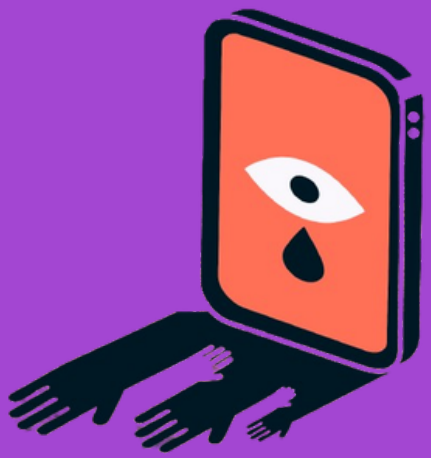
Université Paris Nanterre

EUCLID
Enseignement universitaire
clinique du droit
Université Paris Nanterre

APERÇU : LES CADRES JURIDIQUES FRANÇAIS ET EUROPÉENS RELATIFS AUX CYBERVIOLENCES FAITES AUX FEMMES ET AUX FILLES

Clinique juridique de l'Université Paris Nanterre (EUCLID)

Université Paris Nanterre en collaboration avec Osez le Féminisme (OLF) & la Coordination Française pour le Lobby Européen des Femmes (CLEF)



Auteures
Apolline Anastase,
Christine Cymovonuyk,
Louise Moreau Louapre,
Luna Zedjaoui

Sous la supervision de
Professeure Audrey Darsonville

Avec le soutien de
Alyssa Ahrabare, présidente de la Coordination Française pour le Lobby Européen des Femmes (CLEF) et responsable de plaidoyer d'Osez le Féminisme (OLF)

OSEZ LE FÉMINISME

La Coordination Française pour le Lobby Européen des Femmes

SOMMAIRE

Page 1
Remerciements

Page 2
Méthodologie

Page 6
Introduction

Page 12
Développement

Page 56
Recommandations pour la transposition de la directive 2024/1385

Page 64
Table des matières

Page 65
Bibliographie

Remerciements

Nous remercions chaleureusement Madame Alyssa Ahrabare pour son engagement et son accompagnement dans ce projet mené en collaboration avec Osez Le Féminisme et la Coordination française pour le Lobby Européen des Femmes. Nous sommes reconnaissantes pour les nombreuses opportunités offertes dans le cadre de ce partenariat. Nous avons été particulièrement ravies d'avoir pu assister au colloque organisé à Strasbourg, qui nous a permis de prendre contact avec plusieurs personnes pour des entretiens. Nous remercions également Madame Ahrabare pour les ressources précieuses qu'elle nous a transmises, ses relectures, apports de contenu et d'analyse, ainsi que pour ses conseils et son soutien tout au long de nos recherches.

Nous tenons aussi à exprimer notre profonde gratitude à Madame La Professeure Audrey Darsonville pour son encadrement, sa disponibilité, sa relecture attentive et ses conseils. Sa confiance, ses encouragements et son accompagnement ont été essentiels à l'aboutissement de ce mémoire.

Enfin, nous remercions également Mesdames Cécile Mantel, Julie Caillet, Katty Jorge Maia, Céline Piques, Mariana Branco, Ruth Breslin, Mié Kohiyama et Alejandra Mariscal López pour leur disponibilité, leur engagement et la qualité des entretiens qu'elles nous ont accordés.

Méthodologie

Ce travail, réalisé dans le cadre de la Clinique juridique de l'Université Paris Nanterre répond à une commande formulée par les associations Osez le Féminisme et la Coordination française pour le Lobby Européen des Femmes. Créée en 2009, cette organisation se revendique à la fois féministe, universaliste, laïque, progressiste et abolitionniste. Elle a pour objectif principal la dénonciation et l'éradication des inégalités entre les femmes et les hommes.

Aujourd'hui, l'association regroupe 15 antennes en France. Depuis le 9 janvier 2013, elle est membre du Haut Conseil à l'Egalité entre les femmes et les hommes, et siège également au bureau de la Coordination Française pour le Lobby Européen des Femmes (CLEF).

La CLEF est une organisation non gouvernementale, regroupant une quarantaine d'associations françaises œuvrant pour les droits des femmes. Elle est membre du Lobby Européen des Femmes, réseau de 2000 organisations féministes, première force de défense des droits des femmes à l'échelle européenne. La CLEF porte un plaidoyer auprès des institutions françaises, européennes et internationales, grâce à son statut consultatif auprès de l'Organisation des Nations Unies (ECOSOC).

Osez le Féminisme et la Coordination française pour le Lobby Européen des Femmes portent un plaidoyer commun sur la lutte contre les cyberviolences sexistes et sexuelles et l'exploitation sexuelle en ligne. Ces sujets, qui comportent de manière inhérente une dimension transfrontalière, doivent rencontrer une réponse non seulement nationale, mais également européenne.

C'est dans ce contexte que les associations ont sollicité notre équipe pour la réalisation d'une étude juridique fondée sur la Directive (UE) 2024/1385 relative à la lutte contre la violence à l'égard des femmes et la violence domestique. L'analyse s'est concentrée sur les quatre infractions visant les cyberviolences sexistes et sexuelles (cyberVSS) définies par ledit texte : le partage non consenti de matériels intimes, la traque furtive en ligne, le cyberharcèlement et l'incitation à la violence ou à la haine en ligne. L'objectif initial était double ; d'une part, croiser les dispositions de la Directive relatives aux cyberVSS avec d'autres instruments européens visant la régulation des contenus numériques, afin de clarifier les obligations des Etats membres de l'Union européenne en la matière. D'autre part, faire l'état des lieux du droit positif français sur le sujet, et mesurer sa conformité avec les obligations européennes. *In fine,* l'objectif principal de ce travail consiste en l'élaboration d'un guide de

recommandations à destination de la France, pour une lutte effective contre les cyberVSS. Ce guide a également pour but d'être traduit et de s'adresser à l'ensemble des Etats membres de l'Union européenne, afin de les accompagner dans le processus de transposition de la Directive 2024/1385 en droit national (obligation d'ici 2027).

Si initialement les livrables attendus comprenaient un document de plaidoyer à destination des Etats membres, ainsi qu'une version pédagogique et des supports de communication, les différentes réunions tenues avec les associations partenaires ainsi qu'avec notre professeure encadrante, Audrey Darsonville, ont été déterminantes pour recentrer la commande initiale et l'adapter aux contraintes de temps et de faisabilité de notre groupe.

La première réunion a eu lieu le 25 novembre, en présence de Madame Alyssa Ahrabare, responsable du plaidoyer d'Osez le Féminisme et présidente de la CLEF, ainsi que de notre professeure. Cette rencontre s'est révélée particulièrement utile : elle a permis de clarifier les attentes des associations et de définir les contours précis de notre mission.
A l'issue de cet échange, il a été convenu de réaliser trois livrables. Un premier portant sur les obligations européennes relatives aux infractions susmentionnées, s'appuyant sur plusieurs instruments juridiques de l'UE. Un deuxième, consacré aux obligations issues du droit français. Et enfin, un dernier présentant une comparaison des législations de trois Etats membres de l'UE, permettant d'en déduire des recommandations pour la transposition.
Une première échéance nous a été fixée : finaliser le premier livrable d'ici la fin décembre.

Le 17 janvier, une deuxième réunion s'est tenue, avec Madame Ahrabare et Justine Cassar, élève avocate, alors en stage au sein de la CLEF, ayant pour but d'obtenir des retours sur cette première production. Il nous a été suggéré d'approfondir nos développements en y ajoutant des éléments contextuels, des exemples et des comparaisons avec d'autres infractions. Une nouvelle rencontre a été prévue pour le mois de mars, nous laissant suffisamment de temps pour nous consacrer au deuxième livrable.

La réunion du 13 mars, cette fois-ci uniquement en présence de notre professeure, a été décisive pour la structure finale de notre rendu. Nous avons décidé de l'organiser en quatre parties, correspondant aux infractions étudiées. Chaque partie devait être à son tour subdivisée en quatre sous-parties. Une première sur le contexte, une deuxième sur les obligations européennes, une troisième sur celles françaises et une dernière partie analytique qui nous guiderait vers la rédaction des recommandations.

La réunion du 23 avril avec Madame Ahrabare a servi à valider la structure retenue et à convenir ensemble que nous n'aurions pas le temps de réaliser le travail de comparaison des

législations de trois Etats membres, initialement prévu. Elle a également été consacrée à l'organisation de différents entretiens que nous souhaitions mener. En ce sens, Madame Ahrabare nous a transmis une liste de contacts experts dans différents pays afin de nous permettre d'organiser des entretiens visant à clarifier plusieurs points clefs de notre recherche. Elle nous a également conseillées sur la façon de structurer ces entretiens, afin qu'ils puissent enrichir de manière pertinente notre travail.

Si notre travail reposait en grande partie sur une analyse juridique et documentaire, il a été orienté et enrichi par les apports de nos partenaires, qui nous ont non seulement transmis des ressources pertinentes, mais aussi suggéré des pistes de recherche et conseillé certaines lectures clés. Pour autant, notre approche ne s'est pas limitée à cet aspect théorique : nous avons aussi adopté une démarche de terrain.

A ce titre, le 14 février 2025, nous avons eu l'immense chance d'être conviées à un colloque organisé à Strasbourg par Osez le Féminisme et la CLEF, intitulé « Exploitation sexuelle en ligne : enjeux et réponses européennes ». Réunissant des parlementaires, des eurodéputées, des responsables gouvernementaux ou encore des avocates[1], cet événement nous a permis d'approfondir nos connaissances et d'adopter un regard davantage critique sur les cyberviolences à caractère sexuel. Nous avons pris de nombreuses notes sur les interventions et échanges de cette journée, ils ont ainsi largement contribué à enrichir les développements de ce travail.

Nous avons par ailleurs mené plusieurs entretiens afin de compléter notre réflexion par des expertises variées.

Le premier a eu lieu le 28 mai avec trois représentantes de la MIPROF[2], Cécile Mantel, Julie Caillet et Katty Jorge Maia. Le 30 mai, nous avons échangé avec Céline Piques, membre d'Osez le Féminisme et rapporteuse au sein de la commission sur les violences faites aux femmes du Haut Conseil à l'Egalité entre les femmes et les hommes. Le troisième entretien s'est tenu le 2 juin avec Mariana Branco, qui mène actuellement une étude approfondie sur la plateforme Only Fans. Le 3 juin, nous avons eu l'honneur de rencontrer deux personnalités engagées : Ruth Breslin, directrice de l'Institut irlandais de recherche et de politiques sur l'exploitation sexuelle, puis Mié Kohiyama, cofondatrice de l'association « Be Brave France

[1] Osez le Féminisme. (CP) Colloque international : Exploitation sexuelle en ligne : enjeux et réponses européennes – Osez le feminisme ! (consulté le 16 mai 2025).
[2] Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains.

», de lutte contre la pédocriminalité. Enfin, le 6 juin, nous avons échangé avec Alejandra Mariscal López, directrice de l'association « Point de contact », spécialisée dans la lutte contre la cyberviolence et la protection des droits fondamentaux dans l'espace numérique.

Introduction

L'adoption de la Directive (UE) 2024/1385 du Parlement européen et du Conseil, le 14 mai 2024, marque une avancée majeure dans la lutte contre la violence à l'égard des femmes et la violence domestique. Elle vient combler une lacune normative significative, notamment en matière de cyberviolences. Le Conseil européen[3] a souligné que les initiatives de l'UE visant à mettre fin à ces violences s'inscrivent dans un contexte marqué par une augmentation préoccupante de la violence en ligne.

En France, à titre d'exemple, 348 000 infractions numériques ont été enregistrées en 2024, dont 103 300 atteintes aux personnes, soit une hausse de 7% par rapport à l'année précédente. Les femmes sont surreprésentées parmi les victimes, représentant 66% des victimes majeures et 70% des victimes mineures de ces atteintes[4]. Concernant la cyberviolence spécifiquement, une étude datant de novembre 2022 révélait déjà que plus de 4 françaises sur 10 déclaraient avoir été victimes de ce phénomène. Parmi le nombre total de victimes interrogées, 84% étaient des femmes et 51% des personnes âgées de moins de 30 ans[5]. Les cyberviolences impactent donc principalement les jeunes femmes.

En 2020, une jeune femme sur deux en Europe a subi un acte de cyberviolence fondé sur le sexe, généralement à caractère sexuel[6]. Selon une étude de *The Economist Intelligence Unit*, en 2021, 85% des femmes dans le monde sont exposées à la violence sur internet[7]. Mais les cyberviolences visent aussi particulièrement les femmes qui sont actives dans la sphère publique, telles que les journalistes et les responsables politiques.

[3] Conseil européen et Conseil de l'UE. (2024). « Mesures prises par l'UE pour mettre fin à la violence à l'égard des femmes ». Mesures prises par l'UE pour mettre fin à la violence à l'encontre des femmes - Consilium (consulté le 4 février 2015).
[4] Ministère de l'Intérieur. (2025). « Les infractions liées au numérique enregistrées par les services de sécurité en 2024 » (consulté le 17 février 2025).
[5] Féministes contre le cyberharcèlement. (2022). « Cyberviolence et cyberharcèlement : le vécu des victimes ». Enquête conduite par IPSOS auprès de 216 victimes de cyberviolences âgées de 16 ans à 60 ans ou plus. https://www.vscyberh.org/.
[6] Parlement européen et Conseil européen. (2022). « Proposition de directive sur la lutte contre la violence à l'égard des femmes et la violence domestique ». EUR-Lex - 52022PC0105 - EN - EUR-Lex, p.2.
[7] The Economist Intelligence Unit. (2020). « Measuring the prevalence of online violence against women ». Measuring the prevalence of online violence against women.

En ce sens, en 2018, la Rapporteuse spéciale des Nations Unies sur la violence contre les femmes, a publié un rapport[8] sur la violence en ligne ou facilitée par les technologies de l'information et de la communication (TIC) à l'égard des femmes et des filles du point de vue des droits humains. Ce rapport soulignait le fait que « *les agressions en ligne envers les femmes journalistes et les femmes travaillant dans le secteur des médias constituent une attaque directe contre la visibilité des femmes et leur pleine participation à la vie publique* ». Ces attaques contre les femmes journalistes entravent l'exercice de leur métier, entraînant des conséquences néfastes sur leur participation à l'équilibre démocratique. C'est pourquoi le préambule de la Directive (UE) 2024/1385 insiste sur ce phénomène et énonce que « *la cyberviolence cible et touche tout particulièrement les femmes politiques, les journalistes femmes et les femmes qui défendent les droits de l'homme. (...) La cyberviolence peut avoir pour effet de réduire les femmes au silence et d'empêcher leur participation à la vie de la société sur un pied d'égalité avec les hommes* ».

Face à ces constats, la nécessité d'une réponse juridique européenne harmonisée s'est imposée. Jusqu'à l'adoption de la Directive 2024/1385, aucun cadre spécifique ne permettait de traiter de manière cohérente les cyberVSS à l'échelle de l'UE.

La cyberviolence correspond à l'utilisation de technologies en ligne et de communications - plateformes en lignes, réseaux sociaux, messageries -, pour causer, faciliter ou menacer d'actes de violence des individus[9]. Cette forme de violence « *trouve son origine dans les inégalités de genre, qui sont une manifestation des discriminations structurelles à l'égard des femmes* »[10]. Elle s'inscrit donc dans la catégorie des violences faites aux femmes, qui inclut « *tous les actes de violence qui entraînent ou sont susceptibles d'entraîner des dommages ou des souffrances de nature physique, sexuelle, psychologique ou économique, y compris les menaces d'accomplissement de tels actes* »[11]. Les cyberVSS doivent donc être appréhendées comme faisant partie d'un continuum des violences sexistes et sexuelles. Une étude datant de novembre 2022 relatait que pour 72% des victimes, les violences ayant été

[8] Simonovic Dubravka, Rapporteuse spéciale des Nations Unies sur la violence contre les femmes et filles. (2018). « Rapport 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 ». https://digitallibrary.un.org/record/1641160?ln=fr&v=pdf.
[9] Lobby européen des femmes. (2024). « Rapport sur la cyber violence contre les femmes. Résumé analytique et recommandations », p. 6.
[10] Parlement européen et Conseil européen. (2022). *Op.cit.*, p.1.
[11] *Ibidem*.

initiée en ligne se sont poursuivies en physique[12]. Les violences numériques constituent une forme nouvelle de violences qui s'ajoute à celles déjà existantes, et les renforcent.

Le nombre de femmes victimes de ces « *formes de violence est disproportionné, en raison des schémas sous-jacents de contrainte, de pouvoir et de contrôle* »[13]. C'est pour cela que même si « *toute personne peut potentiellement en être victime, quel que soit son sexe ou son genre* »[14], nous nous concentrerons dans ce dossier uniquement sur les femmes victimes.

Il a été démontré que « *les espaces numériques renforcent et intensifient les inégalités de genre systémiques structurelles, de même que les modèles de masculinité toxique* »[15]. Les masculinistes estiment que les femmes et les féministes cherchent, ou ont déjà réussi, à renverser l'ordre patriarcal au profit d'une société matriarcale — une évolution à laquelle ils s'opposent fermement, convaincus de la supériorité naturelle des hommes sur les femmes[16].

Parmi eux, nous pouvons citer le mouvement « incel » - célibataire involontaire -, qui incite à la violence en ligne envers les femmes et encourage ses membres en les qualifiant d'héroïques[17].

Autre exemple, les « Men Going Their Own Way (MGTOW) » qui défendent la théorie d'un gynocentrisme social - selon laquelle le monde tournerait autour des femmes -, et prônent l'abandon total de relations affectives avec elles pour préserver leur masculinité[18].

Ces groupes ne sont pas isolés : ils s'inscrivent dans un écosystème plus large nommé la « manosphère », un réseau de communautés d'hommes en ligne qui plaide pour ce qu'ils perçoivent comme leurs propres intérêts en promouvant des idéologies misogynes, antiféministes et sexistes.

La dangerosité de la cyberviolence tient autant à son ampleur et à sa rapidité de diffusion qu'à son anonymat, à la difficulté pour les victimes de supprimer les contenus préjudiciables, ainsi qu'à la dimension publique, répétitive et invasive des attaques. Ces caractéristiques peuvent entraîner des conséquences graves pour les femmes.

---

[12] Féministes contre le cyberharcèlement. (2022). *Op. cit.*
[13] Parlement européen et Conseil européen. (2022). *Loc.cit.*
[14] *Ibidem.*
[15] Lobby européen des femmes. (2024). *Loc. cit.*
[16] Service public fédéral Intérieur, Direction générale Sécurité et Prévention. (2022). Fiche informative, « La Manosphère », p.5. FICHE MANOSPHÈRE _FR.pdf.
[17] Parlement européen et Conseil européen. (2022). *Op. cit.*, p.2.
[18] Service public fédéral Intérieur, Direction générale Sécurité et Prévention. (2022). *Ibid.*, p. 7.

Sur le plan psychologique d'abord, les cyberviolences ont un impact dans 80% des cas. Elles peuvent entraîner des syndromes de stress post-traumatique, tels que de l'hypervigilance, des troubles anxieux et dépressifs, des troubles alimentaires, des pensées suicidaires, etc[19].

Ensuite, au niveau économique et social, dans 1 cas sur 2, un impact moyen à très fort est rapporté par les victimes sur leurs études ou leur vie professionnelle[20]. Elles peuvent également rencontrer des difficultés pour trouver un emploi. De plus, certaines subissent les conséquences de rumeurs ou d'exclusion sociale[21].

Face à ces défis, l'instauration de normes minimales pour garantir les droits, le soutien et la protection des victimes de toute forme de cybercriminalité fondée sur le sexe[22] s'est avérée indispensable. En ce sens, au niveau de l'UE, le Parlement a appelé à maintes reprises la Commission à proposer une législation sur la violence à l'égard des femmes, en incluant la cyberviolence fondée sur le sexe. Le Parlement européen a en outre adopté deux rapports d'initiative législative sur le sujet, fondés sur l'article 225 du Traité sur le fonctionnement de l'UE (TFUE)[23]. Finalement, une proposition de Directive visant à garantir un niveau minimal de protection contre ces violences faites aux femmes au sein des Etats membres a été émise le 8 mars 2022. Elle est adoptée le 14 mai 2024[24] dans un environnement européen en carence d'instruments spécifiquement dédiés à cette problématique. Nonobstant, cette Directive vise à compléter la Convention d'Istanbul[25], instrument du Conseil de l'Europe, central dans la lutte contre les violences faites aux femmes. Elle est entrée en vigueur en 2014 et l'UE y a adhéré en 2023. Bien que ce texte constitue un cadre de référence majeur dans la lutte contre les violences faites aux femmes, il ne couvre pas les phénomènes émergents tels que la cyberviolence.

[19] Féministes contre le cyberharcèlement. (2022). *Op.cit.*
[20] *Ibidem.*
[21] Assemblée Parlementaire de la Francophonie, Réseau des femmes parlementaires. (2021). « Rapport final : la cyberviolence envers les femmes et les enfants dans l'espace francophone », p.5, 9. Microsoft Word - Rapport final sur la cyberviolence envers les femmes et les enfants.
[22] Conseil européen et Conseil de l'UE. (2024). *Op.cit.*
[23] Traité sur le fonctionnement de l'UE (version consolidée). (2012). Voir article 225.
[24] Parlement européen et Conseil européen. (2024). « Directive (UE) 2024/1385, du 14 mai 2024, sur la lutte contre la violence à l'égard des femmes et la violence domestique ». Directive - UE - 2024/1385 - EN - EUR-Lex.
[25] Conseil de l'Europe. (2011). « Convention sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (Convention d'Istanbul) » .

Le préambule de la Directive 2024/1385 du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique énonce qu'il y a lieu « d*'harmoniser les définitions des infractions et les sanctions relatives à certaines formes de cyberviolence lorsque la violence est intrinsèquement liée à l'utilisation des technologies de l'information et de la communication* ». Ce texte précise que les caractéristiques de l'infraction sont particulières car les technologies « *sont utilisées pour amplifier de manière conséquente la gravité de l'incidence préjudiciable de l'infraction* ». Les cyberviolences contiennent donc une dimension particulièrement nocive et préjudiciable de manière inhérente.

De nombreuses infractions d'une dimension nouvelle sont permises et facilitées par les outils de communications. Ces derniers ouvrent un nouveau spectre de violences, aux conséquences graves pour les victimes. Ces cyberviolences multiformes ont un impact conséquent dans la mesure où elles permettent à l'agresseur de créer une atmosphère d'insécurité et de contrôle permanent sur la vie de la victime. Toutes les sphères de la vie de la victime sont irriguées par le comportement de l'agresseur : vie publique, vie privée, vie en ligne et hors ligne.

Il convient de rappeler qu'une Directive européenne n'est pas directement applicable. Elle ne produit d'effets qu'après avoir été transposée dans les ordres juridiques nationaux, laissant ainsi aux États membres la discrétion de déterminer les modalités de sa mise en œuvre. Par ailleurs, elle fixe des « standards minimums », permettant aux Etats membres d'opter pour une transposition du texte plus protectrice pour les victimes. En attendant la transposition, qui doit avoir lieu dans les trois ans suivant son adoption par l'UE, la Directive 2024/1385 n'a pas de caractère contraignant pour les justiciables, qui n'ont donc pas la possibilité de s'en prévaloir directement.

Ce livrable s'articulera autour de quatre axes, correspondant aux quatre articles de la Directive 2024/1385 ciblant différents types d'infractions propres à la violence en ligne. A savoir, le partage non consenti d'images intimes (article 5), la traque furtive en ligne - ou « *cyber stalking* » - (article 6), le cyber harcèlement (article 7), et l'incitation à la violence ou à la haine en ligne (article 8). Dans un objectif pragmatique, pédagogique et un besoin de lisibilité, pour chaque incrimination, une même structure en quatre parties sera suivie. La première vise à inscrire les comportements pénalisés par la Directive dans un contexte plus large. La deuxième porte sur la législation européenne, ce qui inclut les dispositions de la Directive, qui seront croisées avec d'autres instruments européens pertinents (Digital Services

Act (DSA), Règlement général sur la protection des données (RGPD), Charte des droits fondamentaux de l'UE, etc.), afin de préciser les obligations concrètes des Etats membres dans chaque matière. La troisième partie se concentre sur la manière dont sont incriminées les infractions susmentionnées par la législation française. Enfin, la dernière consiste en une analyse jurisprudentielle et doctrinale de ces législations, permettant de pointer d'éventuelles lacunes existantes à la fois au niveau européen et au niveau français.

In fine, ce travail a pour optique de formuler des recommandations pour la transposition de la Directive 2024/1385, conformes et cohérentes avec le cadre normatif existant, permettant une transposition et une mise en œuvre du texte efficace et protectrice pour les victimes.

Développement

1. Le partage non consenti de matériels intimes ou manipulés

1.1. Contexte

Le partage non consenti d'images ou de vidéos à caractère intime, qu'elles soient authentiques ou manipulées, constitue une forme particulièrement destructrice de violence numérique. Une fois diffusés en ligne, ces contenus sont extrêmement difficiles à faire disparaître, en raison de leur viralité, de leur hébergement sur des serveurs situés à l'étranger, ou encore du manque de coopération de certaines plateformes.

L'affaire dite « French Bukkake » illustre parfaitement cette impasse. Initiée en 2023 et toujours en cours, elle concerne des faits de viols commis dans le cadre de tournages pornographiques organisés par Pascal Ollitraut et son label. Elle compte 17 mis en cause et 42 parties civiles, parmi lesquelles Osez le Féminisme. Malgré la gravité des charges retenues, beaucoup des vidéos des parties civiles du procès sont toujours en ligne, entraînant une retraumatisation et revictimisation constante des victimes qui subissent des agressions, des discriminations et du chantage. Cette situation n'est pas isolée : une fois publiés, les contenus intimes, sexuels ou de violences sexuelles sont pratiquement impossible à faire retirer de manière permanente, ce qui soulève d'importantes questions relatives à l'inaction des plateformes, et à la responsabilité des institutions européennes et des Etats membres.

La problématique est tout aussi préoccupante en ce qui concerne les matériels manipulés, qui sont pour la majorité pornographiques. La publication sur des sites web de scènes à caractère sexuel montées avec le visage de célébrités témoigne de l'ampleur du phénomène, qui aurait commencé dès 2017. A noter que le fait que ce soient des images non réelles ne modifie en rien la souffrance des victimes[26].

Ce type de violence[27] a des conséquences négatives réelles sur le respect de la vie privée des victimes ainsi que sur leur droit à la dignité et à l'intégrité. Rien n'est véritablement privé sur Internet, et de nombreux sites vivent de la monétisation de contenus érotiques violents. En

[26] Osez le Féminisme et la CLEF. (2025). Colloque : « Exploitation sexuelle en ligne : enjeux et réponses européennes ». Strasbourg.
[27] *Ibidem.*

outre, le partage de telles images a des effets négatifs réels ou prévisibles en matière de violences sexistes, de protection de la santé publique et des mineur-es, ainsi que des conséquences graves sur le bien-être physique et mental des personnes.

Cette réalité soulève alors des enjeux juridiques majeurs, notamment en matière de droit à l'effacement - pourtant garanti par le RGPD -, et de droit à la vie privée.

1.2. Le cadre juridique européen

Le partage non consenti de contenus intimes ou manipulés constitue l'une des infractions pénales prévues par la Directive 2024/1385. Son article 5 le définit comme le fait de « *produire, manipuler ou modifier, puis de rendre accessibles, via des technologies de l'information et de la communication (TIC), des images, vidéos ou autres matériels similaires représentant des activités sexuellement explicites ou des parties intimes, sans le consentement des personnes concernées* »[28]. Constitue également une infraction pénale le fait de menacer de commettre ces actes.
La question des images privées, de leur partage et de leur suppression a déjà fait l'objet de réglementations dans la sphère législative européenne.

1.2.1. Le Digital Services Act (DSA)

Le Règlement du 19 octobre 2022 relatif à un marché unique des services numériques[29], aussi connu sous le nom de Digital Services Act contient des dispositions pertinentes dans le cadre de la lutte contre le partage non consenti de contenus intimes ou manipulés.

Le considérant 12 du texte précise que, parmi les contenus définis comme illégaux, figure le **« partage illicite et non consensuel d'images privées »**[30]. Bien que les considérants

[28] Parlement européen et Conseil européen. (2024). *Op.cit.*, article 5.
[29] Parlement européen et Conseil. (2022). Règlement (UE) 2022/2065 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (ci-après : Digital Services Act). Règlement - 2022/2065 - EN - EUR-Lex.
[30] Parlement européen et Conseil. (2022). *Op. cit.*, considérant 12.

soient dépourvus de valeur contraignante, ils sont rédigés dans le but de rendre le contenu des actes législatifs européens plus clair, et ainsi servir à leur interprétation[31]. Le DSA impose aux plateformes numériques des obligations concernant le contenu accessible aux utilisateurs et utilisatrices, en particulier en matière de contenu illégal. **Le considérant 12 prévoit l'application de ces obligations dans les cas de diffusion illicite et non consentie d'images privées.**

> « *Afin d'atteindre l'objectif consistant à* ***garantir un environnement en ligne sûr, prévisible et fiable,*** *il convient, aux fins du présent règlement, que la notion de « contenu illicite » corresponde de manière générale aux règles en vigueur dans l'environnement hors ligne. Il convient, en particulier, de* ***donner une définition large de la notion de « contenu illicite »*** *de façon à ce qu'elle couvre les informations relatives aux contenus, produits, services et activités illégaux. En particulier, cette notion devrait être comprise comme se référant à des informations, quelle que soit leur forme, qui, en vertu du droit applicable, sont soit elles-mêmes illicites, comme les discours haineux illégaux ou les contenus à caractère terroriste et les contenus discriminatoires illégaux, soit* ***rendues illicites par les règles applicables en raison du fait qu'elles se rapportent à des activités illégales****. Il peut s'agir, par exemple, du partage d'images représentant des abus sexuels commis sur des enfants, du* ***partage illégal d'images privées sans consentement****, du harcèlement en ligne, (...) ».*

En vertu de l'article 18 du DSA, **les fournisseurs de services d'hébergement,** définis par le texte comme des « *entités fournissant un service de stockage des informations* »[32], doivent **signaler** « ***promptement*** » **aux autorités compétentes tout soupçon d'infraction pénale** « *menaçant la vie ou la sécurité d'une personne* ». Ils doivent fournir toutes les informations pertinentes disponibles.

Autrement dit, lorsque les fournisseurs de services d'hébergement disposent d'informations pouvant laisser penser qu'une infraction pénale représentant une menace pour la vie ou la sécurité d'une ou plusieurs personnes a été commise, est en train d'être commise ou est susceptible d'être commise, ils sont tenus d'informer et de transmettre les informations

[31] Den Heijer, M ; Abeelen, T ; Maslyka, A. (2019). « On the Use and Misuse of Recitals in European Union Law ». *Amsterdam Law School Research Paper.* No°2019-31. p. 3.
[32] Parlement européen et Conseil. (2022). *Op.cit.*, article 3§g iii).

pertinentes aux autorités répressives ou judiciaires de l'État membre concerné. Si le fournisseur de service d'hébergement ne peut identifier avec certitude l'État membre concerné, il doit informer les autorités de l'État où il est établi, où réside son représentant légal, ou Europol. L'État membre concerné est défini comme celui où l'infraction a eu lieu, est en cours ou pourrait se produire, ou encore celui où se trouvent l'auteur présumé ou la victime.

Le partage non consenti d'images intimes, notamment sur les réseaux sociaux, entre dans le cadre d'une infraction pénale menaçant la vie ou la sécurité d'une personne. En effet, **les victimes de ce type de violences subissent de multiples formes de « revictimisation » (harcèlement en ligne, chantage, agressions physiques, violences sexuelles, etc)**[33]. De fait, les fournisseurs de services d'hébergement sont tenus de notifier les autorités compétentes en cas de suspicion d'une telle infraction. Il convient de mettre en place des mesures pour rendre effective cette obligation de signalement, ainsi que la notification systématique aux victimes. Cela faciliterait la suppression précoce des contenus, pour une meilleure protection des victimes, ainsi que pour une mise en cause plus rapide des auteurs de l'infraction.

Les articles 34 et 35 concernent les fournisseurs de plateformes en ligne, c'est-à-dire les services d'hébergement qui « *à la demande d'un destinataire du service, stockent et diffusent au public des informations* »[34]. En vertu de ces dispositions, les fournisseurs de plateformes en ligne ont l'**obligation d'analyser et d'évaluer de manière « *diligente* » tout risque systémique découlant de la conception ou du fonctionnement de leurs services**[35]. Ils doivent, en conformité avec l'article 35, prendre des mesures permettant d'**atténuer ces risques « *réels ou prévisibles* »**, lesquels doivent être « ***raisonnables, proportionnées, efficaces et adaptées*** ».

L'Acte délégué sur les audits indépendants au titre de la législation sur les services numériques, adopté par la Commission européenne à la suite du DSA en 2023, précise que pour évaluer si les fournisseurs ont bien réalisé une analyse « diligente » des risques systémiques découlant de la conception ou du fonctionnement de leurs services, doivent au minimum être pris en compte : la considération par le fournisseur des aspects régionaux et linguistiques de l'utilisation de son service - y compris quand ces aspects sont spécifiques à un Etat membre -,

[33] *Ibidem.*
[34] Parlement européen et Conseil. (2022). *Op.cit.*, article 3§i.
[35] Parlement européen et Conseil. (2022). *Ibid.,* article 34.

l'inclusion dans le processus d'évaluation d'expertises techniques et scientifiques, le respect par le fournisseur des délais prévus par les articles 34 et 35 précités et la réalisation d'évaluation des risques avant la mise en place de fonctionnalités susceptibles d'avoir un impact sur les risques énoncés par les articles 34 et 35[36].

En ce qui concerne les mesures que doivent prendre les fournisseurs en application de l'article 35 du DSA, l'article 14 de l'Acte délégué sur les audits indépendants précise seulement que pour évaluer si ces mesures sont raisonnables, proportionnées, efficaces et adaptées, l'entité réalisant l'audit devra vérifier si elles répondent collectivement à tous les risques, et en particulier à ceux concernant l'exercice de droits fondamentaux[37].

La liste de ces risques est dressée à l'article 34 et permet d'étendre l'obligation d'atténuation au partage non-consensuel d'images intimes, en ce qu'elle porte atteinte au droit à la dignité humaine et au respect de la vie privée et familiale.
Les fournisseurs de plateformes doivent également **atténuer les effets négatifs liés aux violences sexistes, à la protection de la santé publique et des mineur-es**, ainsi que **les conséquences graves sur le bien-être physique et mental des individus**[38]. Pour cela, ils doivent examiner la conception de leurs systèmes, les conditions générales d'utilisation et la gestion de leurs données, afin de déterminer la façon dont ces éléments influencent les risques[39].

L'article 34 implique également un **devoir de transparence.** Il énonce en effet que les fournisseurs doivent conserver les données relatives aux évaluations de risques et pouvoir les transmettre à la Commission ainsi qu'au coordinateur pour les services numériques de l'État membre d'établissement.

Les obligations en matière d'évaluation des risques contenues dans les articles cités peuvent ainsi participer à la protection des personnes.
L'absence explicite de mention des cyberviolences à l'égard des femmes dans le texte

[36] Commission européenne. (2023). « Acte délégué sur les audits indépendants au titre de la législation sur les services numériques, C/2023/6807 ». Article 13.
[37] Commission européenne. (2023). *Op.cit.,* article 14.
[38] Parlement européen et Conseil. (2022). *Op. cit.*, article 34.
[39] Citron, D.K ; Franks, M.A. (2014). « Criminalizing Revenge Porn ». *Wake Forest Law Review*, 49 (2), p. 346.

n'empêche en aucun cas que celui-ci soit appliqué à ce type de situations, comme par exemple au partage non-consensuel de contenu intime visé dans la Directive 2024/1385.

1.2.2. Le Règlement général sur la protection des données

Le Règlement UE 2016/679 du 27 avril 2016[40], communément appelé « Règlement général sur la protection des données » (RGPD), met en place des normes protectrices axées sur la protection des données à caractère personnel. Son article 4 les définit comme « *toute information se rapportant à une personne physique identifiée ou identifiable […] ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Dans son arrêt Breyer du 19 octobre 2016[41], la Cour de justice de l'Union européenne apporte des précisions sur ce qui constitue une « donnée à caractère personnel » au sens du RGPD. Elle établit que le fait qu'une personne puisse être identifiée grâce à une donnée ne suffit pas pour que celle-ci soit considérée comme ayant un caractère personnel[42]. Bien que l'arrêt consacre la notion « *d'identification indirecte* » et étend ainsi en apparence la définition de la donnée personnelle, l'affirmation selon laquelle l'identification d'une personne ne suffit pas à qualifier une donnée de personnelle vient poser une limite à l'exercice des droits consacrés par le RGPD dans certaines situations.

La Cour indique au point 41 de l'arrêt susmentionné : « *afin de qualifier une information de donnée à caractère personnel, il n'est pas nécessaire que cette information permette, à elle seule, d'identifier la personne concernée* ». Elle précise au point suivant que : « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens*

[40] Parlement européen et Conseil. (2016). Règlement UE 2016/679 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.
[41] Cour de justice de l'Union européenne. (2016). Arrêt « Breyer ». C-582/14, EU:C:2016:779. Points 39 et 41.
[42] *Ibid.,* point 46.

susceptibles d'être raisonnablement mis en œuvre soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne »[43].
C'est ici qu'est indirectement posée par la Cour une limite : si l'identification de la personne est considérée comme « *irréalisable en pratique, par exemple en raison du fait qu'elle impliquerait un effort démesuré en termes de temps, de coût et de main-d'œuvre* »[44], la donnée ne sera pas considérée comme personnelle. Or la nature « *irréalisable* » de l'identification est susceptible de faire l'objet d'interprétations subjectives, autant par les destinataires du RGPD que par les juridictions.

Il est important de noter que le RGPD met en place des exceptions à l'interdiction de traitement des catégories particulières de données. Son considérant 52 précise que n'est autorisé le traitement de ces données, parmi lesquelles celles concernant la vie sexuelle, que « *lorsque le droit de l'Union ou le droit d'un État membre le prévoit et sous réserve de garanties appropriées, afin de protéger les données à caractère personnel et d'autres droits fondamentaux* ». C'est une approche restrictive des autorisations de traitement de données particulières.

De manière relative au traitement non consenti d'images ou de vidéos intimes, figurent à l'article 9 du RGPD, dans la liste des catégories particulières de données à caractère personnel, **les données concernant la vie sexuelle des personnes physiques**. Cet article interdit purement et simplement leur traitement, sauf dans le cas où la personne concernée a donné son consentement ou dans les cas - listés par l'article - où d'autres motifs justifient ce traitement.

De plus, **le droit à l'effacement** (« **ou droit à l'oubli** ») figurant à l'article 17 du RGPD revêt un intérêt particulier dans le contexte de la transposition de la Directive 2024/1385. En vertu de cet article, toute personne concernée peut obtenir, dans les meilleurs délais, l'effacement de ses données personnelles si les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière (a) ; **la personne concernée retire le consentement sur lequel est fondé le traitement[45]**, et il n'existe pas d'autre fondement juridique au traitement (b) ; **la personne concernée s'oppose au**

[43] *Ibid.,* point 42.
[44] Cour de justice de l'Union européenne. (2016). *Op.cit.,* point 46.
[45] Parlement européen et Conseil. (2016). Idem. Conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a)

traitement en vertu de l'article 21[46], et il n'existe pas de motif légitime impérieux pour le traitement (c); **les données à caractère personnel ont fait l'objet d'un traitement illicite** (d) ; les données à caractère personnel doivent être effacées pour **respecter une obligation légale** qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis (e).

Le « droit à l'oubli » est une expression juridique qui englobe plusieurs droits, parmi lesquels le droit à l'effacement[47] et le droit au déréférencement[48]. Il s'exerce dans un premier temps auprès de l'entité ayant rendu les données publiques, laquelle est tenue de prendre des mesures raisonnables pour informer les responsables du traitement des données que la personne concernée a demandé l'effacement de tout lien vers ses données à caractère personnel, ou de toute copie ou reproduction de celles-ci. « *Le caractère raisonnable des mesures sera apprécié à l'aune des technologies disponibles et des coûts de mise en œuvre* »[49].

Si la demande d'effacement ou de déréférencement est refusée, l'individu débouté peut se tourner vers l'autorité chargée de veiller au respect du RGPD. En France, il s'agit de la Commission nationale de l'informatique et des libertés (CNIL).

Dans un arrêt du 6 décembre 2019, le Conseil d'Etat donne des indications quant aux modalités d'évaluation de la demande d'oubli. La CNIL doit s'appuyer sur un faisceau d'indices qui inclut « *la nature des données en cause, leur contenu, leur caractère plus ou moins objectif, leur exactitude, leur source, les conditions et la date de leur mise en ligne et les répercussions que leur référencement est susceptible d'avoir pour la personne concernée et, d'autre part, la notoriété de cette personne, son rôle dans la vie publique et sa fonction dans la société*. »[50]

---

[46] Parlement européen et Conseil. (2016). Idem. Article 21, paragraphe 1 : *« La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. »*

[47] Andréani, A. (2020). « Le droit à l'oubli : étude comparée entre la France et les Etats-Unis ». Thèse de doctorat. Université Paris II Panthéon-Assas.

[48] Terwangne, C. (2015). « Droit à l'oubli, droit à l'effacement? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique ». *Enjeux européens et mondiaux de la protection des données personnelles.* Création information communication, Larcier. Bruxelles, (p. 245-275).

[49] Boizard, M. (2016). « Le temps, le droit à l'oubli et le droit à l'effacement ». *Les Cahiers de la justice*, no 4, (p. 619-628).

[50] Conseil d'Etat. (2019). 10e et 9e chambre réunies, n° 429154, 6 décembre.

Ainsi, bien que le droit à l'oubli repose sur le principe du consentement, le simple retrait de ce consentement ne suffit pas. Dans le cadre du droit au déréférencement, l'exercice de ce droit est limité, dans la mesure où les juridictions et les responsables du traitement des données peuvent procéder à une appréciation subjective de l'opportunité de ce déréférencement[51].

Le RGPD impose également au responsable du traitement de prendre des **mesures raisonnables, y compris techniques, pour supprimer ces données, ainsi que toutes leurs copies ou reproductions**. Cependant, ces obligations sont **limitées par des exceptions**, telles que la liberté d'expression et d'information (article 17§3), les intérêts publics, ou l'exercice et la défense des droits en justice.

La nécessité de préserver la liberté d'expression est un motif fréquemment invoqué pour limiter la régulation des contenus en ligne[52]. C'est notamment le cas dans le domaine pornographique pour les vidéos à caractère violent[53]. La Directive 2024/1385 elle-même introduit la limitation de la liberté d'expression, ainsi que celle des arts et des sciences, dans son article 5§2. La limite considérée comme indéterminée entre l'expression protégée par la liberté d'expression et l'expression qui constitue une menace[54] incite les législateurs à une prudence qui ne permet pas toujours une protection effective des groupes vulnérables en ligne. **Or, la liberté d'expression constitue une liberté fondamentale pouvant être limitée par des intérêts légitimes[55], incluant « *la prévention du crime, la protection de la santé ou de la morale, la protection de la réputation ou des droits d'autrui* » [56]. Il est essentiel que ces limitations, conditionnées par un principe de nécessité, s'appliquent de manière pleine et entière dans l'espace numérique.** Le droit à l'effacement du RGPD fait écho aux dispositions de l'article 23 de la **Directive 2024/1385**, qui impose que **soient prises des mesures rapides de suppression ou de blocage de l'accès à certains contenus tels que les matériaux intimes ou les incitations à la violence.**

[51] Andréani, A. (2020). *Ibidem.*
[52] Nations Unies. « Hate speech versus freedom of speech ». https://www.un.org/en/hate-speech/understanding-hate-speech/hate-speech-versus-freedom-of-speech. (consulté le 22 mai 2025).
[53] Entretien avec Ruth Breslin. (3 juin 2025).
[54] Udoh-Oshin, G. (2017). « Hate Speech on the Internet: Crime or Free Speech ? ». Thèse undergraduate. Long Island University. (p. 5-6).
[55] Convention Européenne des Droits de l'Homme
[56] Cyberharcèlement. « Cyberharcèlement et liberté d'expression : les enjeux juridiques ». https://cyber-harcelement.info/la-frontiere-entre-cyberharcelement-et-liberte-dexpression-les-enjeux-juridiques/

« Les États membres prennent les mesures nécessaires pour garantir que le matériel en ligne accessible au public visé à l'article 5, paragraphe 1, points a) et b), et aux articles 7 et 8 de la présente directive soit ***rapidement retiré ou que l'accès à ce matériel soit désactivé****.*

Les mesures visées au premier alinéa du présent paragraphe comprennent la possibilité pour les autorités compétentes ***d'émettre des injonctions contraignantes de retirer ce matériel ou d'en rendre l'accès impossible.*** *Les États membres veillent à ce que ces injonctions remplissent au moins les conditions énoncées à l'article 9, paragraphe 2, du règlement (UE) n° 2022/2065».*

[Digital Service Act]

Dans la pratique, le principal défi dans les cas de partage non consenti d'images ou vidéos personnelles est celui de leur retrait rapide des plateformes en ligne. C'est pourquoi il peut être pertinent de s'appuyer sur le droit à l'oubli consacré par le RGPD pour mettre en place le retrait des contenus sanctionnés par la Directive 2024/1385.

Le droit à l'effacement est un mécanisme important pour permettre aux personnes de reprendre le contrôle sur leurs données personnelles, notamment en cas de diffusion non consentie de contenus sensibles. Toutefois, il présente des limites notables : il n'est pas proactif et son efficacité dépend largement de la collaboration des États, ainsi que de la réactivité des plateformes, qui peut varier fortement d'un cas à l'autre. **Cette dépendance rend sa mise en œuvre parfois lente ou inefficace dans des situations d'urgence.**

D'autres textes présentent des mécanismes intéressants pouvant être transposés au partage non consenti de matériels intimes, c'est le cas par exemple du Règlement européen contre la diffusion du terrorisme en ligne.

1.2.3. Règlement européen contre la diffusion du terrorisme en ligne

Ce dispositif a été intégré à la présente analyse car il démontre qu'**une réponse européenne coordonnée et contraignante permet de lutter efficacement contre la circulation rapide de contenus particulièrement préjudiciables.** Il constitue un précédent pertinent pour

envisager des mécanismes similaires dans le cadre des cyberVSS, en particulier s'agissant des contenus intimes diffusés sans consentement, des vidéos d'agressions sexuelles ou des deepfakes pornographiques. **À l'image de ce qui est prévu pour les contenus terroristes, un cadre européen devrait permettre d'imposer des délais stricts de retrait, de renforcer les obligations des plateformes et d'établir une coopération renforcée entre autorités nationales, services d'hébergement et organes européens. Cela permettrait de combler les lacunes actuelles et de mieux garantir le respect des droits fondamentaux des victimes de cyberVSS.**

L'affaire « Pornhub » et les révélations de l'enquête *Traffickinghub* ont mis en lumière la diffusion massive de contenus à caractère sexuel non consenti, y compris de mineur-es, soulignant l'ampleur du phénomène et l'urgence de mesures structurelles[57]. En l'absence de mécanismes contraignants similaires à ceux en vigueur pour les contenus terroristes, les victimes sont souvent livrées à elles-mêmes, avec pour seule option des démarches longues, individuelles et rarement efficaces.

Le **Règlement européen 2021/784 du 29 avril 2021**, relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, a permis la mise en place d'un cadre normatif strict pour éviter l'utilisation abusive des services d'hébergement à des fins terroristes.

Pour y parvenir efficacement, le texte prévoit notamment la possibilité d'émettre une injonction de retrait ou de blocage de contenus illicites[58]. **Ces mesures astreignent les fournisseurs de services d'hébergement à retirer ou bloquer l'accès aux contenus terroristes dans tous les États membres dans un délai d'une heure à compter de la réception de l'injonction de retrait.** Dans les cas où un fournisseur ne peut se conformer à l'injonction pour des raisons de force majeure ou d'impossibilités factuelles non imputables à sa responsabilité (raisons techniques ou opérationnelles justifiables, par exemple), il est tenu d'informer, sans retard injustifié, l'autorité compétente des motifs de son incapacité à agir.

Le Règlement impose également des **mesures préventives pour limiter, voire empêcher, l'exposition au contenu terroriste**[59]. Ces obligations s'appliquent en particulier aux fournisseurs d'hébergement identifiés comme « *exposés à des contenus terroristes* ». Ce statut

[57] Kristof, N. (2020). « The Children of Pornhub », *The New York Times*.
[58] Parlement européen et Conseil. (2021). Règlement (UE) 2021/784 relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne. Article 3.
[59] Parlement européen et Conseil. (2021). *Op. cit.*, article 5.

est attribué par l'autorité compétente de l'État membre où le fournisseur a son siège principal, ou bien où son représentant légal est établi. La décision repose sur des **critères objectifs**, tels que la réception de plusieurs injonctions de retrait au cours des 12 derniers mois. Cette décision doit être notifiée au fournisseur, qui sera ensuite tenu de prendre des **mesures spécifiques**. Parmi celles-ci, les fournisseurs sont enjoints à inclure dans leurs conditions générales une clause dédiée à la lutte contre l'utilisation abusive de leurs services pour diffuser des contenus terroristes, à mettre en place des moyens techniques adaptés pour identifier et retirer rapidement les contenus terroristes ou bloquer leur accès, ou encore proposer des mécanismes accessibles permettant aux utilisateurs de signaler ou de marquer des contenus à caractère terroriste.

Selon le rapport de la Commission européenne, l'application du Règlement (UE) 2021/784[60] a eu une incidence positive sur la limitation de la diffusion de ces contenus en ligne. Au moins 349 injonctions de retrait de contenus à caractère terroriste ont été transmises depuis son entrée en application. De plus, dans la plupart des cas, les fournisseurs de services d'hébergement ont rapidement pris des mesures pour supprimer les contenus ou en bloquer l'accès. Dans seulement 10 cas sur 349, le fournisseur ciblé a dépassé ce délai maximal d'une heure de retrait après avoir reçu l'injonction.

Ce rapport s'inscrit dans le cadre de l'application de l'article 22 du Règlement. La Commission doit présenter régulièrement des rapports au Parlement européen et au Conseil, relatifs à l'application du texte.

Pour assurer une collaboration transnationale, **l'outil PERCI (Plateforme Européenne de Retraits des Contenus illégaux sur l'Internet) a été mis en place.** Il permet de transmettre à la fois les injonctions de retrait et les signalements aux fournisseurs de services d'hébergement, et ce, de manière centralisée et coordonnée. **PERCI offre une solution technique pour le traitement des signalements et des injonctions de retrait et facilite la coopération entre les autorités compétentes, les fournisseurs de services d'hébergement et Europol.**

Les injonctions de retrait doivent respecter les principes de proportionnalité, de nécessité, et garantir le respect des droits fondamentaux tels qu'énoncés par la Charte des droits fondamentaux de l'UE, et ce sans discrimination. En cas de mise en œuvre de telles mesures,

[60] Commission européenne. (2024). Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre du Règlement (UE) 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

les fournisseurs doivent transmettre un rapport à l'autorité compétente dans les trois mois suivant leur adoption. Si les actions entreprises sont jugées insuffisantes, l'autorité peut ordonner des mesures supplémentaires.

1.2.4. Charte des droits fondamentaux de l'UE

La Charte des droits fondamentaux de l'UE a été adoptée le 7 décembre 2000. Depuis le traité de Lisbonne de 2009, elle a valeur contraignante. Ainsi, les droits qui y sont consacrés doivent être respectés tant par les institutions et organes de l'Union, que par les États membres **lorsqu'ils mettent en œuvre le droit de l'Union.**

Certaines de ses dispositions sont pertinentes dans le cas du partage non-consensuel de matériel intime. Son **article 8 consacre la protection des données à caractère personnel et son article 7** consacre **le droit au respect de la vie privée et familiale, du domicile et des communications**. Ce droit, en vertu de l'article 52§3 de la Charte, doit être considéré comme ayant les mêmes implications que **le droit à la vie privée consacré par la Convention de sauvegarde des droits de l'homme et libertés fondamentales.** La Cour européenne des droits de l'Homme, dans son arrêt *Dudgeon contre Royaume-Uni* du 22 octobre 1981 a par ailleurs établi que l'activité sexuelle d'une personne relevait d'un aspect intime de la vie privée[61].

1.3. Le cadre juridique français

En droit pénal français, le partage non consenti de matériels intimes ou manipulés est sanctionné par plusieurs dispositions du Code pénal. Premièrement, il convient de mentionner les articles 226-1 et 226-2 qui, au titre des atteintes à la vie privée, punissent notamment de délit le fait de « *fixer, enregistrer ou transmettre, sans le consentement de celle-ci, l'image*

[61] Cour européenne des droits de l'Homme. (1981). « Dudgeon c. Royaume-Uni ». Series A, No.45, para. 41.

d'une personne se trouvant dans un lieu privé ». Cette infraction est punie d'un an d'emprisonnement et de 45 000 euros d'amende.
Est aussi prévue une circonstance aggravante lorsque les faits sont commis par un conjoint ou concubin de la victime, ou encore par un partenaire lié à celle-ci par un pacte civil de solidarité. Dans ce cas précis, la peine s'élève à deux ans d'emprisonnement et à 60 000 euros d'amende.

Il faut ensuite se pencher sur l'article 226-2-1 qui vise le fait de capter, conserver et/ou diffuser des images à caractère sexuel sans l'accord de la personne concernée. Cette disposition insiste bien sur le « caractère sexuel » du contenu. Dans cette situation, il est important de bien dissocier l'accord de la victime pour la prise des photos, de son accord pour leur conservation, enregistrement et transmission. La diffusion des contenus constitue alors un délit renforcé d'atteinte à la vie privée puni de deux ans d'emprisonnement et de 60 000 euros d'amende.

> « *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.*»

La Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite « Loi SREN »[62], a pour objectif de rendre le droit français compatible avec le droit de l'UE et notamment avec le Digital Services Act. L'article 17 de ce dernier a apporté une modification à l'article 312-10 du Code pénal en y ajoutant trois alinéas pour encadrer le chantage fait à l'aide d'un contenu à caractère sexuel. Dans ce cas précis, la peine d'emprisonnement est de sept ans et l'amende est de 100 000 euros.

> « *Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une*

[62] Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque.

Le chantage est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

La peine d'emprisonnement est portée à sept ans d'emprisonnement et à 100 000 euros d'amende lorsque le chantage est exercé par un service de communication au public en ligne:

1° Au moyen d'images ou de vidéos à caractère sexuel ;

2° En vue d'obtenir des images ou des vidéos à caractère sexuel.»

Finalement, l'article 226-8-1, ajouté par la « Loi SREN » de 2024, vise spécifiquement les « *montages à caractère sexuel* » réalisés avec l'image ou les paroles d'une personne sans son consentement.

« *Est puni de deux ans d'emprisonnement et de 60 000 euros d'amende le fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un montage à caractère sexuel réalisé avec les paroles ou l'image d'une personne, sans son consentement. Est assimilé à l'infraction mentionnée au présent alinéa et puni des mêmes peines le fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un contenu visuel ou sonore à caractère sexuel généré par un traitement algorithmique et reproduisant l'image ou les paroles d'une personne, sans son consentement.*»

Une circonstance aggravante portant les peines à trois ans d'emprisonnement et à 75 000€ d'amende est constituée lorsque la publication du contenu visé a été réalisée « *en utilisant un service de communication au public en ligne.* ».

1.4. Analyse

Au niveau européen d'abord, une disposition du DSA interroge. Il s'agit du considérant 12 qui emploie l'expression « *partage illégal d'images privées sans consentement* ». L'emploi du

terme « illégal » implique qu'un partage non consenti d'images privées - comme des images intimes par exemple -, pourrait, dans certains cas, être considéré comme légal. Cela soulève une question essentielle : où place-t-on le curseur de la légalité et de l'illégalité d'un partage non consenti d'images intimes ? La nécessité de préciser le terme « illégal » soulève des interrogations. En effet, le partage d'images intimes sans le consentement des personnes concernées est strictement encadré, voire interdit, sauf dans des cas très exceptionnels. Par exemple, certaines images peuvent être légalement diffusées sans autorisation lorsqu'elles relèvent d'un événement d'actualité et répondent à un intérêt public[63].

Au contraire, pour d'autres infractions similaires, cette caractéristique n'est pas exigée, c'est notamment le cas du partage d'images représentant des abus sexuels commis sur des enfants. L'asymétrie entre ces deux infractions suggère une hiérarchisation problématique des violences numériques. **Ce choix sémantique peut alors être perçu comme le reflet d'une volonté restrictive du législateur européen, voire une forme de banalisation implicite des cyberviolences dont les femmes sont victimes.**

Par ailleurs, le Règlement (UE) 2021/784 a démontré qu'il était possible d'instaurer des mécanismes d'injonctions de retrait rapides et justifiés, accompagnés de mesures spécifiques visant à prévenir la diffusion de contenus illicites. Il serait donc pertinent que cette logique soit transposée à la Directive 2024/1385. **Cela rendrait envisageable que des fournisseurs hébergeant des plateformes pornographiques, ou des réseaux sociaux tels que Twitter ou Instagram - souvent utilisés pour la diffusion de contenus intimes sans consentement - soient désignés comme « exposés à des contenus à caractère sexuel ». Ces derniers seraient alors contraints de mettre en œuvre des actions spécifiques pour empêcher la diffusion de contenus intimes, y compris manipulés, sans le consentement des personnes concernées.**

Au niveau national ensuite, une formulation suscite elle aussi des interrogations : il s'agit de l'expression « caractère sexuel », utilisée à l'article 226-2-1 du Code pénal . Le 30 juin 2021, le Conseil constitutionnel a justement été saisi d'une question prioritaire de constitutionnalité (QPC)[64] portant sur la conformité du deuxième alinéa de cette disposition aux droits et libertés garantis par la Constitution.

En se fondant sur l'absence de précisions relatives à ce qu'il faut entendre par parole ou images à « caractère sexuel », il était invoqué la méconnaissance du principe de légalité et

[63] Cour de cassation, Ch. civile. (2018). Arrêt n° 16-28.741.
[64] Conseil constitutionnel. (2021). Décision n°2021-933 QPC du 30 septembre 2021. Décision n° 2021-933 QPC du 30 septembre 2021 | Conseil constitutionnel.

de nécessité des délits et des peines. Si l'on peut en effet souligner le caractère subjectif et vague de cette notion, le Conseil constitutionnel a finalement déduit qu'elle était suffisamment claire et précise pour garantir contre le risque d'arbitraire. Elle laisse aux juridictions compétentes la libre appréciation du caractère sexuel des paroles et des images. **Il peut alors en résulter un risque de disparités jurisprudentielles.**

En complément, les modifications apportées par la « Loi SREN » de 2024, et notamment celles relatives à l'article 226-8 du Code pénal méritent d'être soulignées. Il apparaît de manière évidente que le législateur a souhaité intervenir pour « *procéder à une mise au goût du jour du seul délit présenté comme protégeant la représentation de la personne, le délit dit de montage* »[65]. Son intervention, tout comme celle de l'UE s'explique aussi par le contexte évoqué précédemment, et notamment l'apparition de l'intelligence artificielle et des « deepfakes » à caractère pornographique.

D'abord, l'article 15 de cette norme a, comme susmentionné, modifié le verbe « *publier* » sous prétexte que la notion était trop ambigüe et que la conception de publication s'imposant en matière de presse ne pouvait s'appliquer ici. Pour la doctrine, cette modification ne changera sans doute pas l'état du droit car la chambre criminelle de la Cour de cassation affirme depuis de nombreuses années déjà l'autonomie de la notion de publicité de l'article 226-8 du Code pénal par rapport à celle de l'article 23 de la loi du 29 juillet 1981. Elle estime en effet que **même une publicité « restreinte » effectuée sciemment est punissable**[66].

Ce sont des avancées positives qui laissent espérer que la France va suivre la lignée du Royaume-Uni, qui est par exemple parvenu à fermer un site diffusant des « deepfakes ». Reconnaissant l'insuffisance de ses outils juridiques, le pays a d'ailleurs décidé en janvier 2025 d'adopter des dispositions spécifiques visant à criminaliser explicitement la création et la diffusion de « deepfakes » sexuellement explicites sans consentement. C'est un des pays les plus au point sur ce thème avec la Corée du Sud[67].

L'article 5 de la Directive paraît donc avoir des équivalents assez favorables en droit français, notamment grâce aux apports de la « Loi SREN ». Il s'agit maintenant de voir ce qu'il en est de la traque furtive en ligne, aussi appelée « cyber stalking ».

[65] Bossan, J. (2024). « La protection de la représentation à l'ère du numérique et du deepfake : le délit de montage version 2.0 ». *Légipresse*, n°426, (p. 380-385).
[66] *Ibidem.*
[67] Osez le Féminisme et la CLEF. (2025). Colloque : « Exploitation sexuelle en ligne : enjeux et réponses européennes ». Strasbourg.

2. La traque furtive en ligne

2.1. Contexte

En 2021, la société Apple a commercialisé le premier « *AirTag* ». Il s'agit d'un dispositif qui peut se fixer n'importe où et qui permet de géolocaliser des objets perdus. Cependant, il peut être utilisé de façon malveillante, par exemple pour surveiller les déplacements de sa partenaire dans le cadre de violences conjugales[68], comportement qui entre dans le cadre de l'infraction dénommée « traque furtive en ligne ».

La « traque furtive en ligne » ou « cyberstalking » est une pratique consistant à utiliser les technologies de communication à des fins de surveillance, de menace, d'intimidation, ou encore pour communiquer aux victimes une intention de les blesser[69]. Bien qu'il n'existe pas de liste arrêtée des comportements compris dans l'appellation « traque furtive en ligne »[70], ceux qui sont le plus souvent reconnus comme tels sont la captation de messages et de mails mais aussi d'images de la victime, notamment à l'aide de logiciels espions[71].

Le caractère répété de ces comportements est ce qui va permettre d'identifier l'infraction[72]. En pratique, une telle caractérisation demeure cependant difficile puisqu'il doit être prouvé que différents comportements, examinés dans leur ensemble, constituent une traque, ce qui est d'autant plus difficile lorsqu'il y a plusieurs auteurs[73].

---

[68] Centre Hubertine Auclert. (2023). « Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyberviolences conjugales ». Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyberviolences conjugales | Centre Hubertine Auclert (consulté le 23 mai 2025).
[69] Adamson, D.M. et al. (2023). « Cyberstalking: A Growing Challenge for the U.S. Legal System ». RAND Corporation.
[70] Kobets, P. ; Krasnova, K. (2018). « Cyberstalking: Public danger, key factors and prevention ». *Przeglad Wschodnioeuropejski*, vol 9, n°2, (p. 43–53.).
[71] Adamson, D.M. et al. (2023). « Cyberstalking: A Growing Challenge for the U.S. Legal System » ; Dulaurans, M. (2024). « Violences en ligne: décrypter les mécanismes du cyberharcèlement ». Presses universitaires de Bordeaux.
[72] Kamara, I. (2023). « Cyberstalking and online platforms' due diligence in the EU Digital Services Act ». Tilburg University. https://research.tilburguniversity.edu/en/publications/cyberstalking-and-online-platforms-due-diligence-in-the-eu-digita
[73] *Ibidem.*

Le considérant 21 de la Directive 2024/1385 souligne que le plus souvent, les auteurs de traque furtive en ligne sont des proches de la victime, qu'il s'agisse de membres de la famille, d'anciens partenaires ou de connaissances. Il précise aussi que c'est une forme de violence qui sert à intensifier des comportements déjà existants de nature coercitive, dominatrice et manipulatrice. Les femmes sont les victimes principales de traque furtive en ligne puisqu'elles sont près de deux fois plus susceptibles que les hommes d'en faire l'expérience[74]. Au contraire, ces derniers sont majoritaires parmi les auteurs des faits[75]. Par ailleurs, les conséquences sur la vie des victimes sont importantes et variées : elles vont de coûts financiers relatifs à un déménagement jusqu'au développement de troubles de l'anxiété ou de troubles post-traumatiques[76].

2.2. Le cadre juridique européen

L'article 6 de la Directive 2024/1385 définit comme infraction le fait de placer une personne sous surveillance, de manière répétée ou continue, sans consentement ni autorisation légale, à l'aide de TIC, pour suivre et surveiller ses déplacements ou activités. C'est lorsque ce comportement est susceptible de causer un préjudice important à la personne concernée qu'il doit constituer une infraction pénale.

Le considérant 21 de ce texte précise que sont notamment visés les comportements de surveillance rendus possibles par le traitement des données à caractère personnel de la victime, comme par exemple un vol de mot de passe. Cependant, il établit dans le même temps une limite à la pénalisation de ces comportements puisqu'il énonce que la surveillance peut parfois être effectuée pour des motifs légitimes, c'est le cas notamment de la surveillance de la localisation des enfants par leurs parents.

La Directive 2024/1385 clarifie elle-même ce qui doit être entendu par « *suivre* » et « *surveiller* ». Le premier verbe fait référence à la localisation d'une personne et au suivi de ses

[74] Morgan, Rachel E ; Jennifer L. Truman. (2022). « Stalking Victimization, 2019 ». U.S. Department of Justice, Bureau of Justice Statistics.
[75] Dulaurans, M. (2024). *Op.cit.*
[76] Dreßing H. ; Bailer J. ; Anders A. ; Wagner H. ; Gallas C. (2014). « Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims ». *Cyberpsychology, Behavior, and Social Networking*, 17(2), (p. 61–67).

déplacements, alors que le second renvoie à une idée de surveillance plus globale, notamment à l'observation de ses activités. La finalité est la même dans les deux cas : il s'agit de contrôler la victime.

L'infraction de traque furtive en ligne est appréhendée par le droit européen actuel dans la mesure où elle constitue une **manifestation de la violence sexiste et engendre de graves conséquences sur le bien-être physique et mental des victimes.** De plus, bien que la traduction française du DSA ne parle que de « harcèlement en ligne » et non de traque furtive en ligne, la version anglaise de son considérant 12 inclut le « *online stalking* » au titre des contenus considérés comme illégaux. En conséquence, les obligations consacrées par le DSA en matière de contenus illégaux sont de nature à s'appliquer aux cas de traque furtive en ligne.

En tant que telle, la traque furtive en ligne se retrouve incluse dans le champ d'application des **articles 34 et 35 du DSA** qui imposent aux fournisseurs de plateformes en ligne de réduire les risques découlant de la conception de leurs services.

Les obligations des fournisseurs en matière de risques de survenance de traque furtive en ligne sont les mêmes que celles relatives au partage de matériels intimes sans consentement. Conformément au DSA, les fournisseurs d'hébergement ont l'obligation de signaler toute suspicion d'infraction pénale aux autorités compétentes si elles ont connaissance d'informations conduisant à soupçonner qu'une infraction pénale présentant une menace pour la vie ou la sécurité d'une ou plusieurs personnes a été commise, est en train d'être commise ou est susceptible d'être commise. **La traque furtive en ligne, en tant que menace pour la vie ou la sécurité des personnes, devrait relever des infractions que les fournisseurs doivent signaler.** De plus, sa présence dans la liste des contenus illicites du considérant 12 précité conduit les fournisseurs d'hébergement à s'assurer du retrait rapide ou de l'inaccessibilité des contenus pouvant correspondre à une traque furtive en ligne et leur ayant été notifiés[77]. Ils ont également l'obligation de mettre en place des mécanismes de notification et d'action facilement accessibles et faciles à utiliser[78].

[77]Voir considérant 22, *Digital Services Act,* 2022.
[78]Voir considérant 50, *Digital Services Act,* 2022.

2.3. Le cadre juridique français

En droit français, la traque furtive en ligne est englobée dans un premier temps par l'article 226-1 alinéa 3 du Code pénal qui encadre le délit de géolocalisation sans l'accord de la personne concernée. Il peut se traduire par l'installation de balises (sur les voitures ou dans des sacs, par exemple), ou d'un logiciel espion sur le téléphone. L'article prévoit de plus une circonstance aggravante lorsque les faits sont commis par le partenaire de la victime. Dans ce cas, les faits sont punissables de deux ans d'emprisonnement et de 60 000 euros d'amende.

L'installation d'un logiciel espion sur un téléphone, une tablette ou un ordinateur pour contrôler l'activité en ligne de la victime peut également être constitutif d'un délit d'atteinte aux systèmes de traitement automatisé de données (articles 323-1 à 323-3 du Code pénal). De plus, l'article 323-3-1 expose qu'est puni des mêmes peines le fait de détenir un dispositif permettant de commettre l'infraction de l'article 323-1.

L'article 226-15 du Code pénal, portant sur l'atteinte au secret des correspondances pourrait encadrer à la fois l'interception de données privées (SMS, emails, conversations en ligne) et l'installation d'un logiciel espion sur le téléphone, la tablette ou l'ordinateur pour contrôler les communications de l'autre personne et son activité en ligne. Effectivement, son deuxième paragraphe évoque « *l'installation d'appareils de nature à permettre la réalisation de telles interceptions* ». Ce comportement est puni d'un an d'emprisonnement et de 45 000 euros d'amende. De plus, cette norme prévoit une nouvelle fois une circonstance aggravante quand l'auteur du comportement est le partenaire de la victime, dans ce cas-là, la peine est de deux ans d'emprisonnement et de 60 000 euros d'amende.

2.4. Analyse

La définition de l'infraction de traque furtive en ligne donnée par la Directive 2024/1385 renvoie à l'absence de consentement de la victime à l'acte commis. Pour qualifier l'infraction, il semble alors nécessaire de cumuler l'acte spécifique avec la violation du consentement et la conséquence du préjudice. Non seulement ce cumul pour qualifier l'infraction peut restreindre le champ de l'action pénale mais le critère du « sans consentement » peut aussi être retourné contre les victimes dans des relations abusives. La Directive 2024/1385 ne prévoit que les cas

où la traque furtive en ligne s'exerce à la suite d'une première infraction telle que le vol, ou le piratage par exemple. Ainsi, le préambule du texte, au considérant 21, précise que « *cette surveillance peut être rendue possible par le traitement des données à caractère personnel de la victime, comme au moyen de l'usurpation d'identité, par le vol de mots de passe, par le piratage des équipements de la victime, par l'activation furtive de logiciels de capture des frappes pour accéder à leurs espaces privés, par l'installation d'applications de géolocalisation, notamment de logiciels de prédation, ou par le vol des équipements de la victime* ».

La formulation actuelle semble supposer que le consentement donné par la victime invalide la qualification de l'infraction. Cette approche ne permet pas de prendre en compte les cas où la victime aurait par exemple « consenti » à la remise de mots de passe, dans un cadre où ce consentement serait vicié par de la pression affective, du chantage émotionnel ou encore de la manipulation. De plus, une femme peut avoir autorisé l'accès à ses données ou comptes à un moment donné, sans consentir à une utilisation détournée et qui dure dans le temps. Ainsi, le fait d'avoir « autorisé » l'accès aux données ou comptes ne signifie pas que ce consentement est juridiquement libre et éclairé, notamment dans des contextes d'emprise ou de domination psychologique. Lors de la transposition, il conviendrait ainsi de mieux préciser cette notion et notamment de préciser que le consentement n'est valable que s'il est donné en dehors de tout moyen de pression, de coercition ou de dépendance.

Par ailleurs, l'article 6 de la Directive 2024/1385 contient une référence au préjudice causé à la victime comme élément de définition. Les faits commis doivent « *être susceptibles de [lui] causer un préjudice important* ». Or le texte ne propose pas de méthode harmonisée pour évaluer ce préjudice. De surcroît, la notion de « préjudice important » n'est pas définie et peut conduire à restreindre l'action pénale ou mener à des jurisprudences disparates. Le risque d'une telle formulation est que des cas graves - un isolement, une perte d'autonomie ou encore une angoisse continue - ne soient pas considérés comme correspondant à un « préjudice important ». L'infraction est définie au regard du préjudice provoqué à la victime, et non de manière autonome. Il conviendrait de reformuler cette terminologie ou, a minima, d'en préciser les contours lors de la transposition.

Une Directive doit avoir une base légale précise : l'article 83 du TFUE dispose qu'elles peuvent établir « *des règles minimales relatives à la définition des infractions pénales et des sanctions*

dans des domaines de criminalité particulièrement grave revêtant une dimension transfrontière ». Ainsi, le préambule de la Directive 2024/1385 que l'objectif est de « *fixer des règles minimales uniquement pour les formes les plus graves de cyberviolence, les infractions correspondantes définies dans la présente Directive sont limitées aux comportements susceptibles de causer un préjudice important ou un préjudice psychologique important à la victime, ou aux comportements susceptibles de conduire la victime à craindre sérieusement pour sa propre sécurité ou celle des personnes à charge* ». La notion de préjudice important est donc utilisée pour justifier la gravité des actes, et ainsi légitimer la nécessité de la Directive 2024/1385. Cependant, il revient aux Etats membres lors de la transposition de rendre effective la répression, et la France devrait envisager de retenir une formulation plus souple pour remplacer celle de « préjudice important ».

En droit français, il n'existe pas d'infraction autonome définissant et sanctionnant la traque furtive en ligne. Pour autant, le champ couvert par l'article 6 de la Directive 2024/1385 se retrouve dans plusieurs dispositions du Code pénal qui prévoient d'ailleurs, pour la plupart, depuis la promulgation de la Loi n°2020-936[79], une circonstance aggravante lorsque le comportement est commis par le partenaire de la victime. Cependant, alors qu'en droit français, ces infractions recouvrent des comportements très précis : géolocalisation, atteinte aux systèmes de traitement automatisé de données et atteinte au secret des correspondances, l'article 6 de la Directive 2024/1385 mentionne de manière plus large un comportement intentionnel visant « *à placer une personne sous surveillance de manière répétée ou continue* » sans son consentement ou de « *suivre ou contrôler* » ses déplacements et activités. **Il apparaît clairement que c'est un périmètre d'application très large auquel les dispositions françaises ne sont pas suffisamment alignées de par leur champ beaucoup plus restreint.**

Cependant, du fait de la promulgation très récente de la Loi de 2020, plusieurs décisions de justice ont pu reconnaître l'utilisation de la géolocalisation ou de l'atteinte au secret des correspondances comme un élément constitutif du contrôle coercitif. La notion a été consacrée très récemment comme schéma des violences conjugales, dans cinq arrêts rendus par la Cour d'appel de Poitiers le 31 janvier 2024, dont l'un d'entre eux a condamné le conjoint de la victime pour avoir exercé un contrôle coercitif en surveillant tous ses déplacements grâce à des dispositifs électroniques. C'est un terme qui est déjà érigé en infraction dans plusieurs pays

[79] Loi n°2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

anglo-saxons (Angleterre, Pays de Galle, Irlande, etc.) mais qui fait toujours l'objet de vifs débats en France. Dans ces décisions, le contrôle coercitif est défini comme « *une atteinte aux droits humains en ce qu'il empêche la victime de jouir de ses droits fondamentaux* », comme notamment de la liberté d'aller et de venir ou d'entretenir des liens sociaux[80]. De même, la Cour identifie « *les outils du contrôle coercitif* » qui sont « *un ensemble d'actes tendus vers le même objectif de contrôle et d'assujettissement de la victime et qui, sans cette notion commune, seraient traités de manière isolée, voire seraient ignorés*. ». Comme le contrôle coercitif n'est pas encore une qualification pénale, les arrêts caractérisent en tous leurs éléments chaque infraction pour ensuite les replacer dans un contexte global de contrôle coercitif[81]. Ainsi, ce concept, tel qu'entendu par la jurisprudence française, pourrait être appliqué à la traque furtive en ligne, comblant alors le vide législatif existant.

Par ailleurs, dès 2023, la ministre chargée de l'égalité entre les hommes et les femmes, Isabelle Rome, a souhaité faire entrer dans le Code pénal cette notion de contrôle coercitif, tel que résultant des travaux du sociologue américain, Evan Stark[82]. C'est à dire désignant « *le recours à la force ou aux menaces* » et recouvrant « *les formes structurelles de privation qui contraignent indirectement à l'obéissance en monopolisant ressources vitales, dictent les choix préférés, micro-régulent le comportement de la partenaire, limitent ses options et la privent des soutiens nécessaires pour exercer un jugement indépendant* »[83]. Cette volonté s'inscrit sans doute dans un objectif de mise en conformité avec la décision du 14 décembre 2021 Tunikova et autres contre Russie, de la Cour européenne des droits de l'homme (CEDH)[84], dans laquelle les juges ont pointé les lacunes des droits nationaux[85] quant à l'appréhension, grâce au contrôle coercitif, des violences faites aux femmes comme des atteintes à leurs droits fondamentaux[86]. Le 3 avril 2025, le Sénat a adopté en première lecture la proposition de loi n°669 du 3 décembre

[80] Muller, Y. (2024). « Consécration de la notion de contrôle coercitif… Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire ». *Le club des juristes.* Consécration de la notion de contrôle coercitif…. Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire - Le Club des Juristes.
[81] *Ibidem.*
[82] Stark, E. (2023). « Coercive Control : How Men Entrap Women in Personal Life ».
[83] *Ibidem.*
[84] Cour européenne des droits de l'homme. (2021). *Arrêt Tunikova et autres contre Russie*. TUNIKOVA AND OTHERS v. RUSSIA.
[85] Greffière de la CEDH. (2021). Communiqué de presse « Manquements, constitutifs de violations, à l'obligation de traiter les cas de violences domestiques ; modifications législatives requises de toute urgence ». Elle invitait notamment le gouvernement russe à « *introduire dans son droit interne une définition de la violence domestique couvrant les manifestations de comportements de contrôle et de coercition ainsi que les faits de traque et de harcèlement, qu'ils aient lieu physiquement ou en ligne* ».
[86] Hardouin-Le-Goff, C. (2023). « L'incrimination du contrôle coercitif, futur outil de lutte contre les violences conjugales? ». *Le club des juristes.* L'incrimination du contrôle coercitif, futur outil de lutte contre les violences conjugales ? - Le Club des Juristes.

2024 visant à renforcer la lutte contre les violences sexuelles et sexistes. Le texte, tel que modifié par les députés, prévoyait la création d'un nouveau délit de contrôle coercitif, s'inscrivant directement dans la continuité des arrêts de Poitiers, mais il a été supprimé par les sénateurs « *craignant une censure constitutionnelle au regard de la fragilité des notions de peur et de crainte* »[87], qui figuraient dans la définition. Cependant, dans la version du Sénat, sont maintenus les éléments constitutifs d'une attitude coercitive, puisqu'y est défini le délit de harcèlement sur conjoint comme « *les propos ou comportements répétés ayant pour objet ou pour effet de restreindre gravement la liberté d'aller et venir de la victime ou sa vie privée et familiale ou de contraindre sa vie quotidienne par des menaces ou des pressions psychologiques, économiques ou financières* »[88]. Si nous pouvons regretter la mention en tant que telle de « *contrôle coercitif* », les « *comportements répétés ayant pour objet ou pour effet de restreindre gravement la liberté d'aller et de venir de la victime* », pourraient sans trop de difficultés inclure les agissements entrant dans le cadre de la traque furtive en ligne, comme notamment l'utilisation de dispositifs de géolocalisation.

Cependant, une incrimination autonome du contrôle coercitif incluant de manière plus détaillée toutes formes de violence, comme proposé au départ par l'Assemblée Nationale le 28 janvier 2025 dans l'article 3 de la proposition de loi, permettrait de prendre en compte « *l'intention unique de l'auteur de contrôler et soumettre la victime* »[89] , la réponse pénale serait alors plus adaptée et le champ de l'article 6 de la Directive 2024/1385 mieux couvert.

> « *Art. 222-14-3-1. – Sans préjudice de l'application des articles 223-15-3 et 222-33-2-1 du code pénal, le fait d'imposer un contrôle coercitif sur la personne de son conjoint, du partenaire auquel on est lié par un pacte civil de solidarité ou de son concubin, par des propos ou des comportements répétés ou multiples, portant atteinte aux droits et libertés fondamentaux de la victime ou instaurant chez elle un état de peur ou de contrainte dû à la crainte d'actes exercés directement ou indirectement sur elle-même ou sur autrui, que ces actes soient physiques, psychologiques, économiques, judiciaires, sociaux, administratifs, numériques ou de toute autre nature, est puni de trois ans d'emprisonnement et de*

[87] Vie publique. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexistes et sexuelles ». Violences sexuelles et sexistes Contrôle coercitif Viol Proposition loi | vie-publique.fr.
[88] *Ibidem.*
[89] Muller, Y. (2024). « Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! ». *Le club des juristes.* Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! - Le Club des Juristes.

45 000 € d'amende lorsque ces faits ont causé une incapacité totale de travail inférieure ou égale à huit jours ou n'ont entraîné aucune incapacité de travail. »

[Article 3 de la proposition de loi visant à renforcer la lutte contre les violences sexistes et sexuelles[90]]

3. Le cyberharcèlement

[90] Assemblée Nationale. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexuelles et sexistes ».

3.1. Contexte

Le GREVIO, dans un rapport sur la dimension numérique de la violence à l'égard des femmes[91], affine la définition du harcèlement, pour inclure la dimension numérique. Ainsi, il énonce que l'article 34 de la Convention d'Istanbul[92] doit inclure les faits de harcèlement à l'aide d'utilisation des TIC, pour garantir une protection effective de la Convention :

> *« 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 établissement scolaire,* ***de même que la suivre dans un monde virtuel (espaces de discussion, sites des réseaux sociaux, etc****.) ».*

Le président de la 77ème Assemblée Générale des Nations Unies (de septembre 2022 à septembre 2023) a affirmé que « *les femmes sont 20% moins susceptibles que les hommes d'utiliser l'Internet, mais 27 fois plus susceptibles d'être victimes de harcèlement ou de discours de haine en ligne, lorsqu'elles le font* »[93].

Selon l'Agence pour les droits fondamentaux de l'Union européenne dans son étude sur les violences à l'égard des femmes[94], **1 jeune femme sur 5 déclare avoir été victime d'au moins un cyberharcèlement d'ordre sexuel depuis l'âge de 15 ans** et 1 adolescente sur 4 déclare être victime d'humiliations et de harcèlement en ligne concernant son attitude, son apparence physique ou son comportement amoureux ou sexuel.

---

[91] Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO). (2021). « Recommandation générale n°1 sur la dimension numérique de la violence à l'égard des femmes ». https://rm.coe.int/reccomandation-no-du-grevio-sur-la-dimension-numerique-de-la-viomence-/1680a49148

[92] Conseil de l'Europe. (2011). « Convention sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique ». STCE 210 - Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique.

[93] Csaba, K. (2023). « Message lors de la 67e session de la Commission de la condition de la femme, ONU ».

[94] Agence des droits fondamentaux de l'UE. (2014). Rapport: « La violence à l'égard des femmes : une enquête à l'échelle de l'UE ». https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-factsheet_fr.pdf.

3.2. Le cadre juridique européen

Le cyberharcèlement est visé à l'article 7 de la Directive 2024/1385. L'article liste les actes constitutifs de l'infraction de cyberharcèlement et devant être pénalement sanctionnés par les Etats membres de l'Union européenne au niveau national. Parmi ces actes figurent le fait de menacer une personne, seul ou à plusieurs, à l'aide de TIC, le « *cyberflashing* »[95] et le « *doxing* »[96].

Étant donné que le considérant 12 du DSA classe le harcèlement en ligne parmi les contenus illégaux, les obligations relatives à ces contenus s'appliquent[97]. Notamment, en accord avec le considérant 22 du même texte, **les fournisseurs de services ont une obligation de retrait prompte de ce type de contenu.** Ils doivent également, en vertu du considérant 50, mettre en place des **mécanismes de signalement ou de « notification » des contenus illégaux.**

Les articles 4, 5 et 6 du DSA listent les exceptions au principe de responsabilité des fournisseurs de services. L'article 6 prévoit notamment une exonération de responsabilité pour les fournisseurs de services en tant qu'hébergeurs de contenus illicites, à condition qu'ils **n'aient pas eu connaissance** de la présence de ces contenus, ou qu'ils aient **agi promptement** pour les retirer dès qu'ils en ont eu connaissance. À défaut, leur responsabilité peut être engagée. Toutefois, l'article 8 précise que « *les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni de rechercher activement des faits ou des circonstances révélant des activités illégales* ». Cette disposition limite donc fortement leur obligation de vigilance, et risque ainsi de **réduire la portée effective du règlement.** La responsabilité du fournisseur peut également être engagée en accord avec l'article 18 du DSA si celui-ci n'a pas informé les autorités compétentes au sujet d'un contenu illicite qu'il aurait hébergé. Ici par exemple, **si un fournisseur héberge un contenu pouvant s'apparenter à du doxing ou à tout contenu visé à l'article 7 de la**

[95] Parlement européen et Conseil. (2024). *Op.cit.*, considérant 24. « *Envoi non sollicité d'une image, d'une vidéo ou d'un autre matériel similaire représentant des organes génitaux à une personne* ».
[96] *Ibidem.* « *Les informations à caractère personnel de la victime sont mises à la disposition du public au moyen des TIC, sans le consentement de la victime, dans le but d'inciter d'autres personnes à causer un préjudice physique ou un préjudice psychologique important à la victime* ».
[97] Parlement européen et Conseil. (2022). *Op. cit.*, considérant 22. « *Il peut s'agir, par exemple, du partage d'images représentant des abus sexuels commis sur des enfants, du partage illégal d'images privées sans consentement, du harcèlement en ligne…* ».

Directive 2024/1385, **et cela sans en avertir aucune autorité, alors sa responsabilité pourrait être engagée sur la base de l'article 18.**

Quant à l'évaluation des risques relatifs au fonctionnement des services, les articles 34 et 35 dont les dispositions sont détaillées dans les sections précédentes sont applicables ici puisque non seulement le contenu publié aux fins de cyberharcèlement[98] est illicite mais de surcroît, il entraîne un effet négatif relatif à la violence sexiste, ainsi que des conséquences négatives graves sur le bien-être physique et mental des personnes. **Les fournisseurs doivent donc évaluer les risques de survenance du cyberharcèlement et prendre des mesures pour les atténuer.**

3.3. Le cadre juridique français

Afin de pouvoir appréhender au mieux la transposition de la Directive 2024/1385, il convient d'étudier le cadre juridique pénal en droit français concernant les infractions de cyberharcèlement.

Au vu des éléments précités, le cyberharcèlement est une violence aux aspects divers, s'inscrivant dans un contexte plus global de « *violences facilitées par les outils technologiques* » aux implications multiformes et aux conséquences nombreuses, qu'on ne saurait aborder sous le seul angle de l'article 222-33-2 du Code pénal. Nous étudierons les nombreuses infractions qui sont susceptibles de faire partie de cette catégorie.

Le cyberharcèlement « classique », « moral » constitue un délit réprimé par l'article 222-33-2 du Code pénal. L'utilisation d'outils numériques constitue un élément aggravant : le cyberharcèlement est donc puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

L'article 222-33-2-1 incrimine « *le fait de harceler son conjoint, son partenaire lié par un pacte civil de solidarité ou son concubin par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération*

[98] Parlement européen et Conseil. (2024). *Op. cit,* considérant 24. Par exemple, comme précité, le partage d'informations personnelles de la victime au moyen de TIC dans le but d'inciter d'autres personnes à lui causer un préjudice.

de sa santé physique ou mentale ». Cela concerne également les faits commis par un ancien conjoint, ancien concubin ou ancien partenaire lié par un pacte civil de solidarité.

Le cyberharcèlement sexuel est un délit réprimé par l'article 222-33 du Code pénal : « *le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante* ». L'alinéa 6 du III de cet article aborde l'utilisation d'un service de communication au public en ligne ou d'un support numérique ou électronique comme une circonstance aggravante car les peines d'emprisonnement passent de deux à trois ans.

Ces deux infractions sont constituées lorsque ces propos 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. Mais l'infraction est également caractérisée lorsque ces 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 (article 222-33 et article 222-33-2-2). Le législateur, par la loi du 3 août 2018[99] a souhaité lutter contre le cyberharcèlement groupé, également appelé « raid numérique ». Aux termes d'un arrêt en date du 29 mai 2024[100], la chambre criminelle de la Cour de cassation a apporté des précisions intéressantes sur la caractérisation du délit de cyberharcèlement. D'après la Cour, le simple fait de retenir que le prévenu avait connaissance que l'acte qu'il commettait s'inscrivait dans une répétition suffit et dès lors, les juges du fond n'étaient pas tenus d'identifier, dater et qualifier l'ensemble des messages émanant d'autres personnes et dirigés contre la partie civile. Il n'est pas nécessaire non plus de vérifier que le message du demandeur a été effectivement lu par la personne visée. Il en résulte que le fait de publier en ligne un seul message malveillant, dirigé contre une personne qui fait l'objet d'insultes et de menaces sur les réseaux sociaux, peut caractériser l'infraction.

L'alinéa d) de l'article 7 de la Directive 2024/1385 dispose que constitue un cyberharcèlement: « *d) le fait de rendre accessible au public, au moyen de TIC, du matériel contenant les données à caractère personnel d'une personne, sans le consentement de cette dernière, dans le but*

[99] Loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexistes et sexuelles.
[100] Cour de Cassation, chambre criminelle. (2024). Arrêt n°23-80.806.

d'inciter d'autres personnes à causer un préjudice psychologique important ou un préjudice physique à cette personne ».

Cette infraction, communément appelée le « *cyberdoxing* », consiste à dévoiler l'identité d'un internaute et menacer sa vie privée. Les informations concernées par le doxing peuvent être diverses ; il peut s'agir de la diffusion de l'adresse électronique, du numéro de téléphone, des noms et prénoms ou encore des informations sur la vie professionnelle. Ces actes portent atteinte à la vie privée de la personne ciblée et illustrent parfaitement l'idée selon laquelle les violences en ligne s'inscrivent dans le prolongement direct des violences exercées hors ligne, formant un continuum. Ainsi, l'article 223-1-1 du Code pénal sanctionne de trois ans d'emprisonnement et de 45 000 euros d'amende « *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 de la localiser aux fins de l'exposer ou d'exposer des membres de sa famille à un risque direct d'atteinte à la personne ou aux biens que l'auteur ne pouvait ignorer* ».

L'article 226-1 a déjà été mentionné auparavant concernant le partage non consenti de matériels intimes ou manipulés, mais il convient de le citer à nouveau et notamment son alinéa 3° qui dispose : « *en captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci* ».

De plus, l'article 226-4-1 réprime le « *fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération* », notamment commise sur un réseau de communication.

L'envoi réitéré de messages malveillants ou d'appels téléphoniques malveillants (article 222-16 du Code pénal) peut également être considéré dans ce contexte. Ces faits contribuent à créer une atmosphère d'insécurité permanente à travers les outils de communication. Lorsque ces faits sont commis par conjoint, concubin ou partenaire lié à la victime par un pacte civil de solidarité, la peine encourue est de 3 ans d'emprisonnement et de 45 000 euros d'amende. De même, le délit de collecte frauduleuse des données personnelles est réprimé par l'article 226-18, et la commission de ces faits fait encourir 5 ans d'emprisonnement et 300 000 euros d'amende.

3.4. Analyse

La rédaction du délit de harcèlement moral en droit pénal français est décriée par certains auteurs qui condamnent les formules opaques employées par le législateur telles que les « *agissements répétés* » ou la « *dégradation des conditions de vie et l'altération de la santé physique ou mentale* ». L'acte de harcèlement moral doit être susceptible de produire les conséquences visées par la loi : à savoir « *une dégradation des conditions de vie de la victime se traduisant par une altération de la santé physique ou mentale* ». Ainsi, la loi pose une double exigence pour caractériser l'infraction : **il faut non seulement démontrer l'existence d'une dégradation des conditions de vie, mais encore faut-il que cette dégradation porte atteinte à la santé physique ou mentale de la victime.** Cela a été confirmé par un arrêt de la chambre criminelle de la Cour de cassation en date du 9 mai 2018[101]. En effet, cette dernière avait considéré que les juges de la Cour d'appel n'étaient pas parvenus à caractériser en quoi les actes reprochés au prévenu ont eu pour objet ou pour effet une dégradation des conditions de vie de la victime se traduisant par une atteinte à sa santé physique ou mentale. Cette décision indique qu'il est nécessaire de prouver l'existence d'une altération de la santé physique ou mentale de la victime, retenant ainsi une approche matérielle de l'infraction. Cela est quelque peu regrettable dans la mesure où elle revient à démentir l'idée que « *la répression ne peut dépendre de la capacité de résistance de la victime du harcèlement moral* »[102].

De nombreux auteurs considèrent que cet article ne remplit pas « *l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi consacré par une décision du conseil constitutionnel en date du 16 décembre 1999* »[103].

Il serait donc intéressant de revoir la rédaction de cet article dans le cadre d'une transposition de la Directive 2024/1385.

Dans la Directive 2024/1385, l'article 7 met en place des seuils de pénalisation. Pour le « cyberflashing », le « doxing » et les « menaces en groupe », doivent être pénalisés au minimum les comportements susceptibles de causer un préjudice psychologique important à la victime.

[101] Cour de cassation, Chambre criminelle. (2018). Arrêt n° 17-83.623.
[102] Segonds, M. (2014). « Un an de droit pénal du travail », *Dr. pénal. chron. 10.*
[103] Chauvet, D. (2015). « Mérites ou démérites du délit général de harcèlement moral créé par la loi du 4 août 2014 ? ». *Recueil Dalloz*, 2015, (page 174).

Pour les comportements menaçants auxquels est consacré le paragraphe a), devront être pénalisés au minimum les menaces relatives à la commission d'infractions pénales si celles-ci sont susceptibles de faire naître chez la victime une crainte pour sa sécurité ou pour celle des personnes à sa charge.

Bien que cette disposition impose aux États de sanctionner les actes de cyberharcèlement, le texte, comme l'indique son considérant 24, met surtout à leur charge **une obligation de mettre en œuvre des règles minimales couvrant les formes les plus graves de cyberharcèlement.** Entre autres, sont visées les formes de cyberharcèlement que la Directive 2024/1385 considère comme susceptibles de causer des préjudices psychologiques importants. Elle donne à ce titre l'exemple des attaques en groupe ou du harcèlement ayant lieu partiellement hors ligne[104]. L'article contient une référence au préjudice causé à la victime comme élément de définition. Les faits doivent être « *susceptibles de causer un préjudice important* » à la victime. Cependant, **la Directive 2024/1385 ne propose pas de méthode harmonisée pour évaluer ce préjudice. La notion de préjudice psychologique grave étant sujette à interprétation, la condition posée par cet article peut représenter un obstacle pour les personnes faisant valoir leur qualité de victime.**

[104] Parlement européen et Conseil. (2024). *Loc cit.*

4. L'incitation à la violence ou à la haine en ligne

4.1. Contexte

L'incitation à la haine désigne « *tout acte, attitude, ou comportement qui exhorte à la haine d'autrui* »[105] ou plus précisément qui exhorte à la prise de mesures contre un individu ou un groupe[106]. Si sa forme la plus connue aujourd'hui reste l'incitation à la haine raciale[107], nombre de pays, y compris la France, ont reconnu l'existence de l'incitation à la haine fondée sur la religion, l'orientation sexuelle et le handicap[108]. Les personnes les plus touchées par ce phénomène sont les membres de groupes minoritaires[109]. Toutefois, en tant que cibles des violences sexistes et sexuelles, les femmes et les filles en sont également des victimes récurrentes[110].

Cette pratique, lorsqu'elle a lieu en ligne, est exacerbée par la survenance d'événements ou de conflits rapportés par les médias. Elle peut être cause de peur et d'angoisse pour les personnes ciblées. Malgré ces conséquences, le retrait de propos et contenus incitant à la haine dépend encore de la bonne volonté des fournisseurs de service et l'engagement d'une procédure pénale contre des utilisateurs anonymes reste complexe en pratique[111].

Le paragraphe 25 du préambule de la Directive 2024/1385 énonce que l'utilisation des outils de communication, d'internet et des réseaux sociaux a entraîné une forte augmentation de l'incitation à la violence, notamment celle fondée sur le genre. L'effet d'anonymat offert par ces outils renforce la diffusion facile de contenus haineux. Les femmes sont donc souvent la

[105] Cammillieri-Subrenat, A. (2002). « L'incitation à la haine et la Constitution ». *Revue internationale de droit comparé*. vol. 54. n°2. pp. 513-548.
[106] Gordon, G.S. (2013). « Hate Speech Persecution: A Contextual Approach ». *Vanderbilt Journal of Transnational Law*. vol. 303. n° 2. pp. 303-373.
[107] Demaske, C. (2023). « L'opérationnalisation des discours de haine à l'échelle de la communauté. Un plan de lutte contre les discours de haine ». *Réseaux,* vol. 241. n°5. pp. 197-235.
[108] *Ibidem*.
[109] Nations Unies. « Discours de haine : Incidence et prévention : Cibles de la haine ». Disponible : https://www.un.org/fr/hate-speech/impact-and-prevention/targets-of-hate (consulté le 23 mai 2025).
[110] Nations Unies. *Ibidem.*
[111] Humanrights.ch.. (2016). « Incitation à la haine sur Internet – Cas suisses et politique des portails d'informations en la matière ». https://www.humanrights.ch/fr/pfi/droits-humains/droits-politiques/incitation-haine-internet-cas-suisses-politique-portails-informations (consulté le 23 mai 2025).

cible de discours de haines sexistes en ligne, qui peuvent conduire à des crimes et délits hors ligne.

4.2. Le cadre juridique européen

4.2.1. Digital Services Act

Le considérant 12 du DSA classe les « *discours haineux illicites* » parmi les contenus qualifiés d'illicites. Il est ensuite précisé au considérant 40 que, pour garantir un environnement en ligne sûr et transparent, il est nécessaire de mettre en œuvre des mesures visant à assurer la sécurité et la confiance des utilisateurs du service, notamment les consommateurs, les mineurs, ainsi que les personnes particulièrement vulnérables aux discours haineux. Bien que, comme mentionné précédemment, ces considérants ne soient pas juridiquement contraignants, ils servent de guide pour interpréter les objectifs et la portée du texte législatif.

Tel que mentionné auparavant, les articles 34 et 35 du DSA obligent les fournisseurs de plateformes en ligne à **analyser et évaluer les risques systémiques présents sur leur plateforme, et à mettre en place des mesures pour les atténuer.** Parmi ces risques, on retrouve spécifiquement « *tout effet négatif réel ou prévisible lié aux violences sexistes* »[112].
La violence sexiste, qui selon un état des lieux du Parlement européen désigne **toute forme de violence dirigée contre une femme en raison de son sexe ou qui touche les femmes de manière disproportionnée**[113], peut inclure l'incitation à la haine ou à la violence à leur encontre. L'incitation à la haine sexiste constitue une violence sexiste en ce qu'elle affaiblit la liberté d'expression des femmes, en ce qu'elle a pour but de les humilier, de les objectifier, de sous-estimer leurs compétences et opinions, de détruire leurs réputations, de les rendre vulnérable et craintives, et de les punir pour n'avoir pas suivi certains comportements[114]. Les conséquences sévères de cette pratique qu'elles soient psychologiques, émotionnelles ou

[112] Parlement européen et Conseil. (2022). *Op.cit.*, article 34 d).
[113] Parlement européen. (2020). « La violence envers les femmes dans l'Union européenne : État des lieux ».
[114] Conseil de l'Europe. *Factsheet on Combating sexist hate speech*. p. 5.

physiques[115] la font figurer au titre des violences sexistes telles que définies par 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 : *« le terme « violence à l'égard des femmes » doit être compris comme une violation des droits humains et une forme de discrimination à l'égard des femmes, désignant tous les actes de violence fondés sur le genre qui entraînent ou sont susceptibles d'entraîner pour les femmes un préjudice ou des souffrances de nature physique, sexuelle, psychologique ou économique. »*.

A ce titre et en rappelant que le discours de haine sexiste en ligne peut également être à l'origine de crimes haineux hors ligne, le considérant 25 de la Directive 2024/1385 énonce : *« Il convient de prévenir ou de faire cesser ce comportement à un stade précoce. Le langage utilisé dans ce type d'incitation ne renvoie pas toujours directement au genre de la personne ciblée, mais la motivation partiale peut être déduite de la teneur générale ou du contexte de l'incitation. ».*

De façon plus générale, le Conseil de l'Europe définit le sexisme comme : *« toute expression (y compris en ligne) qui véhicule l'idée qu'une personne est inférieure en raison de son sexe »*[116]. Bien que la Convention européenne des droits de l'Homme soit un instrument non contraignant, les Etats parties, y compris la France, sont les destinataires des recommandations du Conseil de l'Europe. Ils doivent donc, selon ces dernières, lutter contre les discours sexistes dans les médias, l'espace public, l'éducation, les tribunaux, et donc contre le discours de haine sexiste en ligne en ce qu'il constitue une violence sexiste.

Ainsi, en vertu du DSA, les fournisseurs de plateformes sont soumis à une série d'obligations qui couvrent indirectement l'incitation à la haine et à la violence à l'égard des femmes, cette dernière étant considérée comme une forme de violence sexiste.

4.2.2. Code de conduite de 2016

Pour lutter contre la prolifération des discours haineux à caractère raciste et xénophobe en ligne, la Commission européenne, en collaboration avec quatre grandes entreprises des technologies de l'information (Facebook, Microsoft, Twitter et YouTube), a présenté le 31 mai

[115] *Ibid.*
[116] Conseil de l'Europe. (2019). « Recommandation sur la prévention et la lutte contre le sexisme ». CM/Rec(2019)1.

2016 un « code de conduite pour la lutte contre les discours haineux illégaux en ligne ».

Depuis, d'autres plateformes telles qu'Instagram, Snapchat, Dailymotion, TikTok, LinkedIn, et Twitch (au printemps 2022)[117], ont également décidé d'appliquer ce code. Le code de conduite est un **engagement volontaire** des plateformes en ligne, et non un instrument juridiquement contraignant destiné aux Etats membres.

Il incite les entreprises des technologies de l'information à adopter des procédures claires et efficaces pour prévenir et empêcher la diffusion de discours haineux sur leur service. Les discours haineux illégaux y sont définis comme « *toute incitation publique à la violence ou à la haine visant un groupe de personnes ou un membre d'un tel groupe, défini par référence à la race, la couleur, la religion, l'ascendance, l'origine nationale ou ethnique* »[118]. **Ils n'incluent pas les discours haineux à caractère sexiste.**

Ces procédures visent, entre autres, à examiner les signalements valides pour ensuite **retirer ou bloquer les contenus illégaux dans un délai de 24 heures**. Pour s'assurer de la validité des signalements, les entreprises doivent vérifier que **les signalements de contenus incitant à la violence et aux comportements haineux proviennent d'expert-es, notamment au moyen de partenariats avec des organisations de la société civile partenaires d'un réseau de « signaleurs de confiance » communiqué par la Commission.**

Une évaluation réalisée par la Commission européenne en 2022[119] a révélé qu'en moyenne, 69,6 % des contenus incitant au meurtre ou à la violence contre les groupes précités, ont été supprimés. 59,3 % des contenus diffamatoires à l'encontre de ces groupes ont été retirés.

Ce code établit donc un cadre avec des lignes directrices précises pour les plateformes, contribuant à prévenir et sanctionner les discours de haine. Dans le cadre de la transposition de la Directive, une initiative similaire pourrait être envisagée pour lutter contre les incitations à la violence et à la haine ciblant spécifiquement les femmes et les filles. Toutefois, les mesures de ce code s'appliquent uniquement aux plateformes qui le souhaitent, et ne sont pas

[117] Commission européenne. (2022). Communiqué de presse : « Code de conduite de l'UE contre les discours haineux en ligne: la dernière évaluation montre un ralentissement des progrès ».
[118] Conseil de l'Union européenne. (2008). « Décision-cadre 2008/913/JAI du 28 novembre 2008 relative à la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal ».
[119] Commission européenne. (2022). « Countering illegal hate speech online 7th evaluation of the Code of Conduct ».

contraignantes, ce qui rend ce cadre insuffisant pour lutter efficacement contre ce type de violence.

4.2.3. Décision cadre de 2008

La **Décision-cadre 2008/913/JAI**, relative à la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, a été adoptée par le Conseil de l'Union européenne en 2008. Son objectif principal est de criminaliser les comportements incitant à la haine et à la violence, et de veiller à ce que les États membres prennent des mesures efficaces pour lutter contre ces dérives, tant au niveau pénal qu'au niveau préventif. Bien que cette disposition ne crée pas de nouvelles infractions en soit, elle impose aux États membres des obligations de transposition afin que ces actes, notamment l'incitation à la haine et à la violence raciste et xénophobe, soient punissables à l'échelle nationale.

L'article premier de la décision-cadre précise que l'incitation publique à la violence ou à la haine, par des actes tels que la diffusion publique d'écrits ou d'images, doit être sanctionnée, notamment lorsqu'elle vise un groupe défini par référence à la race, la couleur, la religion, l'ascendance, l'origine nationale ou ethnique[120]. Bien que le texte se concentre initialement sur des groupes fondés sur des critères raciaux ou ethniques, **il est tout à fait envisageable d'étendre cette approche à la lutte contre les violences sexistes et à l'incitation à la haine et à la violence dirigée spécifiquement contre les femmes.**

Tout comme l'article 8 de la Directive 2024/1385, l'article premier de la décision-cadre adopte une approche restrictive en limitant l'obligation d'incrimination aux comportements susceptibles de troubler l'ordre public. Il est également prévu que l'incitation ou la complicité de commettre un tel acte soit punissable[121]. La décision-cadre renforce aussi la notion de responsabilité en prévoyant celle des personnes morales, entendues comme « *toute entité ayant ce statut en vertu du droit national applicable, exception faite des États ou des autres organismes publics dans l'exercice de prérogatives de puissance publique et des organisations*

[120] Conseil de l'Union européenne. (2008). *Op. cit.*, article premier.
[121] *Idem.* Article 2 et article 3,

internationales publiques »[122]. L'article prévoit que chaque État membre prenne les mesures nécessaires pour faire en sorte que les **personnes morales** puissent être tenues **pénalement responsables** des infractions commises pour leur compte par des personnes exerçant un pouvoir de direction. Elles peuvent aussi être responsables en cas de **défaut de surveillance** ayant permis ces actes. Cela n'exclut pas la responsabilité des individus impliqués[123]. Il est nécessaire de **rendre les personnes morales responsables d'incitation à la haine parce qu'elles ont souvent un rôle central dans la diffusion des messages** (comme les plateformes ou entreprises), et sans cela, elles pourraient se dédouaner de leur responsabilité de retirer les contenus haineux sans être sanctionnées. Cela permet aussi de les obliger à mettre en place des contrôles et à prévenir ces discours.

Une décision-cadre fixe des objectifs à atteindre, laissant aux États membres la liberté de choisir la manière de les réaliser. En France, par exemple, une proposition de loi visant à transposer la Décision-cadre 2008/913/JAI a été déposée le 6 février 2013[124] et pourrait servir de base d'inspiration pour une adaptation similaire. Cependant, la France ne peut pas être considérée comme un élève exemplaire en la matière : la proposition de loi déposée en 2013 pour transposer la décision-cadre était déjà marquée par une approche restrictive, et selon un rapport de la Commission européenne de 2014[125]. En effet, la décision-cadre a bien été prise en compte en France, mais sa transposition reste partielle et certains points ne sont pas complètement intégrés dans la législation nationale notamment concernant la responsabilité des personnes morales.

4.3. Le cadre juridique français

[122] *Idem*. Article 5.4.
[123] Conseil de l'Union européenne. (2008). *Op. cit.,* article 5.
[124] Proposition de loi de Mme Valérie BOYER et plusieurs de ses collègues tendant à la transposition en droit interne de la Décision-cadre 2008/913/JAI du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, n° 690, déposée le 6 février 2013.
[125] Commission européenne. (2014). « Rapport de la Commission au Parlement européen et au Conseil relatif à la mise en œuvre de la décision-cadre 2008/913/JAI du Conseil sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal ».

L'état actuel du droit pénal français dispose de quelques articles afin de lutter contre l'incitation à la violence. On peut à ce titre citer l'incitation à la haine raciale inscrite à l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse[126]. Cet article réprime notamment **la provocation publique sexiste** « *ceux qui auront provoqué à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap* », ainsi que l'incitation à la commission d'une infraction « *ceux qui auront directement provoqué à commettre des atteintes volontaires à la vie, des atteintes volontaires à l'intégrité de la personne et des agressions sexuelles* ».

Sont également prévues des circonstances aggravantes si l'infraction a été commise envers une personne en raison de son sexe, de son orientation sexuelle, de son identité de genre, ou encore de son handicap (articles 32 et 33).

4.4. Analyse

L'incitation à la violence ou à la haine en ligne fait l'objet d'une infraction pénale selon la Directive 2024/1385. Il est prévu à l'article 8 que : *« les États membres veillent à ce que l'incitation intentionnelle à la violence ou à la haine visant un groupe de personnes ou un membre de ce groupe, définie en référence au genre, en diffusant publiquement, au moyen des TIC, du matériel contenant une telle incitation soit passible de sanctions en tant qu'infraction pénale (1) ».*

En outre, « *aux fins du paragraphe 1, les États membres peuvent choisir de ne sanctionner que le comportement qui est soit exercé d'une manière qui risque de troubler l'ordre public, soit menaçant, injurieux ou insultant (2)* ». Le paragraphe 2 limite considérablement la portée de l'article et crée une marge d'appréciation permettant à certains États de ne sanctionner que les manifestations de haine les plus extrêmes ou visibles, excluant potentiellement des propos plus subtils, insidieux, mais néanmoins discriminants ou incitateurs à la haine.

[126] Loi du 29 juillet 1881 sur la liberté de la presse. (Version en vigueur depuis le 25 mai 2025).

Le considérant 25 de la Directive 2024/1385 souligne que le langage employé dans ce type d'incitation ne fait pas toujours explicitement référence au genre de la personne visée. Cela n'empêche toutefois pas de qualifier ces propos comme visant un groupe ou un individu en fonction du genre, car une motivation discriminatoire peut être déduite du contexte général ou de la teneur des propos incitatifs.

Une autre limitation, exposée dans le considérant 25, concerne la définition donnée de « *diffusion au public* ». En effet, il est précisé que ce champ inclut uniquement les situations où « *les utilisateurs cherchant à accéder à ces matériels sont enregistrés ou admis automatiquement, sans intervention humaine pour en décider ou pour sélectionner les utilisateurs auxquels l'accès est accordé* ». Or, cette distinction ne correspond pas à la réalité numérique : rien n'est véritablement privé sur Internet. **Cette restriction risque d'exclure des infractions graves, notamment celles commises sur des boucles privées, des applications de messagerie comme WhatsApp, ou encore des forums et conversations en ligne où circulent régulièrement des contenus non consentis.** Des boucles privées sur des réseaux sociaux peuvent parfois contenir des milliers de participants et risquent cependant d'être considérées comme des espaces virtuels non-publics, restreignant ainsi le champ d'application de cet article. C'est le cas par exemple de groupes Whatsapp ou Telegram, au sein desquels prospèrent la banalisation des agressions sexuelles, les appels au viol, les propos misogynes et racistes ainsi que le harcèlement[127]. Ces groupes, qui ont pu contenir jusqu'à 70 000 hommes[128], seraient difficile à appréhender en raison de leur caractère potentiellement privé alors même que, en plus de la violence y ayant lieu, ces derniers facilitent également la radicalisation[129] et donc la perpétration de violence hors ligne.

En limitant la reconnaissance de l'infraction à un cadre public, la Directive semble minimiser l'impact des violations de la vie privée des victimes. Elle sous-entend qu'une

[127] Garnier, P. (2024). « Mascus, les hommes qui détestent les femmes – Le documentaire ». *Made In Perpignan*. https://madeinperpignan.com/mascus-hommes-detestent-femmes-documentaire-tv/ (consulté le 22 juin 2025).
[128] Ouest France. (28 décembre 2024). « Sur Telegram des milliers d'hommes échangeaient des conseils pour droguer et violer des femmes ». https://www.ouest-france.fr/faits-divers/violence-sexuelle/viol/sur-telegram-des-milliers-dhommes-echangeaient-des-conseils-pour-droguer-et-violer-des-femmes-44497442-c537-11ef-a562-4e48a3fc537f (consulté le 22 juin 2025).
[129] Jaki S, De Smedt T, Gwozdz M, *et al.* (2019). « Online hatred of women in the Incels. me forum: Linguistic analysis and automatic detection ». *Journal of Language Aggression and Conflict*,, vol. 7, n°2, p. 240-268.

diffusion dans un espace privé serait moins préjudiciable, alors qu'en réalité, un contenu partagé en ligne, même dans un cadre restreint, échappe immédiatement au contrôle de la victime et devient irréversible.

Cette approche est en contradiction avec les principes protégés par la Convention européenne des droits de l'homme (CEDH), qui garantit le respect du droit à la vie privée et à la dignité.

La Directive 2024/1385 fait référence aux contenus accessibles « publiquement », risquant d'exclure donc les sites à abonnement de son champ, tel que Only Fans par exemple. Or, on constate que ces types de site servent d'écran à de nombreuses infractions. Selon le Mouvement du Nid, Only Fans participe à la banalisation de la sexualité marchande, mais constitue aussi un « lieu de repérage par les réseaux de proxénètes »[130], le proxénétisme des mineurs ayant d'ailleurs explosé ces dernières années, passant de 21 affaires en 2015 à 192 affaires en 2022[131]. Only fans est un service en ligne d'abonnement à des contenus, principalement utilisés pour du contenu pornographique, dans lequel des « créateurs de contenu » monétisent directement leurs publications auprès d'abonnés. L'article 3 (I) du Digital Service Act définit la plateforme en ligne comme « *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* ». Only fans est un service d'hébergement avec une fonction interactive, et devrait être considérée comme une plateforme en ligne, au regard de cette définition. En la considérant comme une plateforme en ligne, elle devrait se soumettre à un certain nombre d'exigences européennes émanant du Digital Service Act. En outre, le considérant 18 du préambule de la Directive 2024/1385 énonce que les termes « accessible au public » et « publiquement accessible » devraient s'entendre comme renvoyant à la possibilité de toucher un certain nombre de personnes. En 2022, la plateforme rassemblait plus de 3,2 millions de créateurs dans le monde

[130] Ferrand, E. (2021). « Sur Onlyfans, les jeunes peuvent être facilement repérés par des proxénètes ». *Le figaro.* https://etudiant.lefigaro.fr/article/sur-onlyfans-les-jeunes-peuvent-etre-facilement-reperes-par-des-reseaux-de-proxenetes_c88b05ea-607d-11eb-8fde-d92bf2ba0bfe/.

[131] Haut Conseil à l'égalité entre les femmes et les hommes. (2023). « Pornocriminalité : mettons fin à l'impunité de l'industrie pornographique ». https://haut-conseil-egalite.gouv.fr/IMG/pdf/hce-vio-rapport_pornocriminalite-v11-bdef.pdf

et près de 239 millions de « *fans* »[132]. Bien que reposant sur un service d'abonnement, les contenus sont disponibles pour des milliers de personnes, et devraient ainsi recevoir la qualification de « publiquement accessible ». En intégrant Only Fans aux plateformes entrant dans le champ du DSA et de la Directive 2024/1385, le site pourra être tenu responsable des contenus illicites publiés et devra mettre en œuvre des moyens proactifs de déréférencement, de signalement et de retrait.

[132] Radio France. (2023). « OnlyFans, plateforme favorite des créateurs de contenus sexuels, attire toujours plus d'utilisateurs ». https://www.radiofrance.fr/mouv/podcasts/reporterter/onlyfans-plateforme-favorite-des-createurs-de-contenus-sexuels-attire-toujours-plus-d-utilisateurs-1200317

RECOMMANDATIONS POUR LA TRANSPOSITION DE LA DIRECTIVE 2024/1385

1. Recommandations générales

a. Recommandations au niveau français

- Créer en France un Conseil National de Survivants et des Victimes sur le modèle de celui déjà existant en Allemagne. Sa principale mission serait de faire des recommandations de politiques publiques pour prévenir et répondre aux cyberviolences sexistes et sexuelles.
    - Le Conseil serait rattaché à une autorité indépendante qui abriterait aussi une commission d'enquête et un centre de recherche.

b. Recommandations au niveau européen

- Renforcer l'obligation des fournisseurs de services numériques de signaler aux autorités compétentes toute suspicion d'infractions pénales détectées sur leurs plateformes.
    - Imposer des délais de réponse plus courts aux réquisitions légales adressées aux plateformes et fournisseurs de services.
    - Prévoir des sanctions dissuasives en cas de non-coopération ou de réponse tardive aux demandes des autorités, comme une sanction pécuniaire ou une suspension.

- Imposer aux plateformes de fournir régulièrement des rapports sur leur modération, à transmettre à une autorité compétente, comme la Commission européenne dans le cadre de l'application et la mise en œuvre du règlement européen sur la lutte contre la diffusion de contenus à caractère terroriste en ligne. Ces rapports pourraient permettre d'identifier et corriger les biais sexistes des algorithmes pour garantir une meilleure régulation des contenus illégaux.

- Mettre en place des audits réguliers par une autorité compétente, comme la Commission ou des auditeurs indépendants certifiés, sur les mécanismes de modération déployés.

2. Partage de matériel intime (article 5)

a. Recommandations au niveau français

i. Recommendations législatives

- Clarifier la notion de « caractère sexuel » utilisée à l'article 226-2-1 du Code pénal, trop imprécise et subjective. Une reformulation plus rigoureuse telle que « images à connotation sexuelle ou relatives à l'intimité corporelle » permettrait une meilleure sécurité juridique tout en assurant la protection des victimes.

- Inclure dans la transposition de la Directive 2024/1385 les plateformes par abonnement proposant des contenus sexuellement explicites, telles que Only Fans. Elles ne sont pour l'instant absolument pas envisagées[133].

- Lors de la transposition, changer la formulation de l'article 5 de la Directive 2024/1385 : « *lorsque ce comportement est susceptible de causer un préjudice (psychologique ou physique) important* ». La remplacer par une formulation plus souple telle que « lorsqu'une telle conduite est susceptible d'altérer les conditions d'existence, la santé mentale ou la sécurité de la personne concernée » permettrait de rendre la qualification du préjudice moins difficile.

- Dans le cadre de la transposition, pour que l'infraction ne soit pas neutralisée dans la pratique, le droit français doit aller au-delà de la définition minimale.
    - Le texte de transposition pourrait préciser que le consentement n'est valable que s'il est donné en dehors de tout rapport de dépendance, de pression ou de manipulation, notamment dans des contextes de relations intimes, de minorité ou encore de vulnérabilité.

[133] Entretien avec Mariana Branco. (2 juin 2025).

- Cette précision permettrait d'exclure les cas où la victime a « consenti » à donner accès à ses comptes dans un environnement de contrôle et de coercition.

ii. Recommandations pour l'adaptation des dispositifs existants

- Exiger le déréférencement au niveau européen dès lors qu'un contenu a été signalé. Afin de mieux protéger les victimes, il conviendrait d'imposer le déréférencement d'un contenu illicite sur l'ensemble des versions européennes des moteurs de recherche et plateformes concernées, dès lors qu'un tel contenu a été signalé. L'Autorité de régulation de la communication audiovisuelle et numérique pourrait être chargée de surveiller l'effectivité du retrait global et de sanctionner les manquements. Cela suppose également une meilleure coopération entre les différentes autorités de régulation des États-membres.

- Démocratiser la technologie de la signature numérique et du hachage, afin que les plateformes recherchent de manière proactive les contenus qui ont déjà été signalés et retirés, mais républiés. Ceci nécessiterait soit l'intégration du hachage au processus de signalement (soumission du contenu à la plateforme qui procèdera au hachage puis supprimera tous les contenus correspondants), soit une plus grande participation avec les entités disposant des technologies de hachage comme Point de contact ou StopNCII. Les plateformes pourraient par exemple effectuer des démarches pour recueillir les données hachées auprès de ces organes et intégrer la suppression des contenus correspondants à leurs procédés de modération.
    - Il serait pertinent de mettre en place pour lesdites plateformes une obligation d'analyse périodique afin de détecter dans leurs systèmes la trace de contenus hachés, ainsi qu'une obligation corollaire de les supprimer.
    - Il pourrait également être créé un Centre européen de centralisation des haches afin de permettre une suppression générale du contenu que l'utilisateur souhaite protéger.

- Renforcer les outils de signalement pour les utilisateurs des plateformes, en les rendant plus visibles, simples, accessibles et efficaces.

- En ce qui concerne la visibilité, il serait approprié pour les plateformes de mettre en place des campagnes d'information sur les possibilités de signalement étant à disposition des utilisateurs et sur la manière dont celui-ci peut-être réalisé.
- Pour ce qui est de l'accessibilité, les plateformes pourraient par exemple s'inspirer de la méthode « symptoms first »[134] mise à l'essai par Twitter aux Etats Unis. Elle permet, au lieu de demander à l'utilisateur de qualifier le contenu qu'il signale, de lui soumettre un questionnaire complexe permettant d'informer la plateforme qu'elle héberge un contenu ayant causé un préjudice. Ainsi, les questions incluent des exemples plus spécifiques de cyberviolence (harcèlement, partage de contenu intime, incitation à la haine en ligne) et permettent à la personne de signaler le caractère raciste, sexiste ou homophobe du contenu. Twitter avance également mettre, avec l'adoption de cette méthode, l'accent sur un langage plus facilement assimilable et s'assurer de la compréhensibilité du processus de signalement. D'autres méthodes, comme celle avancée par Facebook, qui allègue retirer immédiatement le contenu dès sa signalisation[135] permettraient de mettre en place un système plus sécuritaire dans lequel le retrait serait la règle, et la remise en ligne du contenu ne surviendrait qu'après une vérification extensive.

- Reconnaître davantage d'acteurs de la société civile comme signaleurs de confiance afin de permettre une plus grande prise en charge. L'Arcom cite parmi les signaleurs de confiance potentiels les associations, les entités et les organisations, reconnues pour leurs expertises et leurs compétences. Ainsi, il existe plusieurs entités spécialisées que ce soit dans la protection des mineurs ou dans la lutte contre l'antisémitisme et le racisme. Bien qu'il existe Point de contact - un signaleur de confiance spécialisé dans les cyberviolences -, il n'existe pas de signaleur de confiance dont l'action serait ciblée sur les cyber violences sexistes. Il serait pertinent pour l'ARCOM d'ajouter à la liste des signaleurs un tel organisme. Le choix des acteurs de la société civile, lesquels ont

[134] Common Thread. (2021). « Twitter's new reporting process centers on a human-first design ». https://blog.x.com/common-thread/en/topics/stories/2021/twitters-new-reporting-process-centers-on-a-human-first-design (consulté le 22 juin 2025).
[135] Service public. (28 mai 2024). « How do I report illegal content posted on the Internet ». https://www.service-public.fr/particuliers/vosdroits/F31979?lang=en (consulté le 22 juin 2025).

connaissance des besoins des utilisateurs, permet de mieux intégrer ces derniers au procédé de signalement. Cela peut également assurer qu'ils auront un accompagnement plus complet lorsqu'ils souhaitent signaler un contenu. L'association doit cependant, comme le précise l'ARCOM[136], disposer d'une expertise et de compétences particulières aux fins de détecter, d'identifier et de notifier des contenus illicites, être indépendante de tout fournisseur de plateformes en ligne et exercer ses activités aux fins de la soumission des notifications de manière diligente, précise et objective.

b. Recommandations au niveau européen

- Instaurer une procédure d'injonction contraignante obligeant les hébergeurs à retirer ou bloquer, dans un délai d'une heure, les contenus intimes diffusés sans consentement, sur notification d'une autorité nationale compétente, chargée de faire respecter les injonctions, sous la supervision de la Commission européenne, à l'image du mécanisme prévu par le règlement européen relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne.

- En cas de signalement, prendre immédiatement des mesures pour mettre en place un retrait suspensif, pour faire cesser le préjudice le temps de la vérification des faits[137].

- Simplifier et centraliser les procédures de signalement en instaurant un système de coordination national, sur le modèle de la plateforme PERCI, permettant la transmission unifiée des signalements et des injonctions aux hébergeurs. Cette centralisation doit s'accompagner d'un renforcement des moyens humains et techniques des autorités compétentes afin d'assurer un traitement efficace et rapide des signalements.

- Renforcer le droit à l'effacement prévu à l'article 17 du RGPD en permettant le retrait rapide des contenus intimes diffusés sans consentement sur la base de la simple déclaration de la victime, notamment via des « signaleurs de confiance », sans qu'une décision judiciaire préalable ne soit requise, contrairement à la pratique actuelle. Ce

[136] Arcom. « Signaleurs de confiance : conditions et candidatures ». https://www.arcom.fr/espace-professionnel/signaleurs-de-confiance-conditions-et-candidatures (consulté 22 juin 2025).
[137] Entretien avec Céline Piques. (30 mai 2025).

retrait devrait intervenir dans un délai strict (une heure par exemple) sous peine de sanctions financières dissuasives en cas de manquement.

- Mettre en place un système de veille et de déréférencement automatique pour prévenir la réapparition des contenus déjà supprimés, la mise en place d'un organisme sur le modèle de PERCI permettrait de les coordonner.

- Créer un centre européen de régulation, de coordination et de recherche lié à EUROPOL pour détecter proactivement les contenus illicites et les retirer[138].
    - Y inclure un forum dédié à l'accompagnement des victimes.

3. Traque furtive en ligne (article 6)

a. Recommandations au niveau français

i. Recommendations législatives

- Lors de la transposition, changer la formulation de l'article 6 de la Directive 2024/1385 : « *lorsque ce comportement est susceptible de causer un préjudice (psychologique ou physique) important* ». La remplacer par une formulation plus souple telle que « lorsqu'une telle conduite est susceptible d'altérer les conditions d'existence, la santé mentale ou la sécurité de la personne concernée » permettrait de rendre la qualification du préjudice moins difficile.

- Créer une incrimination autonome du contrôle coercitif incluant de manière plus détaillée toutes formes de violence - dont celles numériques - comme proposé au départ par l'Assemblée Nationale le 28 janvier 2025 dans l'article 3 de la proposition de loi. Cela permettrait de prendre en compte « *l'intention unique de l'auteur de contrôler et soumettre la victime* »[139], le champ de l'article 6 de la Directive 2024/1385 serait alors mieux couvert.

[138] Sur le modèle de la proposition de règlement pour lutter contre les contenus pédopornographiques sur internet. Entretien avec Mié Kohiyama. (3 juin 2026).
[139] Muller, Y. (2024). « Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! ». *Le club des juristes.* Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! - Le Club des Juristes.

4. Harcèlement sexuel en ligne (article 7)

a. Recommandations au niveau français

i. Recommendations législatives

- Supprimer l'exigence de « craindre sérieusement pour sa propre sécurité ou celle de personnes à charge » de l'article 222-33-2 du Code Pénal.

- Lors de la transposition, changer la formulation de l'article 7 de la Directive 2024/1385 : « *lorsque ce comportement est susceptible de causer un préjudice (psychologique ou physique) important* ». La remplacer par une formulation plus souple telle que « lorsqu'une telle conduite est susceptible d'altérer les conditions d'existence, la santé mentale ou la sécurité de la personne concernée » permettrait de rendre la qualification du préjudice moins difficile.

ii. Recommandation pour l'adaptation des dispositifs existants

- Il serait pertinent ici d'appliquer la recommandation précitée relative à l'ajout d'acteurs de la société civile parmi les signaleurs de confiance.

5. Discours de haine sexiste (article 8)

a. Recommandations au niveau français

i. Recommandations législatives

- Clarifier la définition juridique de l'incitation à la haine.
    - Retirer la formulation « comportements menaçants, injurieux, insultants ou troublant l'ordre public » qui limite la portée de l'article et permet de ne sanctionner que les manifestations de haine les plus extrêmes.
    - Retirer la formulation « en diffusant publiquement » qui ne permet pas de prendre en compte certains groupes privés sur les réseaux sociaux et plateformes de communication.

- Définir l'incitation à la haine comme « t*out acte ou comportement qui, par des paroles, écrits, images ou tout autre moyen de communication, encourage, provoque ou incite directement à la discrimination, à l'hostilité ou à la violence envers une personne ou un groupe de personnes en raison de leur origine, leur appartenance ethnique, nationale, religieuse, leur sexe, oeur orientation sexuelle, leur handicap, ou toute autre caractéristique protégée par la loi* ».

Table des matières

Remerciements **1**
Méthodologie **2**
Introduction **6**
Développement **12**
1. Le partage non consenti de matériels intimes ou manipulés 12
1.1. Contexte 12
1.2. Le cadre juridique européen 13
1.2.1. Le Digital Services Act (DSA) 13
1.2.2. Le Règlement général sur la protection des données 17
1.2.3. Règlement européen contre la diffusion du terrorisme en ligne 22
1.2.4. Charte des droits fondamentaux de l'UE 24
1.3. Le cadre juridique français 25
1.4. Analyse 27
2. La traque furtive en ligne 30
2.1. Contexte 30
2.2. Le cadre juridique européen 31
2.3. Le cadre juridique français 33
2.4. Analyse 33
3. Le cyberharcèlement 39
3.1. Contexte 39
3.2. Le cadre juridique européen 40
3.3. Le cadre juridique français 41
3.4. Analyse 44
4. L'incitation à la violence ou à la haine en ligne 46
4.1. Contexte 46
4.2. Le cadre juridique européen 47
4.2.1. Digital Services Act 47
4.2.2. Code de conduite de 2016 48
4.2.3. Décision cadre de 2008 50
4.3. Le cadre juridique français 51
4.4. Analyse 52
RECOMMANDATIONS POUR LA TRANSPOSITION DE LA DIRECTIVE 2024/1385 ..... **56**
Table des matières **64**
Bibliographie **65**

Bibliographie

Ouvrages spécialisés

Adamson, D.M. et al. (2023). « Cyberstalking: A Growing Challenge for the U.S. Legal System ». RAND Corporation. 20 p.

Dulaurans, M. (2024). « Violences en ligne: décrypter les mécanismes du cyberharcèlement ». Presses universitaires de Bordeaux. 236 p.

Stark, E. (2023). « Coercive Control : How Men Entrap Women in Personal Life ».

Thèses

Andréani, A. (2020). « Le droit à l'oubli : étude comparée entre la France et les Etats-Unis ». Thèse de doctorat. Université Paris II Panthéon-Assas.

Udoh-Oshin, G. (2017). « Hate Speech on the Internet: Crime or Free Speech ? ». Thèse undergraduate. Long Island University.

Articles

Boizard, M. (2016). « Le temps, le droit à l'oubli et le droit à l'effacement ». *Les Cahiers de la justice*, no 4, (p. 619-628).

Bossan, J. (2024). « La protection de la représentation à l'ère du numérique et du deepfake : le délit de montage version 2.0 ». *Légipresse*, n°426, (p. 380-385).

Cammillieri-Subrenat A. (2002). « L'incitation à la haine et la Constitution ». *Revue internationale de droit comparé*. vol. 54. n°2. (p. 513-548).

Chauvet, D. (2015). « Mérites ou démérites du délit général de harcèlement moral créé par la loi du 4 août 2014 ?". *Recueil Dalloz*, 2015, (page 174).

Chimchiuri, L. (2024). « Cyberbullying : A Threat to Freedom of Expression ». *Proceedings of the 36th International RAIS Conference on Social Sciences and Humanities*. Scientia Moralitas Research Institute. (p. 31-36).

Citron, D. K ; Franks, M. A. (2014). « Criminalizing Revenge Porn ». *Wake Forest Law Review*, 49 (2), p. 346.

Demaske, C. (2023). « L'opérationnalisation des discours de haine à l'échelle de la communauté Un plan de lutte contre les discours de haine ». *Réseaux,* vol. 241. n°5. (p. 197-235).

Den heijer, M ; Abeelen, T ; Maskyla, A. (2019). « On the Use and Misuse of Recitals in European Union Law ». *Amsterdam Law School Research Paper*. No°2019-31. 25.

Garnier P. (2024). « Mascus, les hommes qui détestent les femmes – Le documentaire ». *Made In Perpignan*.

Gordon G.S. (2013). « Hate Speech Persecution: A Contextual Approach ». *Vanderbilt Journal of Transnational Law*. vol. 303. n° 2. (p. 303-373).

Jaki S, De Smedt T, Gwozdz M, *et al.* (2019). « Online hatred of women in the Incels. me forum: Linguistic analysis and automatic detection ». *Journal of Language Aggression and Conflict*, vol. 7, n°2, p. 240-268.

Kobets, P. ; Krasnova, K. (2018). « Cyberstalking: Public danger, key factors and prevention ». *Przeglad Wschodnioeuropejski*, vol 9, n°2, (p. 43–53).

Kristof, N. (2020). « The Children of Pornhub ». *The New York Times.*

Ouest France. (2024). « Sur Telegram des milliers d'hommes échangeaient des conseils pour droguer et violer des femmes ».

Segonds, M. (2014). « Un an de droit pénal du travail », *Dr. pénal. chron. 10.*

Terwangne, C. (2015). « Droit à l'oubli, droit à l'effacement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique ». *Enjeux européens et mondiaux de la protection des données personnelles.* Création information communication, Larcier. (p. 245-275).

Documents officiels

1. Commission européenne

Commission européenne. (2014). « Rapport de la Commission au Parlement européen et au Conseil relatif à la mise en œuvre de la décision-cadre 2008/913/JAI du Conseil sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal ».

Commission européenne. (2022). « Communiqué de presse : Code de conduite de l'UE contre les discours haineux en ligne : la dernière évaluation montre un ralentissement des progrès ».

Commission européenne. (2022). « Factsheet : Countering illegal hate speech online : 7th evaluation of Code of Conduct ».

Commission européenne. (2023). « Acte délégué sur les audits indépendants au titre de la législation sur les services numériques ». C/2023/6807.

Commission européenne. (2024). « Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre du règlement (UE) 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne ».

2. Conseil de l'Union européenne

Conseil de l'Union européenne. (2008). *Décision-cadre 2008/913/JAI du 28 novembre 2008 relative à la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal.*

Conseil de l'Europe. « Factsheet on Combating sexist hate speech ».

Conseil de l'Europe. (2019). « Recommandation sur la prévention et la lutte contre le sexisme ». CM/Rec(2019)1.

Conseil européen et Conseil de l'Union européenne. (2024). « Mesures prises par l'Union européenne pour mettre fin à la violence à l'encontre des femmes ». Mesures prises par l'UE pour mettre fin à la violence à l'encontre des femmes - Consilium (consulté le 4 février 2025).

Conseil de l'Union européenne. (2024). « Communiqué de presse : Le Conseil adopte la toute première loi de l'Union européenne sur la violence à l'égard des femmes ». Le Conseil adopte la toute première loi de l'UE sur la violence à l'égard des femmes - Consilium. (consulté le 4 février 2025).

3. Parlement européen

Parlement européen. (2020). « Briefing : La violence envers les femmes dans l'Union européenne État des lieux ». www.europarl.europa.eu/RegData/etudes/BRIE/2020/659333/EPRS_BRI(2020)659333_FR.pdf

Parlement européen et Conseil européen. (2022). « Proposition de directive sur la lutte contre la violence à l'égard des femmes et la violence domestique ». EUR-Lex - 52022PC0105 - EN - EUR-Lex

4. Autres

Assemblée Parlementaire de la Francophonie, Réseau des femmes parlementaires. (2021). *Rapport final : la cyberviolence envers les femmes et les enfants dans l'espace francophone*, p. 5, 9. Microsoft Word - Rapport final sur la cyberviolence envers les femmes et les enfants.

Greffière de la CEDH. (2021). Communiqué de presse « Manquements, constitutifs de violations, à l'obligation de traiter les cas de violences domestiques ; modifications législatives requises de toute urgence ».

Ministère de l'Intérieur. (2025). « Communiqué de presse : Les infractions liées au numérique enregistrées par les services de sécurité en 2024 ». https://www.interieur.gouv.fr/actualites/communiques-de-presse/infractions-liees-au-numerique-enregistrees-par-services-de#:~:text=Les%20infractions%20li%C3%A9es%20au%20num%C3%A9rique%20enregistr%C3%A9es%20par%20les%20services%20de%20s%C3%A9curit%C3%A9%20en%202024,-Communiqu%C3%A9s%20de%20presse&text=En%20France%20en%202024%2C%20les,n%C3%A9cessaire%20de%20les%20analyser%20s%C3%A9par%C3%A9ment. (consulté le 17 février 2025).

Service public fédéral Intérieur, Direction générale Sécurité et Prévention. (2022). *Fiche informative, « La Manosphère »*, p.5. Home FR | IBZ - SPF Intérieur.

Rapports et recommandations

Agence des droits fondamentaux de l'UE. (2014). Rapport: « La violence à l'égard des femmes : une enquête à l'échelle de l'UE ». https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-factsheet_fr.pdf.

Centre Hubertine Auclert. (2017-2018). « Rapport Cyberviolences conjugales ». Rapport « Cyberviolences conjugales » | Centre Hubertine Auclert.

Féministes contre le cyberharcèlement. (2022). « Cyberviolence et cyberharcèlement : le vécu des victimes ». Enquête conduite par IPSOS auprès de 216 victimes de cyberviolences âgées de 16 ans à 60 ans ou plus. https://www.vscyberh.org/.

Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (GREVIO). (2021). « Recommandation générale n°1 sur la dimension numérique de la violence à l'égard des femmes ».
https://rm.coe.int/reccomandation-no-du-grevio-sur-la-dimension-numerique-de-la-viomence-/1680a49148

Haut Conseil à l'égalité entre les femmes et les hommes. (2023). « Pornocriminalité : mettons fin à l'impunité de l'industrie pornographique ». https://haut-conseil-egalite.gouv.fr/IMG/pdf/hce-vio-rapport_pornocriminalite-v11-bdef.pdf

Lobby européen des femmes. (2024). « Rapport sur la cyberviolence contre les femmes. Résumé analytique et recommandations ».

Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains (MIPROF). (2024). « Guide cyberviolences au sein du couple ». https://arretonslesviolences.gouv.fr/sites/default/files/2024-11/Guide-cyberviolences-au-sein-du-couple-Miprof-2024-version-accessible.pdf

Plateforme EDVAW. (2020). « Rapport thématique de la plateforme des mécanismes indépendants d'experts sur la discimination et la violence à l'égard des femmes ». 1680a933ae.

Simonovic Dubravka, Rapporteuse spéciale des Nations Unies sur la violence contre les femmes et filles. (2018). « Rapport 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 ». https://digitallibrary.un.org/record/1641160?ln=fr&v=pdf.

UNESCO. (2021). « The Chilling : Global trends in online violence against women journalists ». https://unesdoc.unesco.org/ark:/48223/pf0000377223 (consulté le 9 mars 2025).

Dispositions législatives

Europe :

Conseil de l'Europe. (2011). *Convention sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique.* ouverte à la signature à Istanbul le 11 mai 2011. Série des Traités du Conseil de l'Europe, n° 210.

Traité sur le fonctionnement de l'UE (version consolidée). (2012).

Parlement européen et Conseil. (2016). *Règlement UE 2016/679 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 (RGPD).Journal officiel de l'Union européenne. L119/1 .https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
Parlement européen et Conseil de l'Union européenne. (2022). *Règlement (UE) 2022/2065 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE*. Journal officiel de l'Union européenne. L 277/1 Règlement - 2022/2065 - EN - EUR-Lex.

Parlement européen et Conseil européen. (2024). *Directive (UE) 2024/1385, du 14 mai 2024, sur la lutte contre la violence à l'égard des femmes et la violence domestique*. Journal officiel de l'Union européenne, L 2024/1385. Directive - UE - 2024/1385 - EN - EUR-Lex.

France :

Assemblée Nationale. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexuelles et sexistes ».

Loi du 29 juillet 1881 sur la liberté de la presse. (Version en vigueur au 25 mai 2025)

Loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexistes et sexuelles. (2018).

Loi n°2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

Décisions jurisprudentielles

Europe :

Cour de justice de l'Union européenne. (2016). *Breyer* . C-582/14, EU:C:2016:779. Points 39 et 41.

Cour européenne des droits de l'Homme. (1981), *Dudgeon c. Royaume-Uni*, Series A, No.45, para. 41.

Cour européenne des droits de l'homme. (2021). *Arrêt Tunikova et autres contre Russie*. TUNIKOVA AND OTHERS v. RUSSIA

France :

Conseil constitutionnel. (2021). Décision n°2021-933 QPC du 30 septembre 2021. Décision n° 2021-933 QPC du 30 septembre 2021 | Conseil constitutionnel**.**

Conseil d'Etat. (2019). 10e et 9e chambre réunies, n° 429154, 6 décembre.

Cour de cassation, Chambre civile. Arrêt du 21 mars 2018, n°16-28.741.

Cour de cassation, Chambre criminelle. Arrêt du 9 mai 2018, n° 17-83.623.

Cour de cassation, Chambre criminelle. Arrêt du 29 mai 2024, n°23-80.806

Sitographie

ARCOM. « Signaleurs de confiance : conditions et candidatures ». https://www.arcom.fr/espace-professionnel/signaleurs-de-confiance-conditions-et-candidatures (consulté 22 juin 2025).

Centre Hubertine Auclert. (2023). « Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyberviolences conjugales ». Décryptage de l'Observatoire n°1 : Les nouveaux dispositifs de localisation et les risques d'utilisation dans le cadre de cyberviolences conjugales | Centre Hubertine Auclert (consulté le 23 mai 2025).

Cyberharcèlement. « Cyberharcèlement et liberté d'expression : les enjeux juridiques ». https://cyber-harcelement.info/la-frontiere-entre-cyberharcelement-et-liberte-dexpression-les-enjeux-juridiques/ (consulté le 22 mai 2025).

Common Thread. (2021). « Twitter's new reporting process centers on a human-first design ». https://blog.x.com/common-thread/en/topics/stories/2021/twitters-new-reporting-process-centers-on-a-human-first-design (consulté le 22 juin 2025).

Ferrand, E. (2021). « Sur Onlyfans, les jeunes peuvent être facilement repérés par des proxénètes ». *Le figaro.* https://etudiant.lefigaro.fr/article/sur-onlyfans-les-jeunes-peuvent-etre-facilement-reperes-par-des-reseaux-de-proxenetes_c88b05ea-607d-11eb-8fde-d92bf2ba0bfe/.

Hardouin-Le-Goff, C. (2023). « L'incrimination du contrôle coercitif, futur outil de lutte contre les violences conjugales? » *Le club des juristes.* L'incrimination du contrôle coercitif, futur outil de lutte contre les violences conjugales ? - Le Club des Juristes.

Humanrights.ch. (2016). « Incitation à la haine sur Internet – Cas suisses et politique des portails d'informations en la matière ». https://www.humanrights.ch/fr/pfi/droits-humains/droits-politiques/incitation-haine-internet-cas-suisses-politique-portails-informations (consulté le 23 mai 2025).

Muller, Y. (2024). « Consécration de la notion de contrôle coercitif… Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire ». *Le club des juristes.* Consécration de la notion de contrôle coercitif…. Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire - Le Club des Juristes

- (2024). « Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! ». *Le club des juristes.* Le contrôle coercitif dans les violences intrafamiliales, une affaire de qualification ! - Le Club des Juristes.

Nations Unies. « Discours de haine : Incidence et prévention : Cibles de la haine ». https://www.un.org/fr/hate-speech/impact-and-prevention/targets-of-hate (consulté le 23 mai 2025).

Nations Unies. « Hate speech versus freedom of speech ». (https://www.un.org/en/hate-speech/understanding-hate-speech/hate-speech-versus-freedom-of-speech) (consulté le 22 mai 2025).

New York Times. (2024). « The troubling trend in teenage sex ». https://www.nytimes.com/2024/04/12/opinion/choking-teen-sex-brain-damage.html. (consulté le 9 juin 2025).

New York Times. (2025). « These Internal Documents Show Why We Shouldn't Trust Porn Companies ». https://www.nytimes.com/2025/05/10/opinion/pornhub-children-documents.html. (consulté le 9 juin 2025).

Osez le Féminisme. Osez le feminisme ! – On ne nait pas féministe, on le devient… (consulté le 16 mai 2025).

Radio France. (2023). « OnlyFans, plateforme favorite des créateurs de contenus sexuels, attire toujours plus d'utilisateurs ». https://www.radiofrance.fr/mouv/podcasts/reporterter/onlyfans-plateforme-favorite-des-createurs-de-contenus-sexuels-attire-toujours-plus-d-utilisateurs-1200317.

Service public. (2024). « How do I report illegal content posted on the Internet ». https://www.service-public.fr/particuliers/vosdroits/F31979?lang=en (consulté le 22 juin 2025).

Tilburg University. Kamara, I. (2023). « Cyberstalking and online platforms' due diligence in the EU Digital Services Act ». TTLF Newsletter on Transatlantic Antitrust and IPR Developments, Stanford-Vienna Transatlantic Technology Law Forum : https://research.tilburguniversity.edu/en/publications/cyberstalking-and-online-platforms-due-diligence-in-the-eu-digita (consulté le 12 février).

Vie publique. (2025). « Proposition de loi visant à renforcer la lutte contre les violences sexistes et sexuelles ». Violences sexuelles et sexistes Contrôle coercitif Viol Proposition loi | vie-publique.fr.

Colloque

Osez le Féminisme et la CLEF. (2025). Colloque : « Exploitation sexuelle en ligne : enjeux et réponses européennes ». Strasbourg.