et autres*, req. n° 48787/99.

Cour EDH, 18 octobre 2005, *Perrin c. Royaume- Uni*, req. n° 5446/03.

Cour EDH, 1er décembre 2005, *Vérités Santé Pratique Sarl c France*, req. n° 74766/01.

Cour EDH, 11 avril 2006, *Brasilier c. France*, req n° 71343/01.

Cour EDH, *Weber et Saravia* du 29 juin 2006, req. n° 54934/00.

Cour EDH, 10 juillet 2006, *Sdružení Jihočeské Matky c. la République tchèque*, req. n° 19101/03.

Cour EDH, 7 novembre 2006, *Mamere c. France*, req. n° 12697/03.

Cour EDH, 6 octobre 2006, *Erbakan c. Turquie*, req. n° 59405/00.

Cour EDH, 14 décembre 2006, *Verlagsgruppe News GmbH v. Austria* (no. 2), req. n°10520/02.

Cour EDH, 3 juillet 2007, *Copland c. Royaume Uni*, n°62617/00.

Cour EDH, 13 novembre 2007, *Muscio c. Italie*, req. n° 31358/03.

Cour EDH, 10 décembre 2007, *Stoll c. Suisse*, req. n° 69698/01.

Cour EDH, 2 décembre 2008, *K.U c. Finlande*, req. n° 2872/02.

Cour EDH, 11 décembre 2008, *TV Vest AS & Rogaland Pensjonistparti c. Norvège*, req° n° 21132/05.

Cour EDH, 10 mars 2009, *Times Newspaper c. Royaume-Un*i, req. n° 3002/03 et n° 23676/03.

Cour EDH, 14 avril 2009, *Társaság a Szabadságjogokért c. Hongrie*, req. n° 37374/05.

Cour EDH, 16 juillet 2009, *Féret c. Belgique*, req. n° 15615/07.

Cour EDH, 16 juillet 2009, *Willem c. France*, req. n° 10883/05.

Cour EDH, 9 septembre 2009, *Opuz c. Turquie*, req. n° 33401/02.

Cour EDH (2e sect.), 20 octobre 2009, *Ürper et autres c. Turquie*, req n° 14526/07.

Cour EDH, 22 octobre 2009, *Europapress Holding D.O.O c. Croatie*, req. n°25333/06.

Cour EDH, 25 février 2010, *Renaud c. France*, req. n° 13290/07.

Cour EDH, 22 avril 2010, *Fatullayev c. Azerbadjian*, req n° 40984/07.

Cour EDH, 20 juillet 2010, *Dadouch c. Malte*, req. 38816/07.

Cour EDH, 16 décembre 2010, *A.B.C. c: Irlande*, req. 25579/05.

Cour EDH, 10 février 2011, *Premininy c. Russie*, req. n° 44973/04.

Cour EDH, 5 mai 2011, *Comité de rédaction Pravoye Delo et Shtekel c. Ukraine*, req. n°33014/05.

Cour EDH, 5 mai 2011, *Pravoye Delo*, req n°33014/05.

Cour EDH, 10 mai 2011, *Mosley c. Royaume-Uni*, req n° 48009/08.

Cour EDH, GC, 7 juillet 2011, *Al-Skeini et autres* c. Royaume Uni, n° 55721/07.

Cour EDH, 7 février 2012, *Von Hannover c. Allemagne* n° 2, req. n° 40660/08 60641/08.

Cour EDH, GC, 7 février 2012, *Axel Springer AG c. Allemagne*, req. n° 39954/08.

Cour EDH, GC, *Mouvement raëlien suisse c. Suisse*, 13 juillet 2012, req. n° 16354/06.

Cour EDH, 24 juillet 2012, *B.S c. Espagne*, req n° 47159/08.

Cour EDH, 19 octobre 2012, *Catan et autres c. République de Moldova et Russie*, req. nos 43370/04, 8252/05 et 18454/06.

Cour EDH, GC, 12 novembre 2012, *Söderman c. Suède*, req n° 5786/08.

Cour EDH (2e sect.), 18 décembre 2012, *Ahmet Yildirim c. Turquie*, req n° 3111/10.

Cour EDH, 13 mars 2013, *Eon c. France*, req. n° 26118/10.

Cour EDH, 9 juillet 2013, *Vona c. Hongrie*, aff. 35943/10.

Cour EDH, 24 septembre 2013, *Belpietro c. Italie*, req. n° 43612/10.

Cour EDH, 16 octobre 2013, *Węgrzynowski et Smolczewski c. Pologne*, req. n° 33846/07.

Cour EDH (2e sect.), 19 décembre 2013, *Perinçek c. Suisse*, req. n° 27510/08.

Cour EDH, 16 janvier 2014, *Tierbefreier E.V. c. Allemagne*, req. n° 45192/09.

Cour EDH, 11 mars 2014, *Akdeniz c. Turquie*, requêtes n° 41139/15 et n° 41146/15.

Cour EDH, 3 juin 2014, *Schuman c. Pologne*, req n°52517/13.

Cour EDH, 8 juillet 2014, *Nedim Şener c. Turquie*, req. no 38270/11.

Cour EDH (GC), 16 juin 2015, *Delfi AS c. Estonie*, req. n° 64669/09.

Cour EDH, 23 juin 2015, *Niskasaari et Otavamedia Oy c. Finlande*, req. n°32297/10.

Cour EDH, GC, 10 novembre 2015, *Couderc et Hachette Filipacchi Associés c. France*, req. n° 40454/07.

Cour EDH, 1 décembre 2015, *Cengiz et autres c. Turquie*, req n° 48226/10 et 14027/11.

Cour EDH, 19 janvier 2016, *Kalda c. Estonie*, req. N° 17429/10.

Cour EDH, GC, 29 mars 2016, *Bédat v. Switzerland*, req, n°56925/08.

Cour EDH, 30 août 2016, *Medipress-Sociedade Jornalistica Lda c. Portugal*, req n° 55442/12.

Cour EDH, GC, 8 novembre 2016, *Magyar Helsinki Bizottsàg c. Hongrie*, req. n° 18030/11.

Cour EDH, 17 janvier 2017, *Jankovskis c. Lituanie*, req n° 21575/08.

Cour EDH, 27 juin 2017, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, req. n° 931/13.

Cour EDH, 19 septembre 2017, *Tamiz c.Royaume Uni*, req. n° 3877/14.

Cour EDH, 19 octobre 2017, *Fuchsmann c. Allemagne*, req. n° 71233/13.

Cour EDH, 19 mars 2019, *Høiness c. Norvège*, req. n° 43624/14.

Cour EDH, 11 février 2020, *Buturuga c. Roumanie*, req. n° 56867/15.

Cour EDH, 26 mars 2020, *Centre for democracy and the rule of law c. Ukraine*, req n° 100090/16.

Cour EDH, 5 mai 2020, arrêt *Kövesi c. Romania*, req n° 3594/19.

Cour EDH, 12 mai 2020, *Lilliendahl c. Islande*, req. n° 29297/18.

Cour EDH, 23 juin 2020, *Vladimir Kaharitonov c. Russie*, n° 10795/14.

Cour EDH, 23 juin 2020, *Bulgakov c. Russia*, req. n° 20159/15.

Cour EDH, 23 juin 2020, *Engels c. Russia*, 23 juin 2020, req. n° 61919/16.

Cour EDH, 23 juin 2020, *OOO Flavius and others c. Russia*, req. n° 12468/15, 23489/15 et 19074/16.

Cour EDH, 23 juin 2020, *Vladimir Kharitonov c. Russia*, req. n° 10795/14.

Cour EDH, 9 février 2021, *Ramazan Demir c. Turquie*, req n° 68550/17.

Cour EDH, 2 septembre 2021, *Sanchez c. France*, req. n° 45581/15.

Cour EDH, GC, 15 mai 2023, *Sanchez c. France*, req. n° 45581/15.

Cour EDH, 7 septembre 2021, *Camak c. Turquie*, req. n° 45016/18.

Cour EDH, *Volodina c. Russie* du 14 décembre 2021, req. n° 40419/19.

Cour de justice de l'Union européenne

CJUE, 7 mars 1995, *Fiona Shevill c. Presse Alliance SA*, C-68/93.

CJUE, 6 mars 2001, *Connolly*, aff. C-274/99.

CJUE, 10 mars 2009, *Heinrich*, C-345/06.

CJUE, GC, 23 mars 2010, *Sté Google c. Sté Louis Vuitton Malletier*, affaires C-236/08 à C-238/08.

CJUE, 7 décembre 2010, *Peter Pammer c. Reederei Karl Schlüter GmbH & Co. KG et Hotel Alpenhof GesmbH c. Oliver Heller*, affaires jointes C-585/08 et C-144/09.

CJUE, 29 mars 2011, *Arcelor Mittal Luxembourg c. Commission* et *Commission c. Arcelor Mittal Luxembourg e.a.*, C-201/09 P et C-216/09.

CJUE, 22 septembre 2011, *Mesopotomia Broadcast A/S METV, Roj TV/ AS c. BundesrepublikDeutschland*, aff. jointes C-244/10 et C-245/10.

CJUE, GC, 25 octobre 2011, *eDate Advertising Gmbh c. X*, affaires jointes C-509/09 et C-161/10.

CJUE (3eme chambre), *Scarlet c. Sabam*, 24 novembre 2011, C-70/ 10.

CJUE (3eme chambre), *Samab c. Netlog*, 16 février 2012, C-360/10.

CJUE (4eme chambre), 27 mars 2014, *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH et Wega Filmproduktionsgesellschaft mbH*, C-314/12.

CJUE, GC, 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a*, affaires jointes C-293/12 et C-594/12.

CJUE, GC, 13 mai 2014, *Google Spain et Google Inc c. AEPD*, aff. C 131/12.

CJUE, 21 décembre 2016, *Tele2 Sverige c. Post- och telestyrelsen*, aff. C-203/15.

CJUE, GC, 24 septembre 2019, *Google LLC c. CNIL*, aff. C-507/17.

CJUE, GC, *Google LLC c/ CNIL* du 24 septembre 2019, aff. C-507/17.

CJUE, 3 octobre 2019, *Glawischnig-Piesczek c. Facebook Ireland*, aff. C-18/18.

CJUE, 1re chambre, 17 juin 2021, *Mittelbayerischer Verlag KG c. SM*, aff. C-800/19.

Juridictions nationales

Australie

Federal Court of Australia, 17 septembre 2002, *Jones v. Toben*, FCA 1150.

Allemagne

OLG München, 17.07.2018 - 18 W 858/18.

OLG Dresden du 8 août 2018.

OLG München du 28 août 2018.

LG Frankfurt/Main, 10.09.2018 - 2–03 O 310/18 2018.

Belgique

Corr. Leuven, 8 novembre 2010, *A.M.*, 2011.

Canada

Human Rights Tribunal, *Enst Zundel v. The Queen*, 2002, **n° 953/2000**.

États-Unis

Cour d'appel américaine du 6ème circuit, *Signature Management Team, LLC v. Doe*, No. 16-2188 (6th Cir. 2017).

Cour Suprême de l'État de Virginie, *AOL c./Nam tai Electronics du* 1er novembre 2002.

Cour suprême des États-Unis, 19 avril 1995, *McIntyre v. Ohio Elections Commission*, 514 U.S. 334.

Cour Suprême des États-Unis, *Reno v. American Civil Liberties Union*, 521 U.S. 844, 1997.

Cour Suprême, 9 juin 1969, *Clarence Brandenburg v. State of Ohio*, n°492.

Ohio Supreme Court, *Talley v. California, McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

Superior court of the State of California, *Selena Scola v. Facebook*, Case No. 18-civ-05135.

United States court of appeals for the sixth circuit, *Watchtower Bible & Tract Soc'y of New York, Inc. v. Vill. Of Stratton*, 536 U.S. 150 (2002).

United States District Court, N.D. Georgia, Atlanta Division, *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010).

United States District Court, Northern District of California, *Reece Young and Ashley Velez v. ByteDance Inc. And TikTok Inc.*, 24 mars 2022, case n° 3:22-cv-01883.

France

Cass. civ. 1ère, 19 février 1975.

Tribunal de grande instance de Paris, 5 juillet 1995.

Tribunal de grande instance de Paris, 22 mai 2000.

Civ. 1re, 9 déc. 2003, D. 2004. 276.

Cour d'appel de Paris, 6 juin 2007, n° 06/14890.

Cass. Com., 9 mars 2010, n° 08-16.752.

Cass. Com., 13 juillet 2010, n°06-20.230.

Cass. Com., 23 novembre 2010, n° 07-19.543.

Cass. Com., 20 septembre 2011, n° 10-16.569.

Crim. 16 mars 2016, n° 15-82.676.

Tribunal de grande instance de Montpellier, 15 novembre 2016.

Tribunal de grande instance de Paris, ordonnance de référé, *Lafuma Mobilier c. Alibaba a.*, 21 novembre 2017.

Tribunal de grande instance de Bobigny, Chambre 5 sec 3, 20 novembre 2018.

Tribunal de grande instance de Paris, 25 sept. 2019, n° 18/00402.

Conseil constitutionnel, décision n° 2020-801 DC du 18 juin 2020.

Cass. Com., 3 mai 2021, n° 11-10.505, n° 11-10.507 et n° 11-10.508.

TJ Paris, 6 juill. 2021, n° 20/53181.

Cour d'Appel de Versailles, 28 sept. 2021, n° 634.

CA Paris, 20 janv. 2022, n° 21/14325.

Cass. 1re civ., 11 mai 2022, n° 21-16.497.

Cour d'Appel de Limoges, Ch. corr., arrêt du 20 mai 2022.

Cass., 23 mars 2023, n° 22-13.600.

Italie

Corte di cassazione, Sez. 3, n. 19033 del 26/03/2013, L, Rv. 255295 – 01.

Corte di Cassazione, sez. *I*, 20/3/2018 n. 6919.

Corte di cassazione, Sez. 3, n. 17509 del 30/10/2018, dep. 2019, D., Rv. 275595 – 01.

Corte di cassazione, terza sezione penale, del 2 luglio 2020, Rv. 25266-20.

Suède

Rättelse/komplettering Dom, 2017-11-30. Uppsala Tingsrätt (District Court of Uppsala).

Index thématique

V

Table des matières

Résumé : L'encadrement juridique européen et international des cyberviolences

Les violences en ligne ne sont pas un phénomène nouveau, elles existent depuis la création d'Internet. En perpétuelle évolution, elles prennent différentes formes et touchent les utilisateurs du monde entier. Les caractéristiques d'Internet confèrent à ces comportements illicites des spécificités qui ont un impact sur leur qualification et sur leur régime.
Si progressivement des réglementations juridiques ont été adoptées au niveau national et européen pour les encadrer, il n'existe pas encore une définition claire de cyberviolence et des règles uniformes reconnues par la communauté internationale pour protéger les droits fondamentaux des utilisateurs. De plus, le cadre préventif et répressif demeure insatisfaisant. Cela conduit à des conséquences négatives, notamment en termes d'évaluation du phénomène et d'adoption de mesures appropriées, ainsi que des manquements en matière de protection des destinataires des services.

Descripteurs : droit international ; droit européen ; droit comparé ; droits fondamentaux ; cyberviolences ; Internet ; cyberespace ; prévention ; sanction ; nouvelles technologies.

Title and Abstract: The European and international legal framework for cyber-violence

Online violence is not a new phenomenon, it has existed since the creation of the Internet. It is constantly evolving, taking different forms and affecting users all over the world. The characteristics of the Internet give to these illicit behaviors special characteristics that have an impact on their qualification and on their regime. Although legal provisions have gradually been adopted both at national and European levels to regulate them, there is still no clear definition of cyber-violence and no uniform rules recognized by the international community to protect the fundamental rights of users. Moreover, the preventive and repressive framework remains unsatisfactory. This leads to negative consequences, particularly in terms of evaluating the phenomenon and adopting appropriate measures, as well as a lack of protection for the recipients of the service.

Keywords: International law; European law; comparative law; fundamental rights; cyber-violence; Internet; cyberspace; prevention; sanction; new technologies.