GRANDE ENQUÊTE SUR LES CYBERVIOLENCES SEXISTES ET SEXUELLES

2 136 répondant·es
1 209 victimes · Juin 2026

Féministes contre le cyberharcèlement
Point de Contact · #StopFisha

LE RAPPORT

Une publication coordonnée par :
Yann Lescop, Laura Pereira Diogo,
Laure Salmona.

Rédaction : Wendy Adouki, Angèle Albrengues, Alice Apostoly, Mathilde Fraigneau, Lisa Gauvin-Drillaud, Meryem Khouzaimi, Hugo Krief, Coline Lambrey, Yann Lescop, Laura Pereira Diogo, Victoire Poignet Legray, Laure Salmona.

Ont également participé à cette publication : Audrey Abat, Saskia Juigner Doubinsky, Élisa Mailly, Juliette Maréchal, Alejandra Mariscal Lopez, Eden Martin, Malou Monnier, Agathe Musset, Hajar Outaik, Marie-Hélène Pereira Diogo, Maëlle Roy-Moreau, Mélanie Emerich.

Remerciements : Merci à toutes les personnes répondantes d'avoir pris le temps de partager leur expérience, parfois intime et douloureuse : vos témoignages sont essentiels pour mieux comprendre les cyberviolences sexistes et sexuelles, documenter leurs effets concrets et renforcer les réponses collectives pour les prévenir, les combattre et mieux accompagner les victimes.

Direction artistique, illustrations et maquette :
Vincent Devillard
www.vincentdevillard.com

Impression :
Exaprint, 34130 Mauguio, France

TABLE DES MATIÈRES

AVANT-PROPOS

Sous l'impulsion des associations Féministes contre le cyberharcèlement, Point de Contact et #StopFisha, une Grande enquête nationale sur les cyberviolences* sexistes et sexuelles* a été lancée le 3 juin 2025. Avec 2 136 répondant·es, cette enquête constitue un important vivier de données et de témoignages pour appréhender, au plus près des réalités de terrain, les violences qui structurent l'expérience de nombreux – et surtout nombreuses – internautes.

Malgré l'accélération de ce phénomène et son impact dévastateur sur les victimes, le manque d'études exhaustives sur les cyberviolences sexistes et sexuelles entretient la faiblesse des réponses apportées, que ce soit sur les plans juridique, politique, technique ou social. Face à ce constat alarmant, ce rapport inter-associatif entend rendre compte de ce que représentent concrètement les violences sexistes et sexuelles en ligne en mettant en valeur la parole des victimes.

Souvent reléguées au rang des violences de seconde zone, les cyberviolences sexistes et sexuelles sont pourtant loin de constituer des usages marginaux ou déviants des outils numériques : elles s'inscrivent aussi bien dans les pratiques que dans l'architecture même de ces environnements et se situent au croisement de dynamiques sociales, techniques et économiques qui façonnent nos expériences en ligne. Ces violences numériques traversent les réseaux sociaux, les messageries instantanées et d'autres plateformes de partage de contenus – mais aussi des dispositifs plus discrets, tels que les objets connectés ou les outils de géolocalisation. Leur banalisation apparente masque pourtant des mécanismes de violence complexes, aux effets profonds et durables sur les personnes qui en sont victimes. L'invisibilisation de la parole des victimes maintient les hiérarchies et perpétue les stéréotypes de genre en nourrissant, d'une part, une culture de la honte chez les victimes, marquée par une forme de mort sociale, tandis qu'elle permet, d'autre part, aux agresseurs de poursuivre leur vie en toute impunité, tant dans l'espace numérique que dans la vie réelle.

Pour rompre avec cette logique d'impunité, il faut d'abord nommer précisément les cyberviolences sexistes et sexuelles, comprendre les mécanismes qui les rendent possibles et documenter leurs effets concrets sur la vie des victimes. C'est l'objet de ce rapport : partir des expériences déclarées par les personnes concernées pour mettre en lumière des violences encore trop souvent minimisées, mal qualifiées ou insuffisamment prises en charge.

En articulant données quantitatives, témoignages et analyse des mécanismes techniques, sociaux et institutionnels à l'œuvre, ce rapport entend contribuer à une meilleure reconnaissance de ces violences et à la construction de réponses à la hauteur : prévention, accompagnement des victimes, formation des professionnel·les, responsabilisation des plateformes et renforcement des politiques publiques.

MÉTHODOLOGIE

Les données quantitatives mobilisées dans ce rapport sont issues de la Grande enquête sur les cyberviolences sexistes et sexuelles, une enquête auto-administrée et diffusée en ligne.

La passation du questionnaire a été réalisée selon la méthode CAWI (Computer-Assisted Web Interviewing), avec une diffusion en ligne du 3 juin au 3 août 2025, et une passation en autonomie par les personnes ayant répondu au questionnaire.

Le lien a été partagé sur les réseaux par l'intermédiaire des comptes des associations ayant conçu l'enquête (Féministes contre le cyberharcèlement, Point de Contact et #StopFisha). Il a également fait l'objet de repartages.

L'échantillon repose donc sur une participation volontaire et ne constitue pas un échantillon représentatif de la population générale. Les résultats doivent être lus comme une documentation approfondie des expériences déclarées par les personnes ayant répondu à l'enquête, et non comme une mesure de prévalence à l'échelle nationale. Ce choix méthodologique permet néanmoins de recueillir des données fines sur des violences encore insuffisamment documentées.

Le questionnaire comprend deux parties : la première concerne les victimes de cyberviolences sexistes et sexuelles, et recueille des informations sur ces dernières et sur les violences qu'elles ont vécues au cours de leur vie. La seconde s'adresse à l'ensemble des répondant·es, et porte sur leur connaissance des cyberviolences sexistes et sexuelles.

Deux questions introductives permettent de distinguer les victimes des non-victimes, puis d'identifier les différents types de violences subies. L'enquête permet ainsi de disposer de données précises sur les violences dites NCII (non-consensual sharing of intimate images ou diffusion non consentie de contenus intimes), qui constituent un sous-ensemble des cyberviolences.

Le volet adressé aux victimes déplie progressivement les différents aspects des violences vécues. D'abord, il s'agit de caractériser globalement le phénomène : qui sont les victimes ? Quelles formes de cyberviolences ont-elles subies ? Dans quel contexte se sont-elles produites ? Qui sont les agresseurs ? D'autres questions précisent le panorama, et notamment l'après des violences : elles abordent le dépôt de plainte, les réactions des personnes auxquelles les victimes se sont confiées, les conséquences sur leur vie et sur leur usage des réseaux sociaux, ainsi que l'éventuelle poursuite des violences au-delà des espaces numériques.

Le volet concernant l'ensemble des répondant·es porte sur leur niveau de connaissance des différents types de cyberviolences et de leurs caractéristiques, notamment lorsqu'elles peuvent constituer des infractions pénales. Les questions sont suivies d'encarts explicatifs, permettant d'associer à la collecte de données un objectif de prévention et de sensibilisation du public.

Introduction.
NOTIONS ET CONCEPTS MOBILISÉS

Comprendre les cyberviolences sexistes et sexuelles nécessite d'en dépasser les simplifications médiatiques. Les notions utilisées pour les désigner restent à ce jour hétérogènes mais continuent d'influencer la manière dont ces violences sont identifiées, qualifiées et traitées. Clarifier ces concepts est donc un préalable essentiel à toute analyse rigoureuse des dynamiques qui les irriguent.

A. Concept de cyberviolences sexistes et sexuelles

1 - Comprendre ce que sont les cyberviolences sexistes et sexuelles

Définition. Les cyberviolences sexistes et sexuelles regroupent « toutes les violences de genre qui ont lieu en ligne, que ce soit sur internet, sur les réseaux sociaux, dans les jeux vidéo, ou sur tout autre espace numérique »[1], ainsi que celles perpétrées par le biais des outils et technologies numériques comme des traceurs GPS, objets connectés ou caméras de surveillance. Autrement dit, elles sont le *continuum* des violences sexistes et sexuelles dans le cyberespace*. Elles prennent de nombreuses formes (*deepfake*, dickpic**, chantage à la cam ou encore sextorsion*…) que ce rapport détaillera par la suite.

À l'image des violences sexistes et sexuelles commises dans le monde physique, ces cyberviolences s'appuient sur des logiques de domination patriarcale et s'attaquent à l'intimité des victimes, soit en tirant un profit (économique ou sexuel) soit en l'exposant aux yeux de tous·tes.

Un phénomène interdit par la loi. Au niveau législatif, ces violences sont, pour la majorité d'entre elles, réprimées par la législation française. Leur commission est sanctionnée et l'auteur encourt des peines différentes selon le mécanisme dont elles relèvent (chantage, extorsion, usurpation d'identité, harcèlement, diffusion non consentie de contenus sexuels*, etc.). De plus, l'utilisation du numérique, si elle n'est pas inhérente à la nature de l'infraction, est souvent un facteur aggravant des sanctions encourues, tant au niveau de la durée d'emprisonnement qu'au niveau de l'amende.

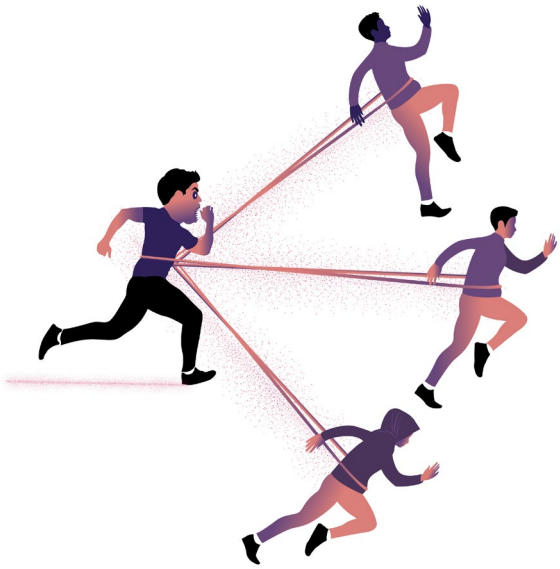
2 - Caractéristiques des cyberviolences sexistes et sexuelles

Derrière l'expression cyberviolences se cache une multitude de violences exercées par le biais ou à l'aide des technologies numériques. Elle comprend aussi bien les violences subies sur les réseaux sociaux ou plus généralement sur internet que toutes celles qui sont facilitées par voie algorithmique – notamment par l'utilisation de l'intelligence artificielle* générative (*deepfakes*) – ou par l'usage des objets connectés tels que les caméras de surveillance, la domotique*, les traceurs GPS ou encore les smartphones.

La sphère numérique ne cesse d'étendre ses ramifications au gré de l'apparition de nouvelles technologies. L'espace physique et l'espace numérique s'entrelacent et les cyberviolences, loin de se cantonner au seul monde numérique, sont perpétrées à travers différentes dimensions.

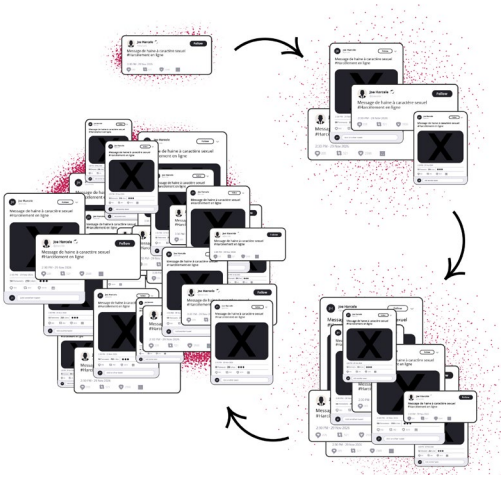
[1] Association #StopFisha : Outaik, H., Outaik, H., Bories, J., Reynaud, L., Diogo, L. P., Drillaud, L. G., Janvier, M., Haouari, S., Maclaren, S. C., & Pardo, R.-F. (Coord.). (2021). *Combattre le cybersexisme*. Éditions Leduc.s. https://www.editionsleduc.com/produit/2561/9791028521783/combattre-le-cybersexisme

Aujourd'hui, fermer ses réseaux sociaux ou éteindre son ordinateur ne suffit plus à échapper à ces violences, le numérique s'étant insinué dans tous les aspects de nos vies.



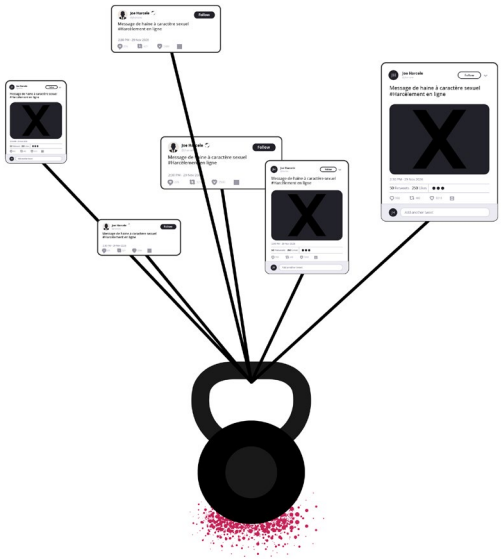
Intemporalité et ubiquité :

les cyberviolences ne connaissent ni limites spatiales, ni limites temporelles. S'il est possible de trouver des moments ou des espaces de repli pour échapper à certaines formes de violences, avec la dématérialisation des échanges, les violences commises via les outils numériques sont susceptibles de nous atteindre à n'importe quelle heure du jour ou de la nuit et dans n'importe quel endroit du monde. Un enfant victime de harcèlement scolaire pouvait – avant l'invention des outils numériques – échapper aux violences par moments, durant les temps extrascolaires par exemple, voire changer d'établissement ou déménager pour mettre fin au harcèlement. Cela est devenu quasiment impossible aujourd'hui : les violences peuvent se poursuivre même si la personne ciblée part à l'autre bout du monde. Cette absence de répit engendre chez la plupart des victimes une hypervigilance particulièrement épuisante.



Haut potentiel de viralité :

Une autre particularité de ces violences est leur dimension virale, un contenu initialement destiné à une audience restreinte pouvant, au fil des partages et des captures d'écran, atteindre des centaines, des milliers, voire des millions d'internautes. Cette viralité potentielle rend tout contrôle de ce que l'on partage en ligne illusoire et cette perte de contrôle peut entraîner des dommages supplémentaires et souvent imprévisibles pour les victimes.



Rémanence et menaces prolongées :

À cela s'ajoute la persistance des contenus qui sont parfois difficiles à faire supprimer par les plateformes et peuvent rester visibles en ligne ou ressurgir soudainement à n'importe quel moment. Or cette menace, qui semble parfois infinie, peut alimenter la souffrance et l'anxiété des victimes.

Pseudonymat ou anonymat ?

On parle souvent du pseudonymat car l'anonymat réel est très rare en ligne. La sphère numérique est assez semblable à la sphère publique, au sein de laquelle nous n'évoluons pas en brandissant sans cesse notre identité au-dessus de nos têtes, sans pour autant être totalement anonymes puisque nous pouvons produire cartes d'identité et extraits de naissance. Le pseudonymat est une forme de service offert par les plateformes numériques sur lesquelles il est possible d'utiliser un pseudonyme sans afficher son état-civil à la vue de tous·tes. Il est en revanche possible, dans l'immense majorité des cas, de retrouver assez facilement l'identité des internautes en retraçant leur adresse IP, qui s'apparente à une sorte de carte d'identité numérique. Ce n'est donc pas tant l'anonymat en lui-même qui facilite la commission des violences, que l'impunité sociale et pénale dont bénéficient les auteurs de cyberviolences et le manque de formation technique au sein de certains services de police.

Déshumanisation et effet cockpit

En revanche l'absence d'empathie et la déshumanisation de l'autre sont des facteurs prédominants de la commission de ces violences. La dématérialisation des relations permise par l'utilisation des outils numériques entraîne une difficulté à percevoir les affects des autres, voire à les considérer comme des individus avec des émotions. C'est ce qu'on appelle l'effet cockpit. Ce terme a tout d'abord été utilisé pour parler de la distance avec la cible qui facilite le fait de larguer une bombe susceptible de tuer et blesser de nombreuses personnes. Et en effet, si ne pas avoir à faire face à sa victime, à se confronter à ses émotions et à sa souffrance peut faciliter certains passages à l'acte, dans d'autres cas, c'est au contraire cette souffrance qui est recherchée. C'est en cela que l'un des facteurs importants reste la déshumanisation : de nombreux travaux de recherche montrent en effet des liens étroits entre le fait de ne pas considérer certaines personnes, ou certains groupes de population, comme des êtres humains à part entière et le passage à l'acte violent[23].

[2] Kelman, H. C. (1973). Violence without moral restraint: Reflections on the dehumanization of victims and victimizers. **Journal of Social Issues**, 29(4), 25-61. https://hckelman.scholars.harvard.edu/sites/g/files/omnuum10576/files/hckelman/files/Violence_1973.pdf
[3] Maoz, I., & McCauley, C. (2008). Threat, dehumanization, and support for retaliatory aggressive policies in asymmetric conflict. **Journal of Conflict Resolution**, 52(1), 93-116. http://www.jstor.org/stable/27638596

3 - Le continuum des violences sexistes et sexuelles entre espaces numériques et physiques

Un reflet des sociétés actuelles

L'espace numérique et l'évolution de ses usages sont un reflet de notre société. L'ensemble des inégalités, des rapports de domination et des violences du monde physique s'y retrouvent – notamment la déshumanisation de certaines catégories de personnes telles que les femmes et les groupes minorisés. Ainsi la déferlante des violences numériques ne naît pas *ex nihilo* ; elle n'est pas uniquement liée au développement des technologies numériques, mais s'inscrit dans un continuum entre les espaces physiques et numériques. Par ce biais, elle vient prolonger via les outils numériques l'ensemble des violences exercées de façon disproportionnée à l'encontre des femmes et des groupes les plus discriminés et vulnérables. Ce continuum fonctionne dans les deux sens : les violences en ligne peuvent être accompagnées ou suivies de violences physiques, et inversement, des violences physiques, comme des violences sexuelles, peuvent se poursuivre en ligne si elles ont été enregistrées et que les images sont diffusées, par exemple. Dans le cas de violences au sein du couple, les outils numériques sont souvent utilisés par les agresseurs en tant que moyens d'exercer un contrôle coercitif sur leur victime. Cela leur permet ainsi de renforcer leur emprise et de leur assurer une impunité.

Un phénomène inhérent au développement des technologies numériques

Le rôle des plateformes. Si les cyberviolences ne sont pas uniquement liées à l'existence des technologies numériques, leur prolifération reste largement facilitée par les plateformes et outils du numérique dont le modèle de conception tend à favoriser les comportements discriminants envers les populations vulnérables – telles que les enfants par exemple – et à encourager la diffusion de contenus violents. Ces derniers sont effectivement souvent mis en avant par les différentes plateformes car ils assurent l'engagement des internautes et génèrent plus d'interactions : vues, likes, partages, commentaires.

L'utilisation détournée de produits numériques. Les objets connectés, quant à eux, sont souvent conçus par des hommes – 80 à 90 % des personnes qui développent ces technologies sont de genre masculin[4] – privilégiés. Les problématiques relatives aux violences et discriminations commises à l'encontre de groupes minoritaires ne sont pas des sujets dont ils se saisissent. Les *AirTags* – petits traceurs GPS – illustrent parfaitement cela. Initialement destinés à tracer des objets, comme une valise ou des clés, pour éviter de les perdre, ils ont finalement été massivement utilisés par des hommes afin de surveiller leur compagne, notamment dans un contexte de violences conjugales.

[4] En France la part de femmes parmi les étudiant·es en informatique et sciences informatiques en cycle ingénieur est de 17 %. Source : Repères et références statistiques 2023 – MESR-DEPP. https://www.education.gouv.fr/reperes-et-references-statistiques-2023-378608

4 - Définition des différentes cyberviolences sexistes et sexuelles

Les injures

Une injure* est « une parole, un écrit ou une expression de la pensée adressés à une personne dans l'intention de la blesser ou de l'offenser. ». Elle peut être appuyée sur des représentations sexistes, LGBTQIA+phobes, racistes, validistes, xénophobes… et peut les renforcer volontairement, en stigmatisant davantage la personne visée. Dans le cadre du cyberharcèlement*, l'injure est utilisée publiquement, en toute impunité, les auteur·ices se cachant souvent derrière un pseudonyme. Sa portée est multipliée par son caractère public et par la facilité de la « partager » sur certains réseaux sociaux (Ex : X, TikTok, Instagram). Pourtant l'injure est punie par la loi.[5]

Le cyberharcèlement

Définition. Le cyberharcèlement désigne les formes de harcèlement commises au moyen d'outils ou d'espaces numériques : réseaux sociaux, messageries, forums, jeux vidéo, courriels, téléphones portables ou tout autre service de communication en ligne. Il peut se définir comme un ensemble de propos, comportements, publications ou partages répétés, produits ou diffusés en ligne, visant une ou plusieurs personnes et ayant pour effet de dégrader leurs conditions de vie, leur sécurité, leur santé psychique ou leur possibilité d'exister librement dans les espaces numériques[8]. La répétition peut résulter des agissements d'une seule personne, mais aussi d'une dynamique collective. Dans ce dernier cas, des personnes différentes peuvent contribuer au harcèlement en publiant, relayant, commentant ou amplifiant des contenus visant une même victime, y compris lorsque chacune d'elles n'intervient qu'une seule fois, dès lors que ces actes s'inscrivent dans une répétition concertée ou dont les participant·es ont connaissance.

Caractéristiques. Le cyberharcèlement se distingue notamment par la porosité qu'il crée entre les espaces publics, privés et intimes. Parce que les outils numériques accompagnent désormais une grande partie de la vie quotidienne, les violences peuvent atteindre la victime à tout moment, dans des espaces où elle devrait pouvoir se sentir protégée : son téléphone, sa messagerie, ses réseaux sociaux, son espace professionnel ou scolaire, voire son domicile. Les limites spatiales et temporelles qui permettaient parfois de se soustraire à la violence se trouvent ainsi considérablement réduites. Cette omniprésence peut produire un sentiment d'insécurité durable, une hypervigilance constante et une impression d'absence de répit. Le cyberharcèlement ne se limite donc pas à une succession de messages ou de publications : il constitue une dynamique de pression, d'exposition et d'épuisement, dont les effets peuvent se prolonger bien au-delà du moment où les contenus sont publiés.

---

[6] Théorisé par William Gibson dans un ouvrage de science-fiction en 1984, Catherine Blaya, professeur en science de l'éducation à l'Université de Lausanne, l'interprète comme suit : « cyberespace est une hallucination consensuelle vécue au quotidien par des milliers d'opérateurs, y compris les enfants. Il s'agit d'une représentation de constellations de données extraites des données des ordinateurs. Il s'agit d'un univers immatériel produit de l'intellect. Dans cet espace, les humains peuvent naviguer et se créer de nouvelles identités cybernétiques dans un jeu labile de mises en scène de soi dans l'interface avec les autres internautes, sans limite de temps ou d'espace ». Blaya, C. (2013). *Introduction. Les ados dans le cyberespace : Prises de risque et cyberviolence* (p. 9-12). De Boeck Supérieur. https://shs.cairn.info/les-ados-dans-le-cyberespace--9782804175948-page-9?lang=fr.

[7] Blaya, C. (2018). Le cyberharcèlement chez les jeunes. Enfance, 2018(3), 421–439. https://doi.org/10.3917/enf2.183.0421

[8] D'après le Code pénal (art. 222-33-2-1), le harcèlement « lorsqu'ils ont été commis par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique » est passible de 2 ans d'emprisonnement et de 30 000 euros d'amende. Les caractères sexiste, sexuel de ces violences ou encore le fait qu'elles se produisent dans un cadre conjugal, ou impliquant un mineur, sont également des facteurs aggravants.

Le stalking*

Définition. Défini comme « une forme grave de harcèlement mêlant recherche d'intimité avec une victime et violation de sa vie privée »[9], le *stalking** est un anglicisme qui peut directement se traduire en français par les expressions « traquer » ou « rôder ». En d'autres termes, le *stalking* est une forme de harcèlement à caractère obsessionnel, où les faits et gestes de la victime sont surveillés continuellement. Ce phénomène existe aussi bien en ligne que dans le monde physique. Dans le cadre des cyberviolences, le *stalking* s'effectue donc en ligne, par un stalker qui cherche à surveiller voire interagir de manière répétée avec la victime, qui, elle, n'a jamais consenti à cette surveillance ni aux échanges.

Exemples. Il peut s'agir d'un *stalker* voulant à tout prix entrer en contact avec la victime par des envois répétés de messages ou par l'usage du harcèlement téléphonique. Mais le *stalker* peut aussi se dissimuler, par exemple en créant de faux comptes sur les réseaux sociaux, afin de surveiller la victime à distance tout en occultant sa véritable identité.

Le *stalking* est considéré comme une agression de la sphère privée des individus. Ses effets sur la victime sont notables. Cette conduite peut aboutir à un sentiment de peur permanente, dans l'idée d'une possible réitération du harcèlement. Légalement, le *stalking* est associé au harcèlement moral.

La menace*

Définition. Définie par le Centre National de Ressources Textuelles et Lexicales[11], comme la « manifestation de la violence par laquelle on signifie à autrui l'intention que l'on a de faire du mal », la menace est une agression verbale largement répandue sur internet et dont la banalisation interroge autant qu'elle inquiète. L'acception ici retenue met l'accent sur l'intention de l'auteur – créer un climat de peur chez la victime, cette dernière craignant la survenance d'un dommage.

Nature et degré de gravité. Les menaces peuvent revêtir différentes formes, entraînant une variation de leur degré de gravité. Ainsi, cette violence peut se manifester par des menaces de diffamation*, de diffusion d'informations ou de contenus, mais peut également aller jusqu'à des menaces de viol ou d'atteinte à la vie. Toutefois, si la nature et le degré des menaces peuvent varier, elles ne devraient jamais être minimisées dans la mesure où elles sont susceptibles de créer chez la victime un sentiment d'insécurité.

Modalités et exemples. Les menaces en ligne sont souvent mises en place par l'intermédiaire du chantage, c'est-à-dire que les menaces sont pour l'agresseur un moyen de pression pour obtenir un avantage de la victime tel que de l'argent ou des informations personnelles. Un exemple concret d'arnaque en ligne consiste à menacer la victime de divulguer certaines informations personnelles si cette dernière n'envoie pas une certaine somme d'argent. Dans certains cas, les menaces peuvent prendre la forme de chantage à caractère sexuel, on parle alors de sextorsion. La menace qu'elle soit en ligne ou non est sanctionnée par la loi.[12]

---

[9] Gonseth, J. (2008). Stalking : une nouvelle figure de la clinique du traumatisme. *Revue Médicale Suisse*, 4(144), 472–475. https://www.revmed.ch/revue-medicale-suisse/2008/revue-medicale-suisse-144/stalking-une-nouvelle-figure-de-la-clinique-du-traumatisme

[10] Le stalking est puni par la loi dans l'article 222-33-2-2 du Code Pénal, d'au minimum 1 an de prison et 15 000 euros d'amende.

[11] Centre National de Ressources Textuelles et Lexicales (CNRTL). (s. d.). Menace. In *Dictionnaire de l'Académie française* (9e éd.). consulté le 1er février 2026 : https://www.cnrtl.fr/definition/menace

[12] Selon l'article 222-17 du Code pénal « La menace de commettre un crime ou un délit contre les personnes dont la tentative est punissable est punie de six mois d'emprisonnement et de 7 500 euros d'amende lorsqu'elle est, soit réitérée, soit matérialisée par un écrit, une image ou tout autre objet. La peine est portée à trois ans d'emprisonnement et à 45 000 euros d'amende s'il s'agit d'une menace de mort. » (8)

Harcèlement sexuel

L'upskirting

L'*upskirting** est une pratique qui consiste « en la prise de photos non consenties »[11], plus précisément « à prendre des photographies sous la jupe ou sous la robe d'une personne, capturant ainsi une image de son entrejambe, et donc, ses sous-vêtements et parfois ses parties intimes, sans son consentement ».

Cette pratique est bien liée à la notion de cyberviolences puisque les auteurs de l'acte se permettent d'attenter à l'intimité des victimes sans leur consentement via la prise de clichés. Ces photographies peuvent servir à des fins personnelles, mais peuvent aussi être partagées ou publiées en ligne (sites pornographiques, compte fisha*...).

L'*upskirting* est une violation de l'intimité des victimes. Ces photographies sont souvent prises dans des lieux publics, comme « les grandes surfaces, les cabines d'essayage, la rue, les transports en commun et les toilettes publiques ». Ce mode opératoire est à l'origine d'un rétrécissement de l'espace public pour celleux qui veulent se sentir libre de se vêtir selon leurs préférences. Cela participe d'un mécanisme misogyne de contrôle des corps, qui limite concrètement leur liberté de circuler.

Le cybercontrôle coercitif*

Le contrôle coercitif au sein du couple s'enracine dans des rapports de domination genrés préexistants, qui en constituent à la fois le terreau et le cadre de légitimation. C'est pourquoi ces violences s'observent davantage au sein de couples hétérosexuels, et sont majoritairement exercées par des hommes à l'encontre de femmes. Elles prennent par ailleurs des formes spécifiques lorsque s'y articulent d'autres rapports de domination, liés notamment à la classe sociale, à la racisation ou à une situation de handicap.

Le contrôle coercitif peut prendre de multiples formes. Il constitue une stratégie globale de domination, d'emprise et d'appropriation de l'autre, fondée sur l'accumulation de pratiques de surveillance, d'humiliation, d'isolement, de harcèlement, de manipulation psychologique, ainsi que de violences sexuelles, économiques ou physiques.

L'usage des outils numériques permet de déployer ces stratégies dans de nouveaux espaces et d'en renforcer les effets. Les cyberviolences se caractérisent notamment par la possibilité de recourir au pseudonymat ou à une dissimulation partielle de l'identité, par la viralité des contenus, par leur persistance dans le temps, ainsi que par la distance créée par l'écran. Ces caractéristiques peuvent accroître le pouvoir de contrôle de l'auteur, renforcer l'isolement de la victime et prolonger les violences au-delà des interactions physiques ou du temps passé au sein du couple.

Ainsi, la surveillance se généralise même à distance ; les humiliations peuvent être encore plus visibles/vues en ligne ; la coupure de contact avec les proches de l'autre peut se faire à distance, le harcèlement peut se poursuivre quotidiennement en ligne et par différents biais quand bien même il y a eu rupture ; les violences sexuelles peuvent notamment prendre des formes de chantage et menaces de diffusion de contenus intimes/sexuels ; le contrôle des documents administratifs et financiers peut aussi se faire à distance ; la géolocalisation peut par exemple permettre à l'auteur de retrouver l'autre et la violenter physiquement, entremêlant ainsi les possibilités de violences dans la vie numérique et la vie physique.

Les cyberdiscriminations*

Le cybersexisme*

Le Centre Hubertine Auclert définit le cybersexisme de la manière suivante : « un ensemble de comportements et propos sexistes sur internet, les réseaux sociaux, ou via les SMS/MMS qui reposent sur des stéréotypes sur les femmes et les hommes, sur des injonctions concernant la sexualité, la manière de s'habiller, l'apparence physique ou le comportement notamment des femmes ». En outre, il constitue un continuum des dynamiques sexistes de nos sociétés dans l'univers numérique. Il peut prendre la forme d'expressions misogynes « classiques » largement banalisées (telles que la diffusion de propos stigmatisants comme « une femme ne devrait pas être musclée » ou un jugement sur le « *bodycount** »), voire appuyés par la généralisation des contenus masculinistes (injonctions à rester chez soi si l'on est une femme, à s'apprêter pour plaire, à se soumettre aux volontés d'un homme). Le cybersexisme peut également se manifester par une généralisation du *slut-shaming** de masse, visant à humilier les femmes, à stigmatiser certains comportements et manières d'être, « en la renvoyant à la figure de la `salope´ ».

Par ailleurs, parler de cybersexisme ne renvoie pas seulement aux contenus explicites mais également à l'architecture même des algorithmes* qui participent à la sexualisation du corps féminin. Par exemple, le contenu posté par une femme sur un réseau social est plus visible (comprendre « plus largement montré à un grand nombre d'auteur·ices ») si la femme y est en partie dénudée. Le mot « écolière » tapé dans la barre de recherche Google renvoie rapidement à des sites types pornographiques où la posture de l'écolière est montrée comme un fantasme sexuel banalisant la pédocriminalité.

Enfin, parler de cybersexisme c'est également évoquer la différence d'accès et de représentation des femmes, et des minorités de genre, dans le domaine de la Tech (au sens professionnel). D'après une étude de l'INSEE, publiée en 2023, seulement 24 % des personnes travaillant dans le domaine de la Tech sont des femmes et, parmi elles, seulement 27 % occupent des postes d'ingénieures.[13]

En 1989, Kimberlé Crenshaw, juriste états-unienne et théoricienne critique du droit, introduit la notion d'« intersectionnalité* » pour désigner la manière dont certaines discriminations ne peuvent être comprises séparément, dès lors qu'elles se situent au croisement de plusieurs rapports de domination. Dans ses travaux sur les violences faites aux femmes racisées, elle montre notamment que les expériences des femmes noires ne sont pleinement intelligibles ni depuis le seul cadre du sexisme*, ni depuis le seul cadre du racisme, mais à partir de leur articulation avec d'autres rapports sociaux, tels que la classe ou la sexualité.[14] Ainsi, les cyberviolences peuvent être pensées et précisées en fonction des dynamiques oppressives qui les traversent. Grâce à la flexibilité de la langue, de nouveaux termes « valises » permettent de désigner ces violences, dont voici plusieurs exemples (non exhaustifs) :

La cybermisogynoir : Contraction de « cyber », « misogynie » et « noire », ce terme désigne l'ensemble des cyberviolences visant à discriminer une personne en fonction de son genre ET de sa couleur de peau.

La cyberarabisogynie* : ce mot renvoie aux termes « cyber », « arabe » et « misogynie ». Il désigne les cyberviolences s'exerçant à l'égard des femmes arabes, en raison de leur genre et de leur origine. Ces cyberviolences se traduisent donc par une stigmatisation à la fois misogyne et raciste des femmes arabes.

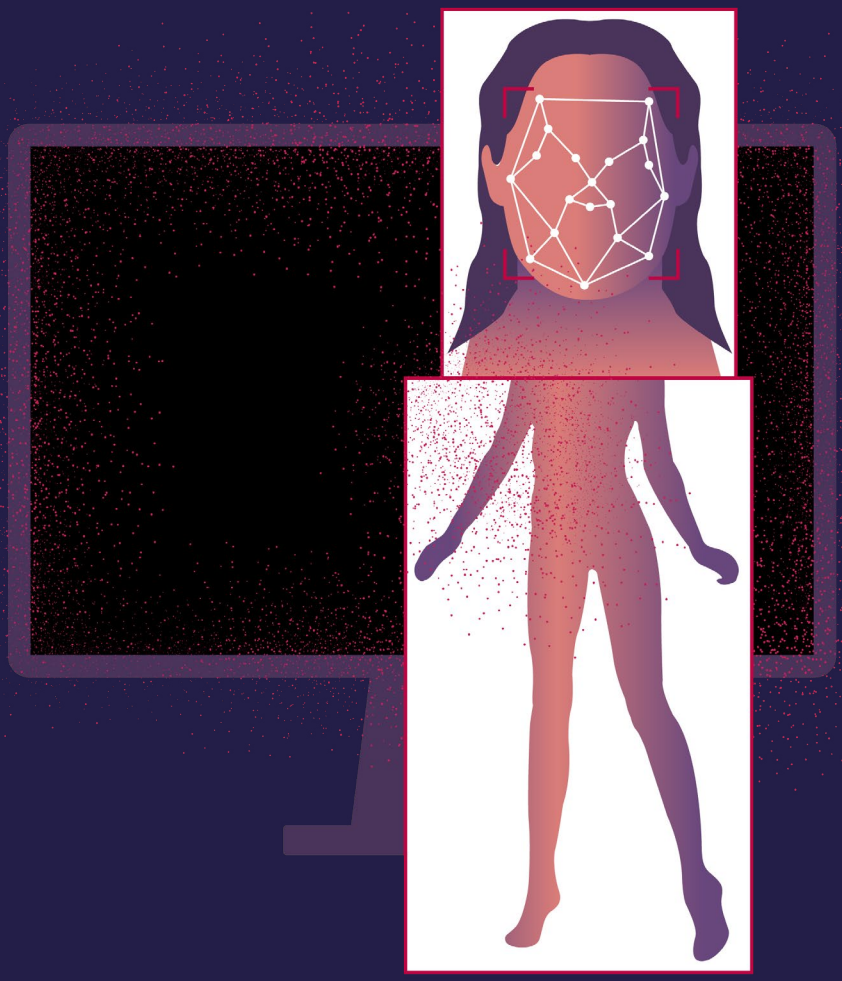
---

[13] Poty, A. (2023). Les femmes restent très minoritaires dans les métiers de la transformation numérique et du développement durable. Insee Références, *Emploi, chômage, revenus du travail*, édition 2023. Insee.
[14] Crenshaw, K. W., & Bonis, O. (2005). Cartographies des marges : intersectionnalité, politique de l'identité et violences contre les femmes de couleur. *Cahiers du Genre*, 39(2), 51-82. https://doi.org/10.3917/cdge.039.0051

Les cyberLGBTQIAphobies* : Ce terme renvoie à « cyber », « LGBTQIA+ » et « phobies ». Il désigne donc les violences numériques touchant spécifiquement les personnes s'identifiant ou identifiées comme appartenant à la communauté LGBTQIA+, en raison de leur genre et/ou de leur orientation sexuelle. Par exemple, ces cyberviolences peuvent se traduire par le « *cyberouting** », c'est-à-dire le fait de révéler l'orientation sexuelle ou l'identité de genre* d'une personne, réelles ou supposées, en ligne, sans consentement de sa part. Cela peut passer par la publication d'une photo sur les réseaux sociaux, de la personne ciblée avec sa ou son partenaire.

Le cybervalidisme* : ce terme se réfère à la notion de « validisme », pensée pour désigner les discriminations visant, explicitement ou non, les personnes avec un handicap, c'est-à-dire « non-valides ».

La cybergrossophobie* : renvoyant à la « grossophobie », ce terme désigne toutes les cyberviolences discriminantes envers les personnes perçues comme grosses.



I. ÉTAT DES LIEUX DES CVSS

Documenter pour comprendre. Procéder à l'état des lieux des cyberviolences à caractère sexiste ou sexuel permettra de mieux en appréhender les ressorts. La connaissance de la problématique par le grand public, la typologie des victimes, les différents espaces de survenance de ces violences ainsi que les recours disponibles pour se protéger ou faire face à celles-ci sont autant d'angles qui sont ici interrogés afin de rendre compte des réalités plurielles que recouvrent ces violences. Un tel travail doit ainsi faciliter la compréhension des dynamiques qui sont à l'œuvre et pourra servir de base à l'édification de politiques publiques ambitieuses.

1. Connaissance des cyberviolences sexistes et sexuelles

Intérêts d'un meilleur repérage. L'identification des cyberviolences sexistes et sexuelles (CVSS) constitue un préalable indispensable à toute politique de prévention et de prise en charge des victimes. Identifier ces violences permet de mieux comprendre les dynamiques sociales et numériques qui les produisent et les font perdurer, mais aussi de reconnaître les situations de victimisation. Cet enjeu concerne à la fois les pouvoirs publics, dans la conception d'initiatives de sensibilisation adaptées mais également l'ensemble des internautes afin de mieux prévenir les violences, soutenir ses proches et s'extraire de certains flous sémantiques en raison desquels les victimes peuvent ne pas se reconnaître comme telles.

A - Repérage des cyberviolences sexistes et sexuelles

Familiarité de surface. Les résultats de la Grande Enquête témoignent d'une familiarité très élevée avec les notions les plus générales relatives aux cyberviolences. Ainsi, ce sont pas moins de :

99 %

des répondant·es qui déclarent savoir ce qu'est le cyberharcèlement

95 %

qui identifient la diffusion non consentie de contenus intimes comme l'une des formes que peuvent prendre les cyberviolences.

Ces niveaux de connaissance sont relativement homogènes, que les répondant·es aient ou non déjà été victimes, ce qui traduit une large diffusion de ces concepts auprès du grand public. Toutefois, si ces notions bénéficient d'une importante popularité, il en va différemment des autres formes de cyberviolences.

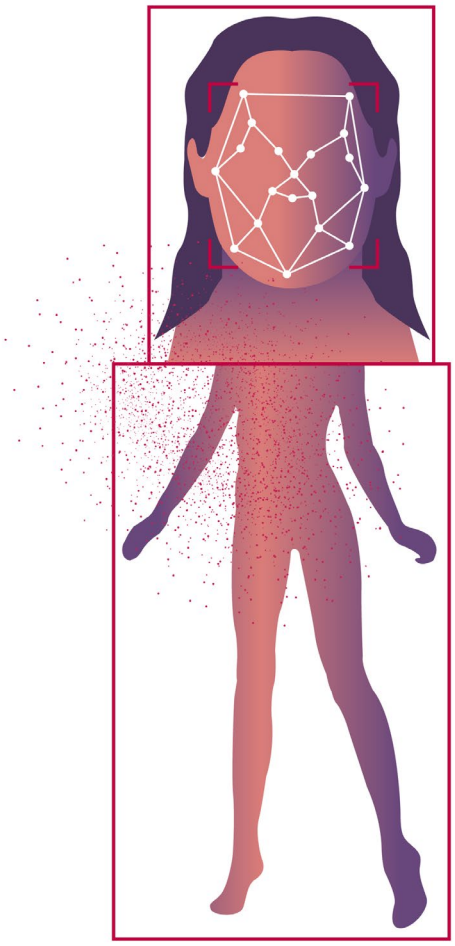
Connaissances partielles. Cette connaissance générale s'atténue notablement lorsqu'il s'agit d'identifier des formes plus spécifiques de cyberviolences. Ce sont ainsi :

59 %
des répondant·es savent ce qu'est la sextorsion[1]

38 %
identifient le *grooming**

24 %
reconnaissent une situation de *doxing**

Ces écarts révèlent une connaissance principalement abstraite du cyberharcèlement, dissociée de la diversité des pratiques concrètes qui le composent. Les termes techniques, souvent issus de l'anglais, constituent un frein à la compréhension et à la qualification des faits, y compris pour les personnes ayant déjà subi des violences numériques.



Exception du *deepfake*. Les deepfakes constituent une exception notable à cette tendance. Ce sont plus de 80 % des répondant·es qui déclarent savoir ce que ce terme recouvre, qu'iels aient été victimes ou non de cyberviolences. Cette importante reconnaissance pourrait aisément s'expliquer par la médiatisation croissante des outils d'intelligence artificielle générative et des usages qui en sont faits[2] – tel que la création d'images à vocation humoristique[3].

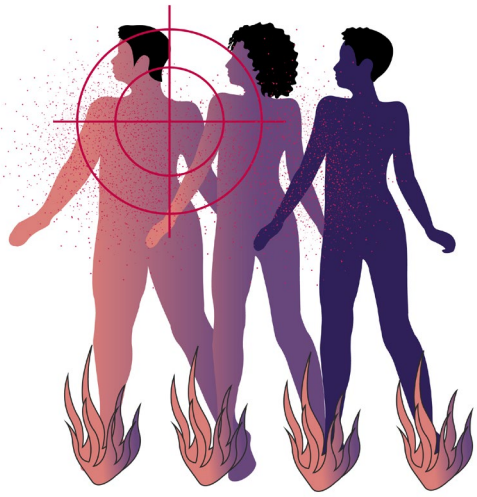
Vigilance de rigueur. Cependant, si le terme paraît largement connu, la compréhension de son usage comme instrument de violences sexistes et sexuelles – notamment par l'association non consentie d'images pornographiques[4] à l'identité d'une tierce personne – demeure incertaine et appelle une vigilance particulière. À ce sujet, l'ONG Deeptrace avançait que 96 % des *deepfakes* vidéos sont à caractère pornographique tandis que 99 % des victimes sont des femmes[5]. En début d'année 2026, le scandale provoqué par l'utilisation de l'intelligence artificielle Grok pour produire facilement et rapidement de nombreuses images de femmes dénudées à partir de photos publiées sur le réseau social X a permis de mettre en lumière le caractère profondément violent de certains usages du *deepfake* et leur inscription dans une logique de domination sexiste et sexuelle.

---

[1] Chantage visant à extorquer à une personne des contenus à caractère sexuel, sous la menace de diffusion de contenus préalablement obtenus ou d'autres types de violences. Le mécanisme de sextorsion peut aller jusqu'au viol.
[2] Voir les reportages suivants : Hofmeier S. Qu'est-ce-qu'un deepfake ?. 2025. ARTE. https://www.arte.tv/fr/videos/125796-000-A/qu-est-ce-qu-un-deepfake
Agence Française de Presse. Deepfake, les méthodes de réalisation. Février 2025. Consulté le 21/11/2025. https://youtu.be/OkFMfA93BM4?si=Lp4V1V22Fqky_BEM
France 3 Occitanie.Tout le monde peut faire un deepfake ? Juillet 2025. Consulté le 21/11/2025. https://youtu.be/XPyjXeP89Kk?si=klWU2nYSb2pmMm8q
[3] Ronfaut L. Deepfake : Avant la présidentielle, le grand faux dans l'inconnu. 14/05/2021. https://www.liberation.fr/economie/economie-numerique/deepfakes-avant-la-presidentielle-le-grand-faux-dans-linconnu-20210514_ZDSIMQUA5BH3TNJBC2AJ5I4O3E/
[4] Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). *The State of Deepfakes: Landscape, Threats, and Impact*. Deeptrace Labs. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf
[5] Security Hero. (2023). 2023 *State of Deepfakes: Realities, Threats, and Impact*. Security Hero. https://www.securityhero.io/state-of-deepfakes

Perception des cyberviolences. La Grande Enquête a aussi permis d'évaluer la proportion des répondant·es qui perçoivent certaines pratiques comme des cyberviolences sexistes et sexuelles après une brève sensibilisation essentiellement destinée à en définir les contours. Les formes de violences les plus explicites font ainsi l'objet d'une reconnaissance quasi unanime : les comptes « fisha », les *dickpics*, le *grooming*, l'*upskirting*, les injures sexistes ou encore les violences conjugales facilitées par la technologie sont identifiés comme des violences numériques à caractère sexuel ou sexiste par plus de 90 % des répondant·es. Ces résultats montrent que le grand public s'accorde à reconnaître le caractère violent et attentatoire aux droits d'autrui qui caractérisent ces pratiques.

Cas du *stalking*. À l'inverse, certaines pratiques ne sont pas toujours perçues par les répondant·es comme des cyberviolences.



Le cas du *stalking* en est un exemple éloquent ; majoritairement mobilisé à des fins de domination, de contrôle et de discrimination[6], il se démarque pourtant comme la cyberviolence sexiste et sexuelle la moins reconnue, avec 61 % des répondant·es qui la qualifient comme telle.

Cette reconnaissance limitée peut s'expliquer par la banalisation – voire la romantisation – de certaines formes de surveillance ou d'insistance relationnelle en ligne. Le fait que cette proportion soit légèrement plus élevée chez les personnes ayant déjà subi des cyberviolences (63 % contre 57 % pour les non-victimes) suggère que l'expérience vécue joue un rôle dans la capacité à identifier ces pratiques comme constitutives d'une violence. Reste que, dans tous les cas, le *stalker*, c'est-à-dire la personne traquant les faits et gestes d'autrui en ligne, se complait dans le pseudonymat et profite de la facilité d'accès à de nombreuses données personnelles, ce qui est largement facilité par la conception actuelle des principaux réseaux sociaux.

Conclusion.

Pris dans leur ensemble, ces résultats mettent en évidence un décalage entre la connaissance abstraite des cyberviolences et la reconnaissance fine de leurs manifestations diverses et variées. Si certaines pratiques sont aujourd'hui clairement identifiées comme des violences sexistes et sexuelles, d'autres restent insuffisamment – ou mal – nommées et reconnues, contribuant à leur banalisation et à l'invisibilisation des victimes. Ce constat souligne l'importance d'actions de sensibilisation ciblées, visant non seulement à diffuser des catégories juridiques ou techniques, mais aussi à expliciter les mécanismes concrets par lesquels s'exercent les cyberviolences dans les espaces numériques.

---

[6] Rodríguez-Castro, Y., Martínez-Román, R., Alonso-Ruido, P., Adá-Lameiras, A., & Carrera-Fernández, M. V. (2021). Intimate Partner Cyberstalking, Sexism, Pornography, and Sexting in Adolescents: New Challenges for Sex Education. International Journal of Environmental Research and Public Health, 18(4), 2181.

B - Connaissance du cadre légal

Des infractions identifiées. Les répondant·es ont été interrogé·es sur leur connaissance préalable du caractère pénalement répréhensible des violences commises en ligne. Les résultats font apparaître une reconnaissance très élevée du caractère infractionnel des formes de cyberviolences les plus médiatisées. Parmi les 2 116 personnes ayant répondu à l'enquête, plus de 90 % déclarent savoir que le cyberharcèlement sexuel* et la diffusion non consentie de contenus intimes constituent des infractions pénales.

94 %

Ainsi, 94 % des répondant·es savaient, avant de répondre au questionnaire, que le cyberharcèlement constituait une infraction pénale

92 %

identifiaient la diffusion non consentie de contenus intimes comme pénalement sanctionnée.

Ces résultats confirment que ces violences, qui étaient déjà perçues comme telles par les répondant·es, sont également connues comme des infractions à la loi par la plupart d'entre eux. On peut présumer ici que la médiatisation régulière d'affaires portant sur ces enjeux permet d'en rappeler le caractère pénalement répréhensible.

Appréhension inégale. Cette reconnaissance s'atténue sensiblement lorsqu'il s'agit d'autres formes de cyberviolences sexistes et sexuelles. La sextorsion et la production ou diffusion de deepfakes à caractère sexuel sont identifiées comme des infractions pénales par une plus faible majorité de répondant·es :

63 %

pour la sextorsion

59 %

pour les *deepfakes* sexuels.

La connaissance de leur caractère infractionnel apparaît relativement homogène selon le statut des répondant·es : l'écart observé entre victimes et non-victimes ne dépasse pas deux points de pourcentage. Ce constat suggère que la méconnaissance de ces infractions ne relève pas tant de l'expérience vécue mais davantage d'un déficit général de sensibilisation et d'information juridique. Le caractère infractionnel de certaines cyberviolences demeure largement méconnu. Ainsi, seul·es

45 %

des répondant·es déclarent savoir que le grooming constitue une infraction pénale

31 %

identifient le *doxing* comme tel.

Peines méconnues. Enfin, les répondant·es ont été interrogé·es sur leur connaissance des peines encourues par les auteurs de cyberviolences sexistes et sexuelles.

› Une majorité significative – 65 % – déclarent ne pas savoir que les sanctions pénales applicables peuvent être élevées.

Les limites de l'enquête ne permettent toutefois ni de définir ce que recouvre, pour les répondant·es, la notion de « peine élevée », ni d'en déduire l'impact concret de cette perception sur le recours à la justice.

› Il ressort néanmoins que seuls 35 % des répondant·es ont conscience du niveau potentiellement dissuasif des peines encourues.

Méconnaissance cumulative. Cette méconnaissance du cadre pénal s'inscrit dans la continuité des résultats relatifs au repérage des cyberviolences. Les pratiques les moins identifiées comme des cyberviolences sexistes et sexuelles sont également celles dont le caractère infractionnel est le moins connu. La terminologie employée, parfois issue de l'anglais, n'en facilite pas l'appréhension : elle complexifie au contraire l'identification des faits, tant sur le plan social que juridique et fait obstacle à la compréhension des possibilités de recours offertes par le droit.

Entrave au recours. Lorsqu'une situation n'est ni clairement identifiée comme une violence, ni admise comme une infraction, les perspectives de dépôt de plainte, de signalement ou de recherche de soutien institutionnel s'en trouvent mécaniquement réduites. Ces résultats invitent ainsi à renforcer les actions d'information juridique, en les articulant étroitement aux efforts de sensibilisation es par le secteur associatif sur les formes concrètes que peuvent prendre les cyberviolences sexistes et sexuelles.

C - Accès au droit, à l'information et aux ressources

1 - Information et sensibilisation des publics

Déficit d'information. L'enquête révèle un décalage préoccupant entre l'ampleur des cyberviolences sexistes et sexuelles et le niveau d'information du public à leur sujet. Ainsi,

58 %

des répondant·es non victimes

48 %

des répondant·es victimes confient ne pas se sentir suffisamment informé·es sur ces violences.

Ce constat interroge directement la responsabilité des acteurs publics et privés dans la diffusion d'une information accessible et adaptée. L'information du public constitue en effet un préalable indispensable à toute stratégie de prévention et d'accompagnement : elle conditionne la capacité des victimes à identifier leur situation, à connaître leurs droits et à accéder aux ressources d'aide. Or, cette information demeure largement défaillante, les pouvoirs publics comme les plateformes numériques déléguant souvent cette mission aux associations, lesquelles ne disposent pas toujours des moyens financiers nécessaires pour concevoir et déployer des campagnes susceptibles d'atteindre une audience élargie.

Relative stagnation du taux de sensibilisation. Une enquête réalisée par l'institut IPSOS pour l'association Féministes contre le cyberharcèlement en 2021 faisait déjà apparaître des niveaux de méconnaissance comparables :

> plus de la moitié des français·es déclaraient ne pas savoir (59 %)
> ou ne pas avoir su (52 %) comment réagir ni à qui s'adresser en tant que victime

Cette méconnaissance s'accompagnait d'une forte disparité de genre, les femmes victimes étant significativement plus nombreuses (66 %) que les hommes (39 %) à déclarer ne pas avoir su comment réagir[7]. Quatre ans plus tard, les résultats de la présente enquête témoignent d'une absence d'amélioration substantielle. Cette stagnation révèle l'insuffisance des politiques publiques de sensibilisation menées au cours de cette période et appelle à une refonte en profondeur des stratégies d'information, tant dans leur ampleur que dans leurs modalités de diffusion.

Devoir de prévention. Le fait que les victimes déclarent se sentir légèrement plus informées que les non-victimes (52 % contre 42 %) suggère que l'accès à l'information intervient fréquemment après coup, à l'occasion du parcours d'orientation et d'accompagnement consécutif aux violences subies. Cette logique réactive – où l'information est délivrée en réponse à une situation de victimisation déjà constituée – témoigne d'une carence en matière de prévention primaire. Elle souligne la nécessité de développer des actions d'information et de sensibilisation en amont, destinées à l'ensemble de la population, afin de favoriser une compréhension partagée des cyberviolences sexistes et sexuelles et de réduire les obstacles à leur identification.

Limites des « bons réflexes ». Par ailleurs, les injonctions à adopter des réflexes de protection peuvent perdre en pertinence lorsque l'on se heurte à des attaques particulièrement violentes et multiples dans les formes qu'elles peuvent revêtir. Les actions qui consistent à signaler, à faire des captures d'écran horodatées qui pourront servir de preuves lors d'un éventuel dépôt de plainte, à bloquer les agresseurs, à en parler à des personnes de confiance, à des associations spécialisées ou à des professionnel·les de santé, font partie de l'arsenal que l'on peut déployer pour mieux lutter contre les cyberviolences, mais il n'est pas toujours possible ou aisé de les mettre en œuvre pour les victimes qui sont parfois extrêmement affectées, voire atteintes de stress post-traumatique[8].

---

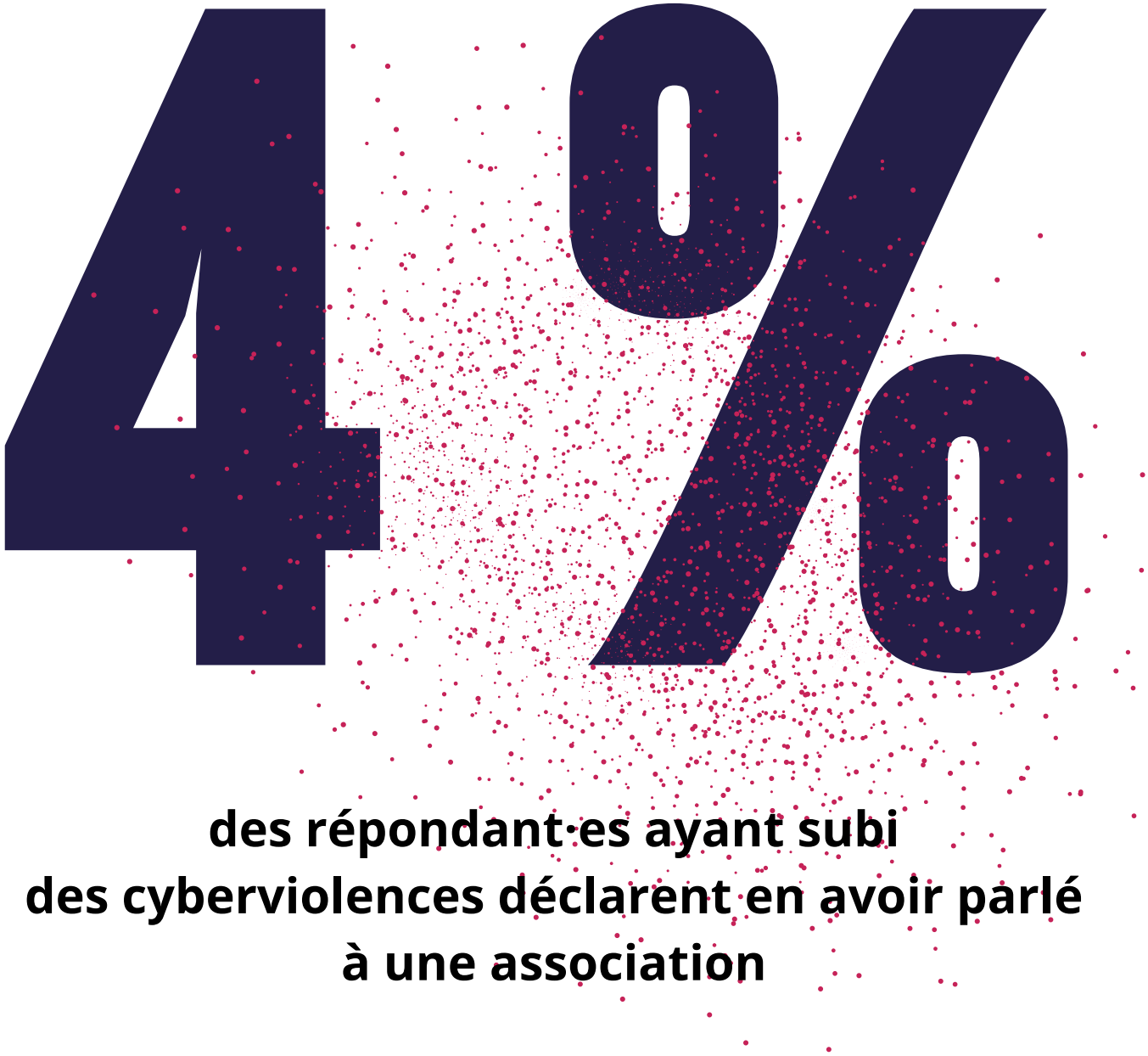
[7] Féministes contre le cyberharcèlement & IPSOS. (2021, novembre). *Cyberviolence et cyberharcèlement : état des lieux d'un phénomène répandu* [Enquête conduite par IPSOS auprès de 1 008 Français·es âgé·es de 18 ans ou plus].

[8] Plus d'une victime de cyberviolences sur trois (35 %) présente tous les symptômes du stress post-traumatique. University of Bedfordshire. (2011). *Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey* (p. 26).

2 - Connaissance et recours aux structures associatives

Foisonnement du tissu associatif. Des structures associatives susceptibles d'apporter des informations, des outils et un accompagnement aux victimes de cyberviolences existent en France. Certaines sont spécialisées dans la lutte contre les cyberviolences[9], tandis que d'autres intègrent cette dimension à un champ d'intervention plus large[10].

Méconnaissance des structures d'aide. Cependant, malgré la richesse de ce tissu associatif, seul·es :



des répondant·es ayant subi des cyberviolences déclarent en avoir parlé à une association

[9] Féministes contre le cyberharcèlement, Point de Contact, #StopFisha, Echap, Wiquaya, LutteHSM ou e-Enfance.
[10] Fédération nationale des centres d'informations sur les droits des femmes et des familles (FNCIDFF), En Avant Toute(s), SOS Homophobie ou la Fédération nationale solidarité femmes (FNSF)

Ce taux extrêmement faible traduit à la fois une méconnaissance de l'existence de ces structures et une difficulté à identifier leurs modalités d'intervention. L'absence de plateforme d'information centralisée, associée à la faiblesse des campagnes de communication institutionnelle, contribue à invisibiliser les ressources disponibles. Ce déficit d'information est d'autant plus préoccupant que :

plus d'un quart des répondant·es victimes déclarent n'en avoir parlé à personne.

Ce chiffre témoigne de l'isolement qui touche de nombreuses victimes et qui renforce les conséquences psychologiques et sociales des violences subies. L'accès à un accompagnement adapté constitue pourtant un facteur déterminant dans le processus de sortie de la violence et dans la capacité des victimes à faire valoir leurs droits.

Accessibilité et inclusivité des dispositifs. Une meilleure information des publics sur l'existence et les modalités d'intervention des structures associatives pourrait contribuer à rompre cet isolement. Cette information doit cependant aller au-delà de la simple mention de coordonnées : elle doit expliciter les formes concrètes d'accompagnement proposées – soutien juridique, psychologique, technique –, les délais de prise en charge et les conditions d'accès aux services. Elle doit également être pensée dans une perspective inclusive, en tenant compte des obstacles spécifiques rencontrés par certains publics : personnes en situation de handicap, personnes LGBTQIA+, personnes migrantes, personnes en situation de précarité numérique ou linguistique.

Enfin, elle doit être diffusée de manière proactive et régulière, à travers une pluralité de canaux – campagnes audiovisuelles, affichage dans les lieux publics, partenariats avec les établissements scolaires et universitaires, présence sur les réseaux sociaux – afin d'assurer une visibilité durable et d'ancrer ces ressources dans l'espace public.

2. Panorama des victimes de cyberviolences sexistes

Tous les prénoms cités ont été modifiés et les témoignages anonymisés.

Célia,
répondante Grande Enquête CVSS

Femme,
17 ans au moment de la cyberviolence

Victime de diffusion non consentie de contenu intime

Célia était en couple depuis ses 15 ans lorsqu'après leur rupture, son ex-partenaire a diffusé sur Facebook une photo intime d'elle, qu'il avait lui-même prise en insistant et en promettant de la supprimer. Bien que l'image ait été retirée quelques heures plus tard, le préjudice était déjà causé. En découvrant la publication, elle a simplement éteint son ordinateur, sans savoir comment signaler le contenu ni vers qui se tourner. Elle n'a pas pu en parler à ses parents, mais a trouvé du soutien auprès de ses ami·es et de son petit frère.

Pendant deux mois, les violences se sont poursuivies sous forme de harcèlement et de menaces par SMS. À l'époque, elle ne percevait pas pleinement l'anormalité de la situation ; ce n'est qu'à l'apparition de menaces de violences physiques qu'elle a pris conscience de la gravité des faits. La compréhension plus profonde de ce qu'elle avait subi est intervenue des années plus tard, à travers les conséquences durables sur son estime d'elle-même et son rapport à son corps. Elle a notamment développé des troubles du comportement alimentaire et traversé un épisode dépressif après les faits.

"Dans un monde idéal, ce qui m'aurait le plus aidé à l'époque c'est de savoir comment signaler un contenu, savoir ce que cela signifie d'avoir une identité en ligne, qu'est-ce que nous on en fait et qu'est-ce que les autres ont le droit d'en faire. Connaître mes droits, pouvoir reconnaître et nommer les violences."

Juliette,
répondante Grande Enquête CVSS

Femme,
entre 15 ans et 20 ans

Victime de *grooming*, demande de contenu à caractère sexuel, violences sexuelles

À 15 ans, sur un forum en ligne, Juliette rencontre un internaute qui dit avoir 17 ans. Elle apprendra plus tard qu'il s'agissait en réalité d'un homme de 38 ans. Pendant plusieurs années, elle s'est retrouvée sous son emprise dans une relation où elle a subi de nombreuses violences psychologiques, physiques et sexuelles, dont un viol à l'âge de 18 ans. L'homme en question travaillerait dans l'éducation nationale. Pour elle, c'est la honte qui l'a empêchée de parler de ce qu'elle vivait. Par ailleurs, son entourage – des ami·es et ami·es d'ami·es – avait tendance à minimiser cette situation ou à la culpabiliser. Ce n'est que sept ans après la rencontre, grâce à des tiers qui lui ont fait réaliser la gravité des faits en utilisant notamment le terme pédocriminalité, qu'elle a pu prendre toute la mesure de la situation. Ces violences ont entraîné de lourdes conséquences sur sa vie et sa santé mentale, dont la perte de son travail, des épisodes psychotiques et une tentative de suicide. Elle a porté plainte pour le viol, mais n'a toujours pas de nouvelles de sa plainte, plusieurs années après.

"J'ai rencontré cet homme à 15 ans, mais dès l'âge de 11 ans j'avais des discussions en ligne avec des personnes majeures. Il est essentiel de ne pas culpabiliser les enfants : il faut être dans une optique de réduction des risques, et la culpabilité empêche de parler"

Clara,
victime affaire French Bukkake, suivie par Point de Contact

Femme,
28 ans

Victime de diffusions non consenties de contenus constitutifs de viols

Clara a participé au tournage de contenus initialement présentés comme pornographiques et qui seront plus tard diffusés massivement sur des plateformes très fréquentées. Les violences représentées dans ces contenus ont ensuite fait l'objet de poursuites judiciaires. La justice a finalement reconnu la gravité des faits : Clara et plusieurs de ses coplaignantes ont obtenu gain de cause, les faits étant qualifiés de viols en réunion avec circonstances aggravantes de racisme et de sexisme.

Malgré cette décision judiciaire définitive en 2025, les contenus continuent d'être largement téléchargés et republiés, exposant Clara et ses coplaignantes à une revictimisation* constante. Face à cette situation, elles ont sollicité Point de Contact pour coordonner le retrait des contenus illégaux. L'association a obtenu la suppression de plusieurs dizaines de liens dans les mois qui ont suivi, mais a également rencontré des services numériques peu coopératifs, rendant difficile la suppression complète des contenus et prolongeant l'exposition des victimes.

Noah,

répondante Grande Enquête CVSS

Femme,

entre 18 et 19 ans

Victime de cyberviolences au sein du couple et violences physiques

À 18 ans, Noah se met en couple avec un homme de 22 ans qui instaure rapidement un contrôle strict sur sa vie, principalement à distance. Il surveille ses déplacements, ses fréquentations et ses sorties, fouille son téléphone, exige l'accès à ses réseaux sociaux et utilise la géolocalisation pour la contrôler en permanence. Il la harcèle quotidiennement par appels et messages, l'empêche de dormir, l'insulte et la menace de se suicider, de la tuer ou de s'en prendre à sa famille.Il critique son apparence, lui impose de modifier son style, la contraint à supprimer ses photos puis son compte Instagram.

Lors de l'une de leurs rencontres physiques, il confisque son téléphone et la viole. Noah apprend que ces violences sexuelles ont été enregistrées et que des captures de contenus intimes envoyés sous contrainte ont été diffusées sur Telegram. Elle découvre également qu'il est marié à une autre femme, sans que cela ne mette fin à son emprise. Malgré plusieurs tentatives de rupture et l'incitation de ses proches à porter plainte, les violences persistent. Après une tentative de suicide de Noah, son agresseur disparaît définitivement, prétendument lassé de l'état de santé de Noah, notamment lié à une prise de médicaments.

"J'avais pas envie d'engager une procédure après parce qu'il faut que t'en parles et parce qu'il faut que tu rabâches des trucs. Et parce que c'est long, parce que ça coûte de l'argent, parce que je suis pas sûre d'être dédommagée à la hauteur de ce que j'ai vécu. Tu vois ce que je veux dire ? Si ça se trouve il va pas aller en prison ?"

Elodie,

signalante à Point de Contact

Femme,

entre 20 et 30 ans

Victime de diffusions non consentie de contenus sexuels

Élodie exerçait une activité de diffusion de contenus à caractère intime ou sexuel, accessibles uniquement à un public payant. Ces contenus étaient destinés à rester privés, mais de nombreuses vidéos ont été enregistrées à son insu et diffusées massivement sur des sites pornographiques depuis plus d'un an, sans son consentement.

Face à cette situation, Élodie a multiplié les signalements auprès de Point de Contact. L'association a pu l'accompagner pour faire retirer un grand nombre de vidéos et limiter leur circulation. Malgré ces démarches, son agresseur continue de republier régulièrement les contenus supprimés, maintenant un harcèlement constant et impactant son bien-être.

Paul,
répondant Grande Enquête CVSS

Homme,
32 ans

Victime de sextorsion

Paul, qui effectue un doctorat sur l'intelligence artificielle, a été victime de sextorsion via une messagerie instantanée. Après quelques échanges avec une personne qu'il a connu sur une application de rencontres, il est incité à continuer la conversation, qui prend rapidement une tournure sexuelle, sur une application tierce. Alors que la discussion se prolonge et qu'il consent à envoyer des nudes* à son interlocuteur, ce dernier coupe court soudainement aux échanges : « Comment on fait maintenant ? ». Débute alors une phase de chantage au cours de laquelle il reçoit de la part de son interlocuteur 10 coupons virtuels d'une valeur de 250€ chacun, l'agresseur exigeant de Paul leur règlement immédiat. Paul refuse de céder au chantage ; il bloque l'utilisateur, le signale aux deux plateformes et se rend rapidement en commissariat pour un dépôt de plainte. Face à la policière qui le reçoit, il se sent culpabilisé et infantilisé. On lui fait comprendre que ces pratiques ne seraient plus de son âge et on le renvoie rapidement vers la plateforme THÉSÉE, destinée aux victimes d'escroquerie en ligne, sans pour autant recueillir sa plainte.

« Le dépôt de plainte, ça a été la partie la plus dure je pense »

« C'est un peu galère de comprendre comment utiliser THESEE »

Léa,
répondante Grande Enquête CVSS

Femme,
28 ans

Victime de cyberharcèlement à caractère sexiste et sexuel

Léa, mannequin et photographe, utilisait son compte Instagram pour publier des photos et partager son opinion féministe, en commentant notamment des publications caricaturales sur le sexisme et le masculinisme*. Elle a ensuite été victime de plusieurs vagues de harcèlement massif sur la plateforme, après que son identité ait circulé au sein de réseaux masculinistes organisant des raids numériques. Le harcèlement comprenait des menaces répétées de viol et de mort, et s'est matérialisé dans le monde physique lorsqu'un homme l'a reconnue à la salle de sport. Initialement dissuadée de porter plainte par un policier, Léa a finalement déposé sa plainte, mais n'a jamais reçu de nouvelles malgré de nombreux appels et un déplacement au commissariat. Ces violences ont perduré plusieurs années, jusqu'à ce que son déménagement hors de France mette fin à ces atteintes.

Manu,
répondant Grande Enquête CVSS

Non-binaire,
entre 16 ans et 19 ans

Victime de cyberviolences conjugales et violences physiques

À 16 ans, Manu se met en couple avec une camarade de lycée plus âgée d'un an. Après plusieurs mois de relation, elle instaure un contrôle strict sur sa vie : elle surveille ses déplacements, récupère ses codes de réseaux sociaux et l'isole de ses proches en supprimant ses conversations et abonnés – dont sa meilleure amie.

Elle le viole, le contraint à envoyer et recevoir des contenus intimes et exerce un chantage affectif et sexuel. Au cours de la relation, Manu fait trois tentatives de suicide. Lorsqu'il tente de rompre, sa partenaire menace à son tour de se suicider. Des rumeurs seront ensuite diffusées à son sujet, ce qui lui vaudra d'être violemment harcelé sur les réseaux sociaux.

Malgré un soutien constant de sa meilleure amie, Manu sombre dans l'alcool et traverse un parcours de soins en hôpital psychiatrique et en centre de désintoxication qu'il suit encore aujourd'hui.

« [J'aurais eu besoin d'] une représentation de ce que je vivais, qui me dise que ça ne doit pas se passer comme ça, quand c'est une relation saine ou pas. Genre, si StopFisha était venu dans l'établissement scolaire pour dire il ne faut pas... Ouais, je pense que... ça m'aurait donné conscience et que les cyberviolences soient pas minimisées. Je sais que mon entourage n'aurait peut-être pas eu toutes les clés, n'aurait pas tout fait parfaitement, mais ça m'aurait aidé à me sortir plus facilement de là plus rapidement. Donc en fait oui, c'était... c'était un gros manque d'informations, de sensibilisation. Et puis même mon entourage, je pense que c'était pareil, ils n'avaient pas les clés en main pour voir ce qui se passait, et encore moins pour réagir. »

A - Diversité des profils de victimes

Sortir des récits caricaturaux. Les cyberviolences sexistes et sexuelles ne concernent pas qu'un profil type de victime. Bien au contraire, l'analyse croisée des résultats de la Grande enquête, des entretiens conduits dans son prolongement et des données issues du traitement des signalements reçus par Point de Contact et #Stop Fisha indique que ces violences touchent une grande diversité de personnes, sans distinction d'âge, de milieu social ou de situation géographique. Néanmoins, certaines catégories de population apparaissent surexposées, témoignant de la dimension structurellement genrée et discriminatoire de ces violences.

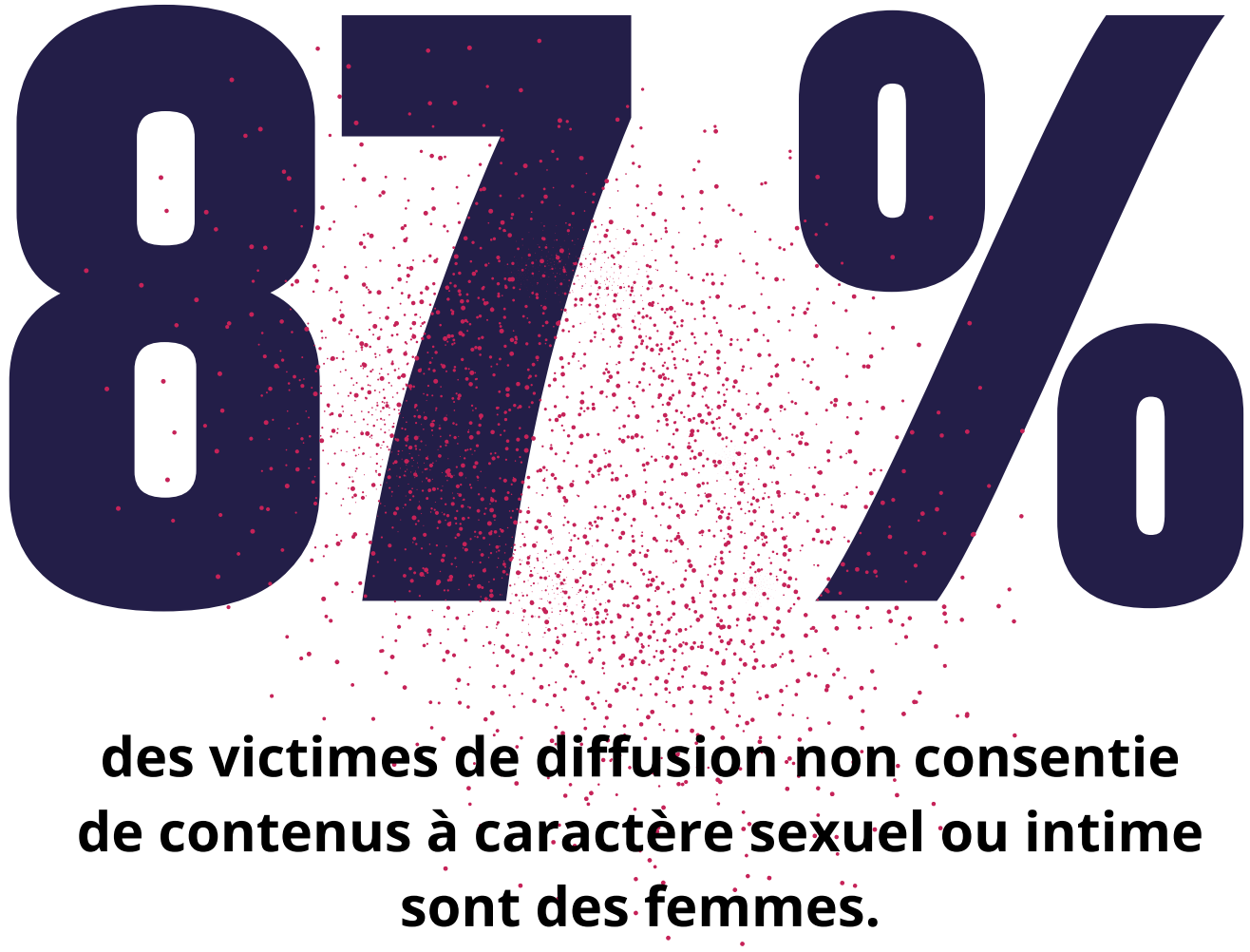
1 - Genres des victimes

Surreprésentation des femmes. À l'instar des violences commises dans le monde physique, les femmes demeurent les premières victimes des cyberviolences sexistes et sexuelles. Les résultats de la Grande Enquête montrent ainsi que

82%

des répondant·es déclarant avoir été victimes de cyberviolences sexistes et sexuelles sont de genre féminin.

UN CHIFFRE QUI PROGRESSE ENCORE DAVANTAGE SELON LA CYBERVIOLENCE CIBLÉE :



des victimes de diffusion non consentie de contenus à caractère sexuel ou intime sont des femmes.

Ces chiffres – qui doivent être manipulés avec précaution eu égard aux modalités de diffusion de cette enquête – confirment un constat issu du travail de signalement mené par Point de Contact et #StopFisha, où les femmes représentent respectivement 82 et 70 % des victimes en 2024.

Victimisation masculine et sextorsion. La diffusion non consentie de contenus sexuels, si elle constitue un phénomène manifestement genré, n'épargne pas les hommes pour autant. Ainsi :

› 21 % des hommes victimes de cyberviolences sexistes et sexuelles ayant répondu à la Grande Enquête déclarent avoir vécu une diffusion de leurs contenus sans leur accord.

Toutefois, les modalités de ces violences diffèrent : la diffusion s'accompagne souvent, chez les hommes, d'une tentative de chantage à des fins financières, relevant davantage d'une logique de sextorsion que d'humiliation publique. Ce sont pas moins de

› 65 % des hommes qui ont subi un chantage financier, contre 8 % des femmes victimes.

Ces données, bien que reposant sur de plus faibles effectifs, suggèrent l'existence de dynamiques genrées distinctes dans les formes et les finalités des cyberviolences sexuelles.

2 - Âges des victimes

Surexposition des mineur·es. En tant que public particulièrement vulnérable, les enfants et adolescent·es sont encore davantage exposés aux risques qui découlent de leurs usages des outils numériques.

Plus de la moitié des personnes ayant été victimes de cyberviolences sexistes et sexuelles au cours de leur vie (56 %) ont subi ces violences au moins une fois en étant mineures.

Ce chiffre témoigne d'une exposition particulièrement précoce et massive des jeunes à ces formes de violences. Si toutes les tranches d'âge sont représentées parmi les victimes ayant répondu à la Grande Enquête – allant de moins de 13 ans à plus de 61 ans, les catégories d'âge les plus élevées demeurent sous-représentées, ce qui révèle à la fois des usages numériques différenciés selon les générations mais aussi une probable sous-déclaration des violences chez les personnes âgées.

36 %

ont été victimes de diffusion non consentie de contenus intimes, contre

20 %

pour les victimes majeures.

Diffusion non consentie chez les mineur·es. Cette surexposition ne doit pas être imputée aux mineur·es, mais à leur vulnérabilité dans des espaces où l'apprentissage affectif et sexuel se mêle aux normes de genre, aux pressions relationnelles et au manque d'éducation au consentement. L'échange de contenus intimes peut s'inscrire dans des relations de confiance et de séduction, mais aussi résulter d'une situation de contrainte difficile à nommer. La violence naît du chantage, de la pression affective ou de la trahison du consentement : la responsabilité ne repose jamais sur les mineur·es qui ont produit ou transmis ces contenus, mais incombe à celles et ceux qui diffusent ces images sans consentement. Cette surexposition des mineur·es souligne enfin la responsabilité des adultes, institutions et plateformes dans le déficit de prévention, de protection et d'accompagnement des victimes.

3 - Motifs de discriminations chez les victimes

Discriminations et cadre légal. La discrimination constitue un mécanisme de domination fondé sur la perception et l'appréhension d'une différence. Elle naît du sentiment de supériorité d'un individu ou d'un groupe d'individus sur un autre jugé différent et s'exerce avant tout dans des configurations où une diversité est présente. Discriminer revient ainsi à utiliser la différence comme justification d'un traitement inégal. À ce titre, le droit français consacre l'interdiction de la discrimination fondée sur une variété de critères – lesquels sont énumérés à l'article 225-1 du Code pénal. Sont alors constitutives de discriminations les différences de traitement opérées entre des personnes physiques en se fondant sur des motifs tels que l'origine, l'orientation sexuelle, le genre, un handicap, une religion, l'âge, la situation économique ou encore l'état de santé.

2 - Âges des victimes

Surexposition des personnes en situation de discrimination.
L'enquête révèle que

79 %
des victimes de cyberviolences sexistes et sexuelles estiment être exposées à au moins une forme de discrimination, contre

21 %
qui n'en déclarent aucune.

Cette forte exposition témoigne du fait que les cyberviolences ne surviennent pas de manière isolée, mais s'inscrivent dans des contextes sociaux marqués par des rapports de domination préexistants.

Principales discriminations et cumul. Les discriminations auxquelles les victimes estiment être exposées concernent principalement :

50 %
le genre

29 %
l'orientation sexuelle

27 %
les opinions politiques

19 %
l'origine ou la religion

19 %
le handicap ou l'état de santé

27 %
l'apparence physique – liée à des standards de beauté ou à la couleur de peau

15 %
l'âge

Ces discriminations se cumulent fréquemment ; plus de la moitié des victimes de cyberviolences sexistes et sexuelles déclarent être touchées par au moins deux motifs de discrimination. Cette accumulation témoigne de situations d'intersectionnalité, où plusieurs systèmes de domination se conjuguent et renforcent mutuellement la vulnérabilité des personnes concernées.

Dimension genrée prépondérante. Le genre apparaît comme le critère de discrimination le plus massivement mobilisé. Cette prépondérance confirme le caractère structurellement sexiste des cyberviolences étudiées et confirme l'hypothèse selon laquelle ces violences constituent une modalité spécifique d'expression des rapports sociaux entre les genres. Même lorsque d'autres formes de discrimination s'y superposent, la dimension genrée demeure centrale, rappelant que le numérique sert de vecteur à la perpétuation et à l'intensification de violences préexistant dans le monde physique.

Caractère systémique et effets différenciés. Le fait que 21 % des victimes déclarent ne pas être exposées à d'autres formes de discrimination rappelle que les cyberviolences sexistes et sexuelles ne concernent pas uniquement les personnes appartenant à des groupes minorisés. Elles s'inscrivent dans des rapports de domination genrés qui traversent l'ensemble de la société et peuvent, à ce titre, toucher des personnes aux positions sociales diverses. Pour autant, leur exposition, leurs formes et leurs conséquences ne sont pas distribuées de manière égale : elles se trouvent souvent aggravées lorsqu'elles s'articulent à d'autres rapports de pouvoir, liés notamment à la racisation, à la classe sociale, au handicap, à l'orientation sexuelle ou à l'identité de genre. Ces violences doivent donc être comprises à la fois comme systémiques, parce qu'elles procèdent d'un ordre social genré, et comme profondément discriminantes, parce qu'elles affectent de manière disproportionnée certaines catégories de population.

4 - Liens des victimes avec leurs agresseurs

Diversité des liens entre victimes et agresseurs. Les résultats de la Grande Enquête montrent que :

55 %

des victimes de cyberviolences sexistes et sexuelles n'avaient aucun lien préalable avec leur agresseur dans le monde physique : celui-ci avait été

- rencontré uniquement en ligne, dans 25 % des cas, ou
- leur était totalement inconnu, dans 33 % des cas.

45 %

des victimes connaissaient l'agresseur hors ligne et la nature de la relation relevait le plus souvent du lien amoureux ou de couple, dans les autres cas il s'agissait plutôt de proches et de fréquentations quotidiennes. Ainsi,

- 52 % des victimes qui connaissaient l'agresseur déclarent avoir subi les violences dans le cadre d'une relation amoureuse ou de couple.
- 36 % par un·e camarade de classe,
- 20 % par un·e ami·e,
- 19 % par un·e connaissance,
- 5 % par un·e collègue de travail,
- 3 % par un·e membre de la famille.

Diffusion non consentie de contenus sexuels. Les chiffres diffèrent cependant en matière de diffusion non consentie de contenus intimes. Dans ce cas, les victimes ont davantage tendance à connaître personnellement leur agresseur :

67 % **des victimes déclarent connaître leur agresseur dans le monde physique et**

76 % **d'entre elles indiquent avoir entretenu une relation amoureuse ou de couple avec cette personne.**

Toutefois, la nature du lien entre victime et agresseur n'est pas uniforme :

27 %
des victimes déclarent avoir été agressées par un·e camarade de classe ;

16 %
par un·e ami·e

13 %
par un·e connaissance

Ces données mettent également en évidence la diversité des profils socioprofessionnels des victimes, certaines étant encore scolarisées ou étudiantes au moment des faits, tandis que d'autres exerçaient déjà une activité professionnelle.

B - Diversité des expériences de victimes de diffusion non consentie de contenus sexuels ou intimes

1 - Modalités de captation et de diffusion

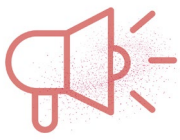
Production initiale des contenus. Pour de nombreuses victimes, les contenus à caractère sexuel ont été auto-produits, c'est-à-dire été réalisés par la victime elle-même, sans que l'on sache pour autant si cette réalisation était contrainte ou consentie. Ainsi :

53 %
des victimes de diffusion non consentie rapportent avoir réalisé ces contenus pour une personne connue de la victime dans le monde physique

31 %
pour une personne rencontrée en ligne.

Captation des contenus et continuum de violences. Pour autant, les résultats de l'enquête montrent que la diffusion non consentie de contenus intimes s'inscrit fréquemment dans un continuum de violences. Nombre de victimes rapportent un contexte dans lequel au moins l'un des contenus concernés a été capturé, obtenu ou créé dans des conditions non respectueuses de leur consentement. Ces situations recouvrent des réalités diverses :

17 %
des contenus ont été pris à l'insu de la personne concernée ou sous contrainte



11 %
proviennent d'enregistrements de diffusions privées

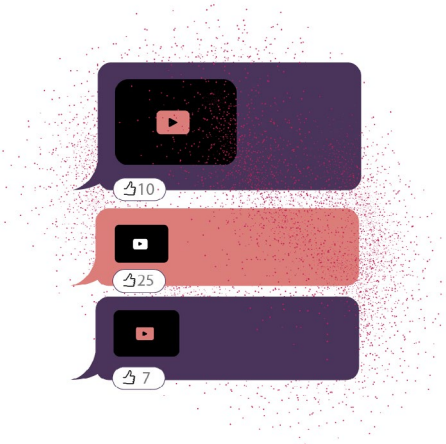
8 %
ont été réalisés lors de violences sexuelles

7 %
sont issus de la réalisation de *deepfakes*

5 %
proviennent du vol de contenus sur des plateformes

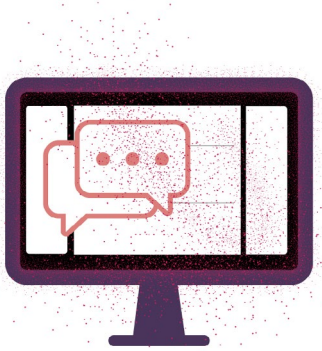
Diversité des espaces de captation. Les contenus pris à l'insu peuvent être réalisés dans des espaces privés physiques – vestiaires, piscines, toilettes – ou numériques, via des captures et enregistrements d'écran réalisés lors de conversations ou diffusions privées, ou via un piratage de webcam. Ils peuvent également être captés dans des espaces publics, notamment par des photographies sous les jupes. Certains agresseurs recourent à des caméras connectées dissimulées dans des toilettes ou des chambres de locations touristiques afin de voler des images. Le chantage dans le but d'extorquer des contenus intimes est également fréquent, tout comme le chantage à la diffusion, l'agresseur essayant alors, le plus souvent, d'obtenir d'autres contenus intimes, des actes sexuels ou de l'argent.

Modalités de diffusion. En outre, les diffusions elles-mêmes peuvent survenir de diverses manières :



66 %
des répondant·es rendent compte de diffusion par message privé

30 %
sur un réseau social



27 %
sur un groupe ou site dédié au partage de ce type

8 %
sur un site à caractère pornographique

Dans tous les cas, ces diffusions peuvent rapidement devenir publiques et virales puisqu'une capture d'écran faite dans un fil de conversation privée peut aisément être partagée à de nouveaux destinataires ou rendue publique.

2 - Contextes relationnels et situations d'emprise

Situations d'emprise et violences conjugales. Ces diffusions non consenties sont souvent le fait de partenaires, de petits amis ou de personnes pour lesquelles la victime nourrissait un intérêt amoureux. Les situations d'emprise sont fréquentes dans ce contexte : elles sont décrites par plusieurs des répondantes à la Grande Enquête, pour certaines mineures au moment des faits, et se retrouvent aussi bien lorsque l'auteur des violences est majeur que lorsqu'il est lui-même mineur. Selon les récits des victimes enquêtées, ces situations d'emprise conduisent à des violences répétées qui s'inscrivent dans la durée et sont à l'origine de troubles psychiques, somatiques et sexuels ayant lourdement impacté leur vie. Par ailleurs, l'étude réalisée en 2018 par le Centre Hubertine Auclert auprès de victimes de violences au sein du couple révélait qu'une femme victime de violences conjugales sur trois déclarait avoir été menacée par son partenaire ou ex-partenaire de diffusion de contenus intimes et que 16 % d'entre elles avaient été victimes de diffusion effective[11].

La diffusion non consentie de contenus intimes peut donc être associée à d'autres types de violences sexuelles, physiques, psychologiques ou économiques.

Motivations des agresseurs et objectification des victimes. Des travaux de recherche réalisés en 2018[12] montrent par ailleurs que les hommes qui diffusent des contenus intimes disent l'avoir fait :

- **dans 22 %** des cas parce que la victime est une ex-partenaire ;
- **dans 22 %** des cas parce qu'ils la trouvent sexy ;
- **dans 15 %** des cas parce qu'ils la considèrent comme peu respectable et
- **dans 6 %** des cas parce qu'elle a été infidèle.

À travers ces chiffres se dessine une vision où la femme est reléguée au rang d'objet, un objet sexuel que les agresseurs souhaitent contrôler et posséder. Les femmes victimes souffrent d'ailleurs particulièrement de cette objectification et de la dépossession liée à la perte de contrôle de leur image[13].

[11] Centre Hubertine Auclert. (2018). *Cyberviolences conjugales : recherche-action menée auprès de femmes victimes de violences conjugales et des professionnel·les les accompagnant*. Centre Hubertine Auclert.
[12] Uhl, C. A., Rhyner, K. J., Terrance, C. A., & Lugo, N. R. (2018). An examination of nonconsensual pornography websites. *Feminism & Psychology*, 28(1), 50-68. https://doi.org/10.1177/0959353517720225
[13] Mincke, M. (2021). *Le phénomène du Revenge Porn : entre reconnaissance et stigmatisation, le point de vue des victimes* [Mémoire de master, Université catholique de Louvain]

C - Diversité des parcours des victimes

1 - Nature des conséquences pour les victimes de CVSS

> Pour l'ensemble des victimes de cyberviolences sexistes et sexuelles

78 %

Une large majorité (78 %) des répondant·es victimes témoignent de conséquences suite aux cyberviolences sexistes et sexuelles subies. Ces dernières affectent de multiples façons les personnes qui en sont victimes et les conséquences rapportées par les répondant·es impactent divers aspects de leur vie et de leur santé. Pour tout type de violences confondues, ce sont :

58 %
des répondant·es qui rapportent des conséquences psychologiques

40 %
des conséquences sur leur vie sociale

38 %
des conséquences sur leur vie sexuelle

30 %
des conséquences sur leur santé physique

22 %
déplorent des conséquences sur leurs études ou leur travail

> Pour les victimes de diffusions non consenties de contenus sexuels

Les victimes de diffusion non consentie de contenus sexuels sont plus nombreuses à déplorer des conséquences sur leur vie et leur santé que celles qui ont uniquement subi d'autres cyberviolences sexistes et sexuelles.

63 %

En particulier pour les conséquences sur la vie sexuelle, puisqu'elles sont 63 % à déclarer un impact contre 28 % pour les autres répondant·es.

La diffusion non consentie de contenus sexuels semble également avoir de lourdes conséquences sur la santé psychique des victimes : ainsi, 75 % des répondant·es à en avoir été victime témoignent de ce type d'impact, tandis qu'environ **la moitié déplore des conséquences sur leur santé physique (45 %) et leur vie sociale (51 %), et plus d'un tiers (37 %) sur leurs études ou leur travail.** Par ailleurs, des entretiens complémentaires conduits auprès de répondant·es montrent à quel point ces violences peuvent impacter profondément et durablement la vie et la santé mentale des victimes, tout particulièrement lorsqu'iels étaient mineur·es au moment des violences.

> Des conséquences graves qui mettent en péril la vie des victimes

Risque suicidaire. Les souffrances engendrées par ces violences sont telles qu'elles peuvent conduire les victimes à des gestes extrêmes. Lorsque les violences se sont produites uniquement dans la sphère numérique, 7 % des répondant·es victimes de cyberviolences sexistes et sexuelles rapportent avoir tenté de se suicider et 10 % y avoir songé.

Dans les cas où les violences ne se sont pas limitées aux espaces numériques et se sont donc également manifestées hors ligne, les chiffres sont particulièrement alarmants : **ce sont 24 % des répondant·es victimes de (cyber)VSS qui ont tenté de mettre fin à leurs jours et 30 % qui rapportent des idées suicidaires.**

Superposition des violences. Les mises en danger sont réelles et les violences rapportées ne se restreignent pas aux espaces numériques, elles peuvent s'accompagner de violences exercées dans le monde physique. **Ainsi, plus d'une victime sur quatre déclare que les violences numériques ont été accompagnées de violences psychologiques, tandis que près d'une victime sur dix rapporte que des violences sexuelles se sont superposées aux cyberviolences subies. On retrouve la même proportion pour les violences physiques.** Ces résultats invitent à inscrire les cyberviolences sexistes et sexuelles dans un continuum plus large de violences, le numérique ne constituant pas un phénomène isolé mais une modalité supplémentaire – et parfois aggravante – par laquelle des violences préexistantes ou concomitantes peuvent s'exercer à l'encontre des victimes.

2 - Durée des conséquences pour les victimes de CVSS

Les cyberviolences sexistes et sexuelles peuvent s'inscrire dans le temps long, non seulement sous la forme d'épisodes répétés, mais aussi par rémanence et réactivation : un contenu peut faire l'objet d'enregistrements ou de captures d'écran, être dupliqué, rediffusé, et ressurgir par vagues bien après l'événement initial.

Répétition des violences. Les données recueillies montrent ainsi qu'une exposition unique aux cyberviolences sexistes et sexuelles constitue l'exception plutôt que la norme, et qu'il existe une forte probabilité pour les victimes d'y être confrontées de manière répétée ou prolongée. En effet, **seules 36 % des victimes répondantes déclarent que les violences ne sont survenues qu'une seule fois,** tandis qu'elles sont 16 % à rapporter des cyberviolences qui durent entre un et six mois, et 14 % des cyberviolences persistant plus d'un an… Enfin, **une victime sur dix déclare que les violences « durent encore aujourd'hui ».**

Persistance des violences. Les entretiens individuels conduits en marge de la Grande Enquête montrent que les cyberviolences peuvent se poursuivre des années durant, notamment lorsqu'elles s'exercent dans le cadre d'une relation intime. Le numérique devient alors un outil de contrôle et d'emprise et peut s'articuler à d'autres violences psychologiques, physiques et sexuelles. Ces durées déclarées recouvrent ainsi des configurations diverses, mais qui contribuent toutes à installer la violence dans le temps.

Phénomène de culpabilisation. Nombreux sont les témoignages de victimes faisant état d'un accueil inadapté de la part des forces de l'ordre mobilisées lors du dépôt de plainte, ces dernières pouvant même aller jusqu'à tenir des propos culpabilisants ou discriminants à leur encontre, créant ainsi une nouvelle expérience traumatique[14]. Les données de la Grande enquête indiquent également que **près de 40 % des répondant·es se sont senties mises en cause, blâmées ou responsabilisées par les personnes auprès de qui elles ont cherché du soutien, un chiffre qui culmine à 66 % lorsque l'interlocuteur représente les forces de l'ordre.** Les raisons de cette culpabilisation sont quant à elles diverses : exposition en ligne, interactions et échanges avec l'agresseur, confiance accordée à celui-ci.

Phénomène de revictimisation. À l'instar des violences sexuelles commises dans le monde physique, le phénomène de revictimisation est fréquent chez les victimes de cyberviolences sexistes et sexuelles. Ce phénomène peut être alimenté par les réactions de l'entourage, les réponses institutionnelles inadaptées ou le manque de prise en considération de la parole des victimes. La revictimisation constitue d'ailleurs un objet d'analyse récurrent dans les enquêtes consacrées aux violences sexuelles commises hors ligne.

a) Revictimisation institutionnelle. Une dynamique se manifeste particulièrement lors du dépôt de plainte : 74 % des victimes de diffusion non consentie d'images intimes déclarent avoir été culpabilisées à ce moment, contre 57 % pour les victimes d'autres formes de cyberviolences sexistes et sexuelles. Cet écart illustre la persistance de représentations sociales spécifiques autour du partage de contenus intimes, encore perçu comme une prise de risque volontaire, donnant lieu à des jugements moraux qui déplacent la responsabilité de l'agresseur vers la victime.

b) Découragement au dépôt de plainte. Pire, certaines victimes déclarent avoir été découragées de porter plainte par les forces de l'ordre elles-mêmes. C'est le cas de Léa, l'une des répondantes à la Grande enquête. Victime de raids masculinistes qui se sont matérialisés par plusieurs vagues de cyberharcèlement à caractère sexiste et sexuel, Léa a tenté de déposer plainte en ligne via la plateforme gouvernementale THESEE. Cette plateforme l'a mise en relation avec un policier afin qu'elle puisse exposer sa situation et sa volonté de déposer plainte. Cependant, ces démarches n'ont pas abouti : le policier lui a vivement déconseillé de déposer plainte, affirmant que de telles démarches seraient inutiles compte tenu de la nature des violences subies. Léa a tout de même souhaité maintenir son dépôt de plainte mais n'a jamais obtenu de retour, malgré de nombreux appels de sa part et un déplacement physique au commissariat.

c) Revictimisation par l'entourage. La prolongation des situations de victimisation ne se limite pas aux institutions : lorsqu'elles se confient à une tierce personne, 56 % des victimes de diffusion non consentie de contenus sexuels rapportent avoir été culpabilisées, contre 32 % pour les autres cyberviolences. Cette stigmatisation constitue un frein supplémentaire à la libération de la parole et limite *de facto* les chances de soutien.

[14] Roney, E. (2025, 31 janvier). « Quand je vois la police, je tremble » : le double traumatisme de femmes victimes de violences qui portent plainte. INDEX.

Intersectionnalité et exposition à la revictimisation.

La revictimisation ne se limite pas à la culpabilisation ; elle prend également une dimension intersectionnelle qui affecte la manière dont les victimes sont accueillies, entendues ou crues lors d'une démarche de plainte ou de recherche de soutien. Nos résultats mettent en évidence une corrélation entre l'exposition aux discriminations et la probabilité de renoncer à porter plainte. Lorsqu'aucune discrimination n'est déclarée, les victimes engagent plus facilement une procédure ; à l'inverse, plus elles déclarent de discriminations, moins elles déposent plainte, favorisant ainsi la poursuite des violences et consolidant les mécanismes de revictimisation. Cette dimension intersectionnelle est corroborée par des travaux institutionnels soulignant que refus de plainte, moqueries, propos discriminants ou découragement explicite constituent des obstacles fréquents à l'accès à la justice pour les victimes de violences sexistes[15].

Impact prolongé. Ainsi, la revictimisation – qu'elle prenne la forme de culpabilisation, de mise en doute ou de discrimination – ne constitue pas un phénomène secondaire. Elle prolonge la violence initiale, accroît l'isolement, entrave l'accès à la réparation et fragilise la confiance dans les institutions. Elle peut également se prolonger dans le parcours judiciaire lui-même, lorsque les décisions, les requalifications ou l'absence de suite apparaissent comme une nouvelle forme d'effacement de la parole et du préjudice. Elle souligne la nécessité de considérer l'expérience complète des victimes de cyberviolences sexistes et sexuelles, et non le seul moment de l'agression, afin de concevoir des dispositifs capables d'accueillir, de protéger et de reconnaître pleinement leur vécu.

Ces données confirment que les cyberviolences sexistes et sexuelles ont des effets importants et pluridimensionnels – pouvant aller jusqu'à la mise en danger de la vie – et qu'elles s'inscrivent fréquemment dans un continuum entre numérique et hors ligne. La diffusion non consentie de contenus sexuels se distingue par des conséquences accrues, appelant une prise en charge adaptée. Afin d'améliorer l'accompagnement des victimes et de faire reculer leur isolement, il est essentiel que toutes ces conséquences soient mieux détectées. Les professionnel·les de la santé et du social devraient, à titre d'exemple, poser systématiquement la question des cyberviolences et ne pas minimiser l'impact de celles-ci pour les victimes lors de leur prise en charge.

[15] Haut Conseil à l'Égalité entre les femmes et les hommes. (2025). *Violences faites aux femmes : mettre fin au déni et à l'impunité*. HCE.

3. Lieux de survenance et recours disponibles face aux cyberviolences sexistes et sexuelles

A - Les espaces où se produisent les cyberviolences sexistes et sexuelles

L'analyse des espaces numériques dans lesquels se produisent les cyberviolences sexistes et sexuelles constitue un point d'entrée essentiel pour comprendre les difficultés rencontrées par les victimes dans leurs démarches pour obtenir protection et assistance, ou envisager des possibilités de recours. Les plateformes ne sont pas de simples supports techniques : elles organisent les interactions, structurent les rapports sociaux et conditionnent les possibilités de signalement, de retrait des contenus et d'accès à la preuve. Examiner les lieux de survenance des violences permet ainsi d'éclairer des logiques structurelles et inhérentes à l'architecture de ces espaces.

1 - Le rôle central des plateformes de réseau social

Prévalence des réseaux sociaux. Les réseaux sociaux apparaissent comme les principaux espaces où se produisent les cyberviolences sexistes et sexuelles. Le fait que 72 % des victimes ayant rencontré leur agresseur en ligne déclarent le connaître par le biais des réseaux sociaux souligne que ces violences s'inscrivent au cœur des usages numériques ordinaires. Elles émergent dans des lieux et au sein de systèmes conçus pour favoriser l'interaction, la visibilité et la mise en relation et où l'exposition personnelle constitue une modalité habituelle de participation.

Plateformes concernées. Les plateformes mentionnées par les répondant·es comme lieux de rencontre des agresseurs permettent de déployer plusieurs grilles de lecture. Les données ici récoltées sont ainsi susceptibles de renseigner aussi bien au sujet des usages de la population qu'au sujet des pratiques et stratégies mises en place par les agresseurs.

31 %
Instagram
occupe le premier rang, concentrant 31 % des rencontres entre victimes et agresseurs suivi par ;

15 %
Snapchat

12 %
X
(anciennement Twitter)

11 %
Facebook

10 %
Discord

4 %
TikTok

3 %
YouTube

6 %
des victimes mentionnent d'autres réseaux sociaux.

Usages en mutation. Ces données reflètent à la fois le poids persistant de certaines plateformes historiques et l'évolution des usages, marquée par l'émergence d'espaces plus récents, structurés autour de communautés, de messageries privées ou de logiques algorithmiques spécifiques. Parallèlement, la mention récurrente de plateformes comme Discord témoigne d'une transformation des environnements dans lesquels s'exercent les cyberviolences sexistes et sexuelles. Ces espaces, initialement conçus pour des usages communautaires ou ludiques, reposent sur des logiques de groupes fermés, de faible modération *ex ante* et de circulation rapide des contenus, qui peuvent favoriser des formes de violences plus diffuses, durables et difficiles à documenter.

Technologie et politique. Le fait que plusieurs des plateformes les plus fréquemment citées relèvent de grands groupes technologiques internationaux, aujourd'hui au cœur de débats sur la modération, la régulation et la responsabilité des acteurs du numérique, invite à interroger le rôle des choix industriels et politiques dans la structuration des espaces de violence en ligne. Il nous faut ainsi dépasser les analyses strictement quantitatives ou comparatives des plateformes et orienter le débat vers le rôle structurant des choix de conception – organisation des interactions, circulation des contenus, porosité entre espaces publics et privés – dans la production de situations d'exposition aux cyberviolences sexistes et sexuelles.

2 - Diversité et perméabilité des espaces numériques

Autres services numériques concernés. Par-delà des réseaux sociaux, les cyberviolences sexistes et sexuelles émergent aussi au sein d'autres environnements numériques :

11 % des victimes les situent sur des forums ou blogs

11 % sur des sites ou applications de rencontre

7 % dans les jeux vidéo

3 % sur des sites dédiés aux mineurs

2 % sur des plateformes de webcam

5 % via d'autres supports

Leur point commun réside dans la création de liens fondés sur la confiance, le jeu, l'intimité ou la sociabilité, autant de contextes susceptibles d'être détournés à des fins de domination ou de contrôle. Ces résultats rappellent que les violences traversent des environnements numériques hétérogènes, aux normes et aux publics distincts.

Perméabilité. La circulation des informations, et par extension la diffusion des actes de violences d'une plateforme à une autre rendent la qualification de la situation, son signalement et la récolte des preuves à son sujet particulièrement complexes pour les victimes. **Cette porosité entre les espaces numériques souligne les limites d'approches fragmentées, centrées sur un type de service ou un espace numérique spécifique et invite à considérer la lutte contre les cyberviolences sexistes et sexuelles non comme un enjeu sectoriel, mais comme une problématique structurelle de conception, de modération, de gouvernance et de responsabilité des plateformes.**

B - Les dispositifs de lutte et de prévention

1 - Le signalement des cyberviolences

Intérêt et lacunes. **Le signalement constitue l'un des premiers leviers à la disposition des victimes pour accéder à une protection et un accompagnement.** Il est toutefois regrettable de constater que les dispositifs nationaux existants présentent d'**importantes lacunes**, en particulier sur le volet sexiste et sexuel des cyberviolences. Les parcours des victimes en sont directement impactés et cela peut **résulter en une prise en charge imparfaite et séquencée, décourageant la victime et l'exposant à de la revictimisation.**

> Le signalement aux pouvoirs publics

Plateforme gouvernementale. Pharos est le portail gouvernemental de signalement des contenus illicites circulant sur internet. Les équipes mobilisées assurent des missions d'harmonisation, d'analyse, de recoupement et d'orientation des signalements à l'échelle du Ministère de l'Intérieur. Rattaché à l'Office anti-cybercriminalité, Pharos permet à toute personne de signaler un contenu lui paraissant manifestement illégal dans des domaines aussi variés que la pédocriminalité, la haine en ligne ou la mise en danger des personnes.

Limites. Il n'est toutefois pas possible de signaler toutes les formes de cyberviolences sexistes et sexuelles par le biais du formulaire mis à la disposition du public par le Ministère de l'Intérieur. À titre d'exemple exemple, une victime de diffusion non consentie de contenus sexuels ne peut pas recourir à cette plateforme pour signaler sa situation et sera donc laissée sans interlocuteur immédiat. Le périmètre d'action de Pharos étant circonscrit aux contenus manifestement illicites et le caractère illicite de ce type de contenu ne pouvant être établi par simple consultation du contenu – contrairement à une image pédocriminelle – le retrait des contenus litigieux ne pourra avoir lieu en sollicitant cette procédure.

> Le signalement aux organisations de la société civile

Rôle de la société civile. En l'absence de dispositif officiel en la matière, le relais est généralement assuré par des structures associatives spécialisées. Toutefois, la visibilité accordée à ces organisations est encore trop dépendante des logiques algorithmiques ou du degré d'implication des pouvoirs publics pour les faire connaître. Une réalité confirmée par les résultats de la Grande Enquête : **seules 4 % des victimes de cyberviolences ont sollicité une association pour évoquer les violences qu'elles ont subies.** Reste que ces organisations offrent une nouvelle modalité de signalement et d'accompagnement aux victimes et aux témoins et incarnent en ce sens un rempart face aux cyberviolences.

Signaleurs de confiance. En tant que structure indépendante et experte dans la détection, l'identification et le signalement des contenus illégaux en ligne, les signaleurs de confiance sont des organismes spécialistes des violences numériques. Désignés en France par l'Arcom, ces associations constituent un appui décisif pour les victimes dans la mesure où leurs signalements doivent être traités en priorité par les services numériques. Ils sont donc en capacité d'obtenir une réponse plus rapide de la part des réseaux sociaux et ainsi garantir un haut niveau de prise en charge des sollicitations de victimes de cyberviolences.

Point de Contact

association de lutte contre les cyberviolences, désignée signaleur de confiance en mars 2025

Missions :

- neutraliser les contenus illégaux et préjudiciables en ligne ;
- aider les victimes de cyberviolences ;
- formation et sensibilisation du grand public et des professionnels;
- étudier les phénomènes cybercriminels ;
- transformer le numérique par le plaidoyer.

Signaler une cyberviolence ou un contenu choquant - L'association met à la disposition de tout internaute, victime comme témoin, adulte comme enfant, un formulaire de signalement permettant de faire remonter à une équipe de juristes une situation ou un contenu en ligne afin de faire retirer la source du préjudice. Les domaines d'action de Point de Contact s'étendent de la protection de l'enfance, de la dignité et de l'identité à la lutte contre les discours illicites (haine en ligne, terrorisme) et les violences sexuelles.

Associations spécialisées. Les structures spécialisées dans les cyberviolences sexistes et sexuelles occupent une place singulière dans l'écosystème de lutte contre les cyberviolences. Leur valeur ajoutée tient à leur capacité à proposer un espace de signalement et d'accompagnement sans jugement, fondé sur une compréhension fine des mécanismes de domination, de honte et de culpabilisation qui traversent les parcours de victimes. Contrairement aux dispositifs généralistes, ces associations sont en mesure de saisir les subtilités propres aux violences sexistes et sexuelles en ligne – consentement ambigu, emprise, chantage, exposition différenciée selon le genre ou l'orientation sexuelle – et d'y apporter des réponses adaptées.

#StopFisha

association française de lutte contre le cybersexisme et les cyberviolences sexistes et sexuelles

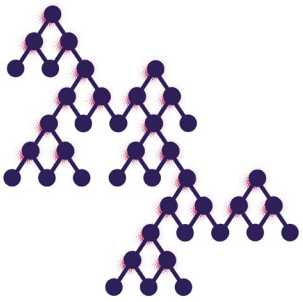
Missions :

- accompagnement juridique et psychologique des victimes ;
- aide aux témoins ;
- signalement des contenus illicites ;
- sensibilisation du grand public ;
- organisation de campagnes de plaidoyer.

#StopFisha propose un formulaire de signalement des cyberviolences accessible via son site internet ou sur Instagram. Le panel de cyberviolences pouvant être signalé à l'association est large et dépasse le cadre strictement légal. En effet, certaines cyberviolences sexistes et sexuelles ne sont pas encore prévues par la loi pénale française. Il est par exemple possible de signaler : un chantage à la cam, un compte fisha, un contenu mettant en scène une agression physique et/ou sexuelle, la divulgation de son identité de genre et/ou d'orientation sexuelle par cyber-outing, une situation de cyberharcèlement, la diffusion non consentie de contenus intimes, l'envoi d'une photo de pénis non sollicitée, une situation de harcèlement par diffusion non consentie d'une photo de soi en hijab, des injures sexistes ou LGBTQ+phobes, des menaces, un deepfake à caractère sexuel, une situation de sextorsion, une situation d'upskirting. Ce formulaire permet aussi de signaler une tendance *(trend*)* observée paraissant dangereuse, haineuse ou encore discriminante.

> Les limites du signalement

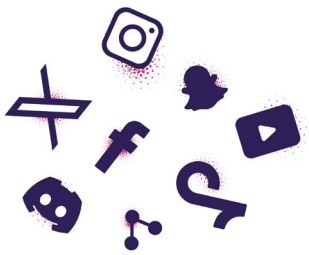
Réponses parcellaires. Si le signalement constitue aujourd'hui l'un des principaux leviers de réponse aux cyberviolences sexistes et sexuelles, il ne saurait, à lui seul, être considéré comme un remède suffisant. Les pratiques de signalement se heurtent à des limites structurelles, juridiques, techniques et humaines, qui en restreignent l'efficacité tant du point de vue de la régulation des contenus que de la protection effective des personnes victimes.



Duplication et rediffusion des contenus. Sur le plan technique, plusieurs obstacles sont régulièrement identifiés. La viralité des contenus, leur duplication rapide, leur hébergement sur des services multiples ou leur diffusion dans des espaces semi-fermés (messageries privées, groupes de discussions, serveurs de jeux) compliquent leur retrait effectif. Plus le retrait sera tardif, plus il amplifiera le risque que chaque suppression ne soit suivie de nouvelles mises en ligne. Même lorsqu'un contenu est supprimé sur une plateforme, il peut subsister ailleurs sous des formes identiques ou légèrement modifiées, pouvant échapper aux mécanismes de détection automatisée – qui sont localement mis en place et n'ont pas vocation à s'appliquer en dehors du service concerné. Le signalement agit alors de manière ponctuelle, sans garantir une interruption durable de la diffusion.

Nature des violences. Par ailleurs, certaines formes de cyberviolences sexistes et sexuelles reposent moins sur des contenus isolés que sur des comportements répétés (harcèlement coordonné, raids, campagnes de dénigrement), qui sont difficilement appréhendables par des outils de signalement avant tout conçus pour des publications isolées. Le traitement fragmenté des signalements peut ainsi conduire à une appréhension à la baisse de situations pourtant extrêmement dommageables.

Risques d'exposition supplémentaire. En outre, le signalement n'est pas un acte neutre socialement. Les victimes peuvent craindre des représailles en ligne, une intensification des attaques, ou une exposition accrue de leur situation. Ces risques sont d'autant plus marqués dans les contextes où les agresseurs agissent de manière collective ou organisée. Ces difficultés sont particulièrement saillantes dans les cas de diffusion non consentie de contenus sexuels, où le parcours de signalement peut paraître sans fin.



Dépendance à la volonté de coopération. Le retrait de contenus préjudiciables repose essentiellement sur la coopération des hébergeurs* de contenus et des plateformes numériques. Or, la qualité de cette coopération demeure encore aujourd'hui variable et inégalement efficace selon les services numériques et les types de contenus concernés. Si elles sont tenues par la loi, les plateformes disposent de politiques de modération qui leur sont propres, fondées sur leurs conditions d'utilisation et qui ne coïncident pas toujours avec les qualifications juridiques nationales ou européennes.

Rigidité du cadre légal. Le signalement se heurte également à des limites juridiques, liées à l'absence ou à l'insuffisance de dispositifs légaux ; toutes les situations vécues par les victimes ne relèvent pas nécessairement d'une infraction pénale caractérisée, ou du moins facilement qualifiable au moment du signalement. C'est notamment le cas lorsqu'il s'agit d'apprécier l'absence de consentement dans la diffusion de contenus sexuels, le caractère sexiste ou discriminatoire d'un propos, ou l'intention de nuire de l'auteur. Cette appréciation requiert souvent une analyse contextuelle fine, difficilement compatible avec les logiques de traitement automatisé ou semi-automatisé des plateformes. En outre, les dispositifs institutionnels de signalement sont fréquemment limités aux contenus dits manifestement illicites[16].

Revictimisation constante. Devoir documenter les faits, conserver ou transmettre des contenus violents, ou répéter son récit à plusieurs interlocuteurs peut constituer une source de stress et aggraver l'impact psychologique de la violence. La multiplicité des dispositifs de signalement – plateformes, associations, autorités administratives, forces de l'ordre – contribue également à une complexification des parcours. Les victimes peuvent se trouver confrontées à des injonctions contradictoires, à des délais de traitement variables ou à des renvois entre acteurs, renforçant un sentiment de découragement ou d'abandon. Cette complexité est un facteur reconnu de non-recours, en particulier pour les personnes les plus vulnérables. La difficulté à être mise en relation avec des interlocuteurs humains joue aussi et amplifie l'isolement dans lequel se trouvent souvent les victimes.

Charge mentale. Dans cette configuration, charge à la victime de partir à la recherche d'éventuelles rediffusions, les signaler, parfois – souvent – devoir relancer les plateformes pour en obtenir le retrait. Il s'agit d'une charge mentale et d'un investissement temporel considérable, parfois difficilement compatibles avec d'autres obligations (professionnelles, scolaires, familiales, ...) – sans parler de l'impact que ce parcours peut avoir sur le temps de la reconstruction psychique. Sans mécanisme empêchant la remise en ligne, le signalement reste peu efficace pour obtenir la suppression définitive de contenus liés à de la diffusion non consentie de contenus sexuels ou intimes.

Absence de réparation. Il faut enfin souligner une limite à laquelle se heurte l'écrasante majorité des victimes de cyberviolences : le signalement n'entraîne pas la réparation du préjudice causé. Les dispositifs de signalement visent avant tout une action de modération sur un contenu, rarement la reconnaissance d'un tort, l'accompagnement de la victime ou une quelconque réparation. En pratique, la victime obtient parfois la suppression des contenus signalés, mais reste, hélas, souvent seule face à de lourdes conséquences sociales et psychologiques – sans que les plateformes ayant facilité la commission de ces violences ne proposent de dispositifs de prise en charge à la hauteur des dommages subis.

[16] Voir infra, notamment la section "le signalement aux pouvoirs publics"

2 - La prévention des cyberviolences

Dispositifs et limites. La prévention des cyberviolences sexistes et sexuelles repose sur un ensemble de mécanismes destinés à limiter leur occurrence, à en faciliter le signalement et à protéger les victimes. Il s'agit désormais d'examiner les dispositifs nationaux et internationaux mis en place à cette fin, en interrogeant leur accessibilité, leur efficacité et leur articulation. Elle met en évidence les lacunes persistantes dans la prise en charge des victimes et les obstacles qui entravent l'accès au droit.

> La technologie de hachage*

Concept. Le **hachage est un processus qui transforme une donnée en une suite de chiffres et de lettres constituant un code unique** qu'on nomme une « signature numérique ». Le hash, c'est donc **cette signature numérique unique associée à un autre contenu initial – il en facilite ainsi l'identification** sans pour autant que ce contenu d'origine ne soit conservé ou stocké.

Usages. Ce type de technologie est notamment utilisé pour identifier et retirer des contenus pédocriminels*. Il a aussi été mis à profit par l'industrie dans le cadre de la lutte contre la diffusion de contenus à caractère terroriste sur le web. Depuis quelques années, certaines structures mobilisent ce procédé pour lutter contre la diffusion non consentie de contenus sexuels ou intimes.

Disrupt. En novembre 2023, l'association Point de Contact a développé le seul dispositif français permettant aux victimes de diffusion non consentie de solliciter le hachage de leurs contenus sexuels ou intimes afin de se prémunir d'une diffusion ultérieure. Le service s'adresse aux victimes – mineures et majeures – de diffusion non consentie de contenus intimes mais aussi aux victimes de sextorsion en ce qu'il permet de prévenir une future diffusion – donc dès le stade du chantage. Disrupt constitue un service additionnel aux actions menées par Point de Contact en matière de signalement et de retrait de contenus illicites. Les signatures numériques ou hashs générés par Point de Contact font systématiquement l'objet d'un examen humain et alimentent ensuite une base de données stockée sur des serveurs indépendants et localisés en France.

Autres services et limites. Des initiatives similaires ont pu voir le jour telles que *Take It Down*, opérée par le National Center of Missing Exploited Children (NCMEC), une organisation américaine – mais dont l'intervention est réservée aux contenus figurant des mineur·es[17]. Quant au dispositif *StopNCII*, qui propose également le hachage de contenus intimes, il est quant à lui accessible uniquement aux victimes majeures[18] et a été développée conjointement par SWGfL et l'entreprise Meta[19] – laissant planer le doute sur la propriété et les conditions d'exploitation de cette base de données.

> L'information, la sensibilisation et l'accompagnement des victimes

Pallier l'isolement. L'accès à une information claire et accessible sur les cyberviolences sexistes et sexuelles, sur les droits des victimes et sur les structures d'aide disponibles conditionne la capacité des personnes concernées à identifier leur situation, à se protéger et à solliciter un accompagnement adapté. L'association Féministes contre le cyberharcèlement propose sur son site internet des informations et des ressources adaptées permettant d'orienter et d'outiller les personnes concernées.

---

[17] Take It Down, « À qui s'adresse Take It Down ? », consulté le 28 janvier 2026.
[18] StopNcii.org, Frequently Asked Questions, « Who can use this service ? », consulté le 28/01/26.
[19] Ibid., « Is StopNCII.org a government initiative? », consulté le 28 janvier 2026.

Féministes contre le cyberharcèlement

association féministe intersectionnelle crée en 2016 et mobilisée contre les violences faites aux femmes, aux filles et aux personnes LGBTIQ+ via les outils numériques

Missions :

› information et sensibilisation des publics
› formation des professionnel·les
› travaux de recherche
› campagnes de plaidoyer

Pour s'informer sur les recours possibles et les ressources à mobiliser en cas de cyberviolences, l'association propose un guide dédié à l'information et l'orientation des victimes de cyberviolences : « Que faire en cas de cyberharcèlement et de cyberviolences ? ». Ce guide met à la disposition du public des ressources techniques et juridiques ainsi que des contacts utiles afin de bénéficier d'une première écoute et d'un suivi médical. Il rassemble des conseils d'autodéfense numérique et des informations utiles sur les démarches que peuvent effectuer les victimes : conserver des preuves, signaler la situation, obtenir le retrait des contenus malveillants, porter plainte, demander un financement de ses frais de justice.

Autres structures et dispositifs. D'autres structures œuvrent à la sensibilisation du public et à la prévention des cyberviolences sexistes et sexuelles.

› Le Centre Hubertine Auclert, centre francilien pour l'égalité femmes-hommes, qui apporte expertise et ressources notamment en matière de violences faites aux femmes. Le Centre a récemment mené une campagne sur les cyberviolences de genre et a publié une étude sur les cyberviolences de genre chez les 11-18 ans[20].

› Le site #stopcybersexisme, conçu par l'Observatoire régional des violences faites aux femmes du centre, propose de multiples ressources et outils permettant de se prémunir contre ces violences. Entre autres, un kit de prévention pour lutter contre les (cyberviolences) de genre est disponible, ainsi qu'un tutoriel pour signaler le cybersexisme en ligne ou encore un guide pour protéger ses outils numériques est mis à disposition du public.

[20] Centre Hubertine Auclert. (2025). *(Cyber)violences de genre chez les 11-18 ans : victimisations sexistes, sexuelles et LGBTphobes dans des collèges et lycées franciliens*. Centre Hubertine Auclert.

Constats. L'analyse des données recueillies met en évidence **une connaissance encore lacunaire des cyberviolences sexistes et sexuelles, une diversité des profils et des parcours des victimes soulignant leur caractère systémique ainsi qu'une ineffectivité persistante des dispositifs de modération, tout comme un accès insuffisant des victimes aux ressources d'information et d'accompagnement.** Si certaines formes de violences sont désormais largement identifiées, d'autres demeurent invisibilisées, contribuant à la banalisation des faits et à la méconnaissance des recours disponibles. Les victimes se heurtent à des obstacles multiples – techniques, institutionnels, sociaux – qui entravent leur accès à la justice et renforcent leur isolement.

Nécessité de transformations structurelles. **Ces constats appellent une transformation en profondeur des politiques publiques de prévention et d'accompagnement.** Il ne s'agit pas seulement de renforcer les dispositifs existants, mais de repenser les rôles et responsabilités respectives des plateformes, des pouvoirs publics et des acteurs associatifs dans la lutte contre les cyberviolences sexistes et sexuelles. Cette transformation doit s'accompagner d'un effort soutenu de sensibilisation, d'une amélioration de l'effectivité des mécanismes de régulation et d'une meilleure coordination des structures d'aide.

II. ENJEUX ÉMERGENTS

L'utopie démocratique. Les prémices d'internet portaient en eux de véritables aspirations émancipatrices : celles d'un espace réellement démocratique, d'une agora permettant à toutes et tous de débattre et d'exposer publiquement leurs opinions, affranchis des médias traditionnels et des modalités d'expression qui ont précédé l'avènement du web. Ces promesses représentaient une opportunité sans précédent pour les personnes auparavant exclues du débat public – parce que discriminées et marginalisées – de faire entendre leurs voix. La puissance de ce potentiel émancipateur a pu se mesurer concrètement. Les Printemps arabes, des contestations populaires nées en Tunisie en 2010 et largement relayées sur les réseaux sociaux Facebook et Twitter – à tel point que l'on entendit parler de « révolution 2.0 » –, ont ébranlé des régimes autoritaires. Les mouvements autour des hashtags #MeToo et #BlackLivesMatter ont, sinon renversé, du moins profondément remis en question l'ordre établi et mis en lumière des violences systémiques longtemps invisibilisées.

Cyberviolences et contre-offensive réactionnaire. Cette puissance transformatrice engendre toutefois un coût considérable, particulièrement pour les femmes et les minorités. Ce phénomène correspond à ce que l'on désigne parfois sous le terme de *backlash** ("contrecoup") – la réaction hostile aux avancées sociales des groupes historiquement discriminés – qui se manifeste fréquemment à travers les cyberviolences. Pour les groupes dominants, l'enjeu consiste à réduire au silence les voix dissonantes afin de maintenir une hégémonie culturelle et préserver les privilèges structurels établis. Les cyberviolences fonctionnent ainsi comme instrument de restauration d'un ordre social contesté.

Logiques économiques et structuration de la violence. L'utopie d'un espace numérique démocratique demeure largement inaccomplie. Une part substantielle de l'Internet est désormais gouvernée par des entreprises dont le modèle économique repose sur la captation de l'attention. Les technologies ne sont pas neutres et les plateformes sociales obéissent à des logiques capitalistes : maximiser l'engagement des internautes, capter leur attention pour augmenter l'exposition publicitaire et recueillir des données permettant d'analyser et de prédire les comportements. Cette orientation économique produit une conséquence observable : les algorithmes de recommandation accordent une visibilité préférentielle aux contenus violents, spectaculaires et polarisants. Les cyberviolences, loin de constituer des anomalies, deviennent structurelles. Les fonctionnalités d'engagement – commentaires, partages, mentions – fonctionnent comme autant de dispositifs augmentant l'exposition aux violences. Au sein de l'espace public numérique, la participation implique désormais une exposition au risque, distribuée de manière profondément inégalitaire. Cette dynamique vise à créer un climat dissuasif poussant ces populations à s'autocensurer ou à se retirer de ces espaces. Ce processus contribue à un rétrécissement effectif de leur liberté d'expression en les cantonnant hors des sphères d'influence et de production du savoir.

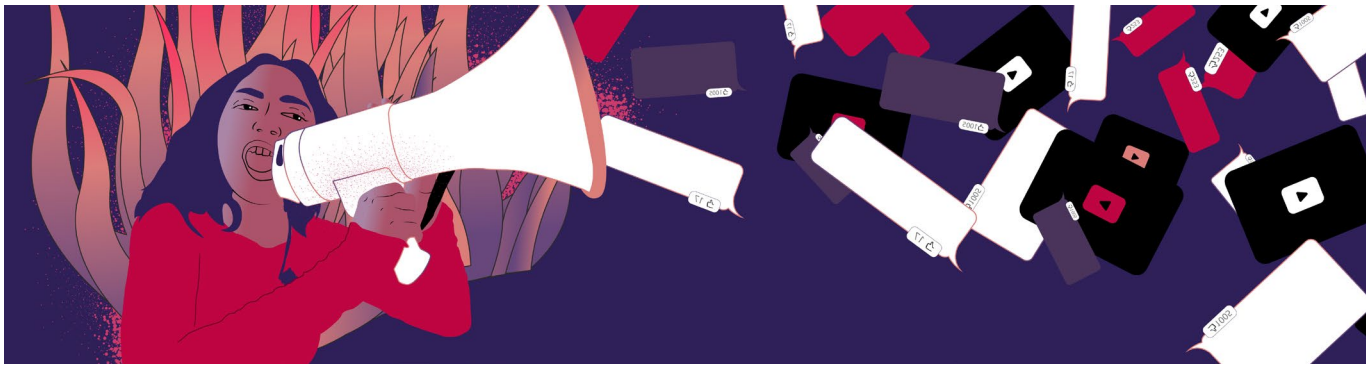
Relâchement des politiques de modération. Les déclarations de Mark Zuckerberg, dirigeant de Meta, en janvier 2025 annonçant un rétropédalage au sujet des règles de modération sur ses plateformes illustrent cette offensive : une section interdisant de qualifier les femmes d'objets ou de propriété a été supprimée, ainsi que des restrictions portant sur l'immigration, l'identité de genre et le genre, au prétexte que ces sujets se trouveraient « au cœur de débats politiques fréquents »[1]. Depuis la réélection de Donald Trump à la présidence des États-Unis, nombreux sont les dirigeants d'entreprises du secteur des nouvelles technologies qui ont cessé d'afficher des ambitions en matière de régulation des contenus violents et invoquent la liberté d'expression pour justifier cette posture. À mesure que la violence s'amplifie sous l'effet de politiques de modération inadaptées et opaques – et parfois inexistantes –, ce sont les voix des femmes et des minorités qui s'éteignent.

[1] Leloup, D. (8 janvier 2025). « Meta assouplit fortement sa modération des contenus haineux sur Facebook ou Instagram ». *Le Monde*. https://www.lemonde.fr/pixels/article/2025/01/08/meta-assouplit-fortement-sa-moderation-des-contenus-haineux-sur-facebook-ou-instagram_6488001_4408996.html

1. Enjeux politiques

A - Les mouvements féministes et progressistes

1 - La réappropriation des espaces numériques par les femmes



Le numérique pour politiser l'intime. La réappropriation des espaces numériques par les femmes pour faire porter leur voix s'est imposée comme l'un des faits politiques majeurs des deux dernières décennies : des femmes, des personnes minorisées de genre et des collectifs féministes s'en sont saisi comme d'un terrain de lutte, où développer des mises en récit et construire un contre-pouvoir[2]. Les blogs, les forums puis les réseaux sociaux ont permis de déplacer des expériences naguère reléguées à l'intime – harcèlement de rue, violences sexuelles, violences au sein du couple, violences médicales, incestes, humiliations ordinaires – vers l'espace public, en les qualifiant comme telles et en leur donnant une visibilité collective. Ce qui était jusque-là vécu comme une somme d'expériences individuelles a pu être décrit comme un système, c'est-à-dire comme un rapport social de domination. La qualification d'un fait social en problème public étant toujours plus tardive lorsque les personnes concernées appartiennent à des groupes minorés. En facilitant l'agrégation des témoignages, leur mise en visibilité à grande échelle et le contournement des hiérarchies médiatiques traditionnelles, les outils numériques ont contribué à accélérer ce processus de politisation.

Faire porter sa voix. Le cas de Paye Ta Shnek est, à cet égard, fondateur. En 2012, à partir d'un blog Tumblr[3], la militante féministe Anaïs Bourdet rend visible l'ampleur des violences et intimidations subies par les femmes dans l'espace public ; en quelques jours, les témoignages affluent par centaines. Cette initiative ouvre la voie à d'autres déclinaisons dans des univers professionnels ou sociaux spécifiques (Paye Ta Robe, Paye Ta Blouse, Paye Ta Truelle, etc.), montrant que les violences misogynes ne relèvent pas d'accidents ou d'expériences isolées mais se retrouvent au sein de toutes les institutions et les corps de métiers. Le numérique permet alors une double réappropriation : réappropriation de la parole – en révélant ce qui était tu – et réappropriation de l'interprétation : en refusant que d'autres – souvent les groupes dominants – ne décident de ce qui serait grave ou acceptable, voire même dicible.

---

[2] Ketsia Mutombo et Laure Salmona, Politiser les cyberviolences. Une lecture intersectionnelle des inégalités de genre sur Internet, Le Cavalier Bleu, 2023.
[3] Tumblr est une plateforme de microblogging qui permet de publier facilement des textes, images, citations, liens ou vidéos, et qui a souvent servi de support à des blogs militants ou culturels grâce à sa simplicité de partage.

L'ère des *hashtags* militants. Les hashtags ont prolongé et amplifié ce mouvement. Leur puissance tient à leur simplicité technique et à leur efficacité politique : ils permettent, sans structure préalable, de fédérer des personnes dispersées et d'agglomérer des contenus, mais aussi de produire de la tendance, donc de l'exposition et de l'engagement. Autrement dit, ils fabriquent un espace commun qui relie des vécus dispersés. Des mobilisations comme #TVAG (autour des touchers vaginaux réalisés sur patientes anesthésiées sans leur consentement), #TwitterAgainstWomen (lancé par les membres de Féministes contre le cyberharcèlement pour dénoncer les cyberviolences sexistes et sexuelles vécues sur Twitter), #StopFisha (qui a donné son nom à l'association éponyme) et nombre d'autres hashtags portés par des collectifs antiracistes et féministes, ont montré comment de tels outils permettent non seulement de dénoncer des violences, mais aussi d'imposer des cadres d'analyse, des définitions, de rallier autour de mots d'ordre, et parfois de déplacer le centre de gravité du débat public. Plus qu'une suite de témoignages, ils incarnent, pour les groupes historiquement discriminés, une manière de reprendre la main en nommant et en décrivant leurs expériences.

La déferlante #MeToo. Dans cette séquence, #MeToo constitue l'exemple le plus spectaculaire de libération de la parole sur les violences sexuelles. À partir d'octobre 2017, dans le sillage des révélations sur le producteur de cinéma Harvey Weinstein et de la reprise d'un outil militant élaboré plus tôt par la militante états-unienne Tarana Burke[4], des millions de femmes racontent les violences sexuelles qu'elles ont subies, souvent pour la première fois, autour du hashtag #MeToo. L'événement est décisif : les femmes victimes se réapproprient une narration qui leur avait été confisquée, elles forcent l'écoute, elles exposent le caractère massif et systémique des violences sexuelles, déplacent l'opprobre du côté des agresseurs, en dénonçant le système qui les protège. C'est cette redistribution du pouvoir symbolique – à savoir qui est légitime pour dénoncer la violence et pour être cru – qui explique aussi l'intensité du *backlash* : accusations de délation, fantasmes d'un soi-disant tribunal populaire, comparaisons outrancières avec la chasse aux sorcières ou le régime de Vichy, cyberharcèlement des femmes qui témoignent. Plus la parole féministe en ligne devient structurante, plus elle est attaquée, précisément parce qu'elle menace les mécanismes d'impunité mis en place par l'ordre patriarcal.

Des espaces numériques de socialisation politique. Cette réappropriation numérique dépasse toutefois la seule question des violences sexuelles au sens strict. Elle a permis à une nouvelle génération – souvent plus jeune, parfois isolée géographiquement ou socialement – d'accéder à des ressources pour comprendre ce qu'elle vit, de découvrir une contre-culture féministe, et de mettre en circulation des expériences longtemps maintenues dans l'invisibilité : violences domestiques, inceste, errance médicale, psychophobie, racisme ordinaire, LGBTIQphobies, etc. Le Web social a servi de porte d'entrée vers les luttes, mais aussi d'espace de socialisation politique, d'autoformation et d'entraide. Des femmes lesbiennes, bi, trans, intersexes, en situation de handicap, musulmanes, juives, afro-descendantes, asiatiques, grosses, atteintes de maladies chroniques ou marginalisées ont pu s'y organiser pour faire entendre des voix que les espaces médiatiques, militants ou institutionnels rendaient souvent secondaires[5]. En ce sens, la réappropriation des espaces numériques n'est pas seulement féministe : elle est aussi profondément intersectionnelle, car elle lutte contre la confiscation de la parole par les groupes les plus privilégiés, y compris à l'intérieur des mouvements progressistes.

---

[4] Murhula, C. (5 octobre 2022). « Tarana Burke, la lanceuse méconnue de #metoo ». Le Monde. https://www.lemonde.fr/m-le-mag/article/2022/10/05/tarana-burke-la-lanceuse-meconnue-de-metoo_6144424_4500055.html

[5] Mutombo, K., & Salmona, L. (2023). Politiser les cyberviolences. Une lecture intersectionnelle des inégalités de genre sur Internet. Le Cavalier Bleu.

L'exemple Take Back The Tech!

Dès le début du siècle, des initiatives comme la campagne transnationale et collaborative Take Back The Tech![6] ont appelé les utilisateur·ices à reprendre le contrôle des technologies de l'information et de la communication afin de lutter contre les violences de genre en exhortant les utilisateur·ices à un usage stratégique des plateformes et supports à leur disposition – téléphones, ordinateurs, messageries instantanées, blogs, sites web, appareils photos, courriels, podcasts, jeux vidéo, etc. – dans le but de promouvoir un idéal féministe et antidiscriminatoire.

Résister au *backlash*. Pour autant, cette dynamique d'émancipation possède un revers, et non des moindres : si l'espace numérique favorise la prise de parole et l'agentivité[7], il est aussi structuré par les mêmes rapports de domination que le monde physique, qui sont souvent amplifiés par la viralité, la brutalisation du débat et le fonctionnement des algorithmes de recommandation. Les cyberviolences s'apparentent dès lors à des outils d'intimidation destinés à rappeler les femmes et les groupes minorés à l'ordre, à les épuiser, à les faire taire et à les chasser des espaces numériques. Elles s'inscrivent dans le continuum des violences hors ligne, dont elles prolongent les effets. C'est pourquoi la réappropriation des espaces numériques est une conquête conflictuelle : chaque avancée en matière de visibilité, de parole ou d'organisation s'accompagne de contre-attaques. Pour vraiment libérer la parole, il apparaît nécessaire de construire collectivement les conditions matérielles et politiques permettant de rendre visible cette parole, de l'amplifier et de la rendre légitime.

Enjeux démocratiques. Des années plus tard, le web est plus que jamais un espace à investir par celles et ceux mis à la marge. Donner à croire en ces outils et en faciliter l'accessibilité – et la sécurité – aux femmes et groupes minorisés constitue aussi bien un projet politique émancipateur qu'un levier stratégique destiné à contre-attaquer une haine omniprésente et banalisée. Face à une mainmise toujours plus importante des discours misogynes sur le débat public en ligne, l'un des contrepieds mobilisé a été de percevoir ces espaces comme des lieux sujets à la réappropriation et à utiliser comme outil porteur des idées féministes.

[6] Le site de la campagne est disponible ici : https://takebackthetech.net/fr.
[7] Le terme agentivité, emprunté à l'anglais *agency* et formé sur la racine latine agere (« agir »), désigne la propriété d'un individu ou d'un groupe d'être la source d'actions ayant des effets sur le monde. (Wikipédia)

L'empouvoirement* des femmes. Par ce biais, trois formes d'empouvoirement des femmes dans et par le numérique émergent[8] :

› **Le pouvoir *avec*** : il s'agit d'une forme d'empouvoirement s'appuyant sur la force du collectif. Cet aspect peut être illustré par l'apparition de réseaux de femmes qui renforcent leur capacité à entrer, agir et s'affirmer dans l'espace numérique.

› **Le pouvoir *pour*** : il se manifeste à travers des initiatives telles que le mouvement FemTech et des applications favorisant la maîtrise par les femmes de leur propre corps.

› **Le pouvoir *intérieur*** : il correspond au dépassement d'une domination intériorisée, notion particulièrement liée aux premiers mouvements cyberféministes.

Limites. Investir les espaces numériques afin de les utiliser comme vecteur d'idées féministes et de lutter contre la haine misogyne en ligne suppose malgré tout une maîtrise de ces technologies couplée à une représentation plus importante des femmes dans ces secteurs professionnels. Pourtant, en 2019, une baisse continue du nombre de professionnelles des TIC était observée[9]. L'accès à ces corps de métiers, rendu plus difficile en raison de biais genrés, de stéréotypes dévalorisants ou de l'effet dissuasif que peut générer le fait que le secteur reste majoritairement masculin – augmentant notamment le risque d'exposition à des violences – peuvent expliquer ce regrettable constat. Un changement de culture apparaît néanmoins indispensable. Il permettrait sans doute la remise en cause de certains processus de décision et de conception des produits et services numériques de sorte à, enfin, favoriser des technologies plus inclusives et égalitaires.

2 - Le développement de pratiques de cyberautodéfense

Définition. L'autodéfense féministe en ligne constitue une volonté globale de résister à la continuité des dominations genrées et des violences numériques. De nombreuses formes de cyberautodéfense sont à l'œuvre, pas toujours avec les mêmes approches mais toujours dans cette même optique d'émancipation.

> La cybersécurité*

Causes. Une attention particulière à la cybersécurité émerge au sein de la société civile afin que chaque personne dispose des moyens de protéger son existence numérique. S'informer et se former, transmettre des conseils en matière de protection des données est indispensable à tout âge et dans toute situation. Et ce d'autant plus que la récolte d'informations opérées par une large partie des grandes plateformes contemporaines est de nature à globalement desservir les internautes.

Captation des données par des multinationales. Le cyberespace étant largement détenu par des entreprises qui réalisent leur profit sur l'exploitation des données issues ou générées par les internautes, une riposte citoyenne s'organise. Souvent enjolivée sous couvert de "mieux cibler" les envies et besoins de chacun·e, cette logique dévoile ici son versant capitaliste, incitant toujours plus à la consommation de produits, de services, de contenus. Mis au service d'idéologies libérales et conservatrices, ce modèle économique favorise la polarisation du débat – alimenté notamment par les très décriées 'bulles algorithmiques'.

---

[8] Morley C. & Kuntz P., « Empowerment des femmes par les technologies numériques : *pouvoir avec, pouvoir pour et pouvoir intérieur* »? *Terminal* [En ligne], 125-126 | 2019, mis en ligne le 01 décembre 2019, consulté le 29 octobre 2025.
[9] *Ibid.*

Utilisation des données afin de nuire à autrui. L'exploitation des informations personnelles peut servir à porter atteinte aux individus et aux collectifs. L'éventail des diffusion des informations, piratage des données, usurpation d'identité, entrave à la vie privée, mise en danger de personnes...

> La réappropriation de termes stéréotypés

Concept. Le fait de détourner des contenus ou termes violents, insultants ou discriminants est une stratégie qui s'ancre dans une véritable bataille culturelle. Il existe de nombreux exemples de réappropriation par des personnes concernées des termes homodiscriminants tels que "pédé", "gouine", transdiscriminants, ou tout simplement insultants tels que "tana*"[10]. Si une partie des personnes concernées souscrivent à cette approche, une autre considère pour sa part qu'il faudrait exclusivement en dénoncer l'usage de sorte à ne pas les banaliser et ainsi laisser l'opportunité à l'oppresseur de l'utiliser comme une arme.

Attaque. L'un des exemples récents de cette réappropriation est le terme Tanaland. Initialement, le mot 'tana' a été popularisé par le rappeur Niska dans l'un de ses morceaux et doit s'entendre comme une variante du terme "pute". Il a largement été repris en ligne, majoritairement par des hommes, pour commenter les faits et gestes de femmes, principalement à des fins de stigmatisation. Ce terme réinvente la haine patriarcale à l'ère des réseaux sociaux et musèle les femmes qui osent se faire une place dans l'espace public numérique.

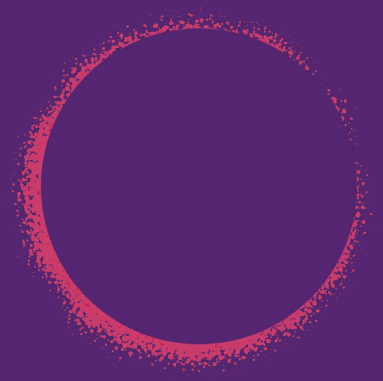
Contre-attaque. La réponse la plus impactante à cette nouvelle tendance a été la réappropriation du terme par les premières concernées - c'est-à-dire des femmes et travailleur·ses du sexe. Elles ont décliné le mot et inventé un véritable monde pour toutes les personnes considérées comme des "tanas" : Tanaland. C'est @Hadja_bh2 qui est à l'origine de l'idée de ce pays imaginaire symbolisant la liberté, l'égalité et l'émancipation de toutes les personnes jugées par une vision patriarcale. Des milliers de personnes se sont mises à revendiquer le fait d'être une tana (sur la base de condition d'avoir déjà été insultée de 'salope', 'pute', etc voire d'en être un·e et fier·e) et à demander à rejoindre cette cité merveilleuse.

[10] Voir *infra*, Partie 2, III, B, 2.

> Exister malgré la censure

Problématique d'invisibilisation. Dans un contexte de modération automatisée – susceptible de supprimer ou d'invisibiliser des contenus relatifs aux violences sexuelles, à la santé sexuelle, aux récits de traumas ou aux témoignages de survivant·es – de nombreuses personnes recourent désormais à un langage codé pour garantir la visibilité de leurs messages. Ces pratiques s'expriment notamment via l'usage d'émojis, d'euphémismes, ou de détournements orthographiques, phonétiques ou sémantiques. Elles ne relèvent pas d'un choix esthétique ou d'une volonté de dissimulation, mais répondent à la nécessité de permettre la circulation d'informations parfois vitales – dénonciations, prévention, appels à l'aide – dans des environnements numériques où certains mots-clés déclenchent suppression, relégation, démonétisation ou invisibilisation.

Violet comme viol



L'un des exemples emblématiques et particulièrement populaire est l'utilisation de la pastille violette ◯ pour remplacer le mot « viol » ou évoquer la violence[11]. Massivement utilisé dans le cadre militant, ce symbole s'est imposé comme signe de reconnaissance et canal alternatif permettant de repérer créateurs, contenus et espaces de discussion autour des violences sexuelles. Dans les moteurs de recherche internes de certaines plateformes, ce symbole offre parfois davantage de résultats que le mot lui-même, ce qui le transforme en un outil de référencement communautaire.

Concept. Souvent désignée comme *algospeak**, cette pratique fonctionne comme un outil de contournement ici compris comme un acte de résistance face à une forme de censure algorithmique – parfois nommée shadowban. Elle rend possible la circulation de contenus cruciaux d'un point de vue individuel et collectif et qui s'étendent des témoignages et récits de violences à l'information et la prévention.

[11] Croquet, P. (23 octobre 2024). « Exprimer le viol avec l'émoji violet, paradoxe et symbole de la libération de la parole sur les réseaux sociaux ». *Le Monde*.

Atteintes systématiques à la liberté d'expression. Ces contournements révèlent les limites de la libération de la parole telle qu'elle est souvent présentée depuis l'émergence des mouvements de dénonciation en ligne. En effet, la nécessité de transformer les mots – pourtant décisifs pour qualifier juridiquement, politiquement ou socialement des violences (viol, inceste, agression, avortement, travail du sexe, VIH, contraception, etc.) – souligne que cette liberté de dire n'est pas acquise. Elle reste conditionnée par des architectures techniques et des impératifs commerciaux qui privilégient la protection de l'image des plateformes au détriment du droit à l'information et du processus de reconnaissance des victimes. Parler en émojis ou en orthographes altérées, c'est renoncer aux termes communément employés et admis : cela peut fragiliser la portée politique des discours et limiter leur accessibilité, en particulier pour les personnes qui cherchent de l'aide sans maîtriser ces codes.

Censure de la parole des victimes. Les victimes ou les personnes non initiées se trouvent ainsi confrontées à un double silence : celui qu'imposent leurs agresseurs, et celui qu'imposent les plateformes. Le simple fait que plane l'incertitude quant à une éventuelle censure du terme « viol » contribue à politiser encore davantage la prise de parole. Le débat public au sujet des (cyber)violences devient ainsi un espace sous contrainte, où la portée d'une parole dépend en partie de sa capacité à contourner des règles fixées par des algorithmes – au risque de ne pas être entendus par ceux qui en auraient besoin.

> Le boycott

Concept. S'agissant des réseaux sociaux, divers mouvements invitent à boycotter les plateformes qui mènent trop explicitement une modération au profit des idées conservatrices et masculinistes.

Exemple. Entre autre, un important mouvement de boycott du réseau social Twitter s'est lancé lors de son rachat par Elon Musk[12] et s'est poursuivi en 2025[13], avec la campagne *HelloQuitX*. Il s'agit, en plus de la dénonciation des idées prônées par leurs dirigeants, de remettre en question le fait que ces plateformes capitalisent sur l'addiction, la frustration et la violence qu'elles sont accusées d'entretenir. Se mêlent ainsi des revendications sociales, féministes, anti-discriminations et écologiques.

Visibiliser d'autres plateformes. Le boycott* peut aussi être accompagné de solutions alternatives en recommandant d'autres plateformes considérées plus éthiques et/ou open-source pour y délocaliser son activité numérique, comme ont pu l'être présentées les plateformes Bluesky ou Mastodon.

Preuve. Le signalement sert aussi de preuve pour les autorités si la victime souhaite engager des poursuites et en cas de refus de prise en compte dudit signalement, cela peut tout de même servir à démontrer aux pouvoirs publics et aux plateformes qu'il est nécessaire d'améliorer les pratiques de modération.

[12] https://www.liberation.fr/idees-et-debats/boycotter-x-un-dilemme-plus-complexe-que-prevu-20241123_L2M6ZAIURZFVJMBFPDIYI376NE/

[13] Dang, L. (17 janvier 2025). « L'idée, c'est de créer une issue de secours pour la démocratie », Socialter.

> Le piratage

Concept. Si le piratage informatique et autres techniques de contrôle en ligne sont des formes de violences numériques et d'atteinte aux systèmes de sécurité, il est parfois mobilisé à des fins progressistes dans la mesure où il permet la révélation de crimes et délits et peut ainsi servir la lutte contre les cyberviolences sexistes et sexuelles.

Exemple. Le mouvement de cyberactivisme Anonymous mène des actions en lançant des cyberattaques permettant de dénoncer des faits pédocriminels, de rechercher et divulguer des preuves dans des affaires de viol, etc.

B - Les mouvances masculinistes et réactionnaires

1 - Genèse et incarnations de la pensée masculiniste

Émergence. Le masculinisme est un mouvement idéologique antiféministe. Si cette doctrine n'est pas nouvelle et a toujours existé en opposition aux nombreuses luttes féministes engagées au cours de l'histoire[14], la forme contemporaine de cette mouvance est née au cours des années 70. D'abord développé hors-ligne ou au sein de forums et sites Internet thématiques, le mouvement a pris de l'ampleur au début des années 2000, parallèlement à l'essor d'internet et plus particulièrement des réseaux sociaux. Les possibilités d'interconnexion mondiale offertes par ces outils ont permis au mouvement de diffuser massivement son champ lexical et ses narratifs, sans contrainte de temps ni de frontière géographique, favorisant une propagation continue de son idéologie.

Origine. Aujourd'hui internationalement répandues, les idées masculinistes contemporaines ont d'abord émergées en Amérique du Nord, particulièrement aux États-Unis, et influencent fortement celles diffusées actuellement en Europe. À titre d'exemple, les Incels et les MGTOW (Men Going Their Own Way), groupes emblématiques du mouvement, se sont constitués aux États-Unis. Définition. La féministe et sociologue québécoise Mélissa Blais a défini le masculinisme comme une forme moderne antiféministe, dont les idées sont fondées sur la théorie d'une crise de la masculinité. En d'autres termes, les hommes souffriraient aussi bien d'une société jugée excessivement féminisée que de la place occupée par les femmes jugée trop importante[15]. Stéphanie Lamy, spécialiste des guerres de l'information, autrice et militante féministe, établit l'objectif du mouvement masculiniste comme étant celui de « maintenir, voire renforcer, la domination masculine par la normalisation des violences masculines à l'égard des femmes et des minorités de genre »[16], notamment en prônant la violence sous toutes ses formes.

---

[14] Définition du masculinisme par Blais, M. (25 novembre 2023), France Info. https://www.franceinfo.fr/societe/violences-faites-aux-femmes/le-masculinisme-gagne-du-terrain-carle-feminisme-est-populaire-et-audible-estime-la-sociologue-melissa-blais_7025672.html#:~:text=Franceinfo%20%3A%20Qu'est%2Dce,y%20prendraient%20trop%20de%20place.

[15] *Ibid.*

[16] Lamy, S. (2024). *La Terreur Masculiniste*. Détour, p. 12.

Ampleur. Si certains peuvent penser que le mouvement masculiniste ne regroupe qu'une poignée d'hommes échangeant uniquement sur internet, la réalité est toute autre. Les communautés masculinistes rassemblent, en ligne comme hors ligne, des centaines de milliers de personnes. Parmi leurs adeptes, certains sont des influenceurs et utilisent leur nombre élevé d'abonnés sur les réseaux sociaux pour propager plus rapidement et massivement leurs idéaux, souvent sous couvert de conseils en musculation, en développement personnel ou encore en crypto-monnaie et investissement financier.

Extrémisme politique. Les mouvements masculinistes évoluent et progressent au sein de divers milieux favorisant la radicalisation – à la fois en ligne et hors ligne[17] – et s'inscrivent dans des dynamiques conservatrices – en opposition aux dynamiques féministes. Baptiste Marchais et Valek qui cumulent plus de 650 000 abonnés à eux deux, ou encore Papacito, dont la chaîne YouTube a été fermée en 2023, sont emblématiques de ces tendances réactionnaires. De manière plus frontale parfois, les influenceurs incarnant ces mouvements sur les réseaux sociaux sont identifiés comme des partisans de formations politiques d'extrême droite. L'usage des plateformes en ligne aux fins de diffuser des idéologies traditionalistes a notamment permis à des groupes politiques tels que le Rassemblement National de toucher plus facilement de jeunes audiences.

Attentats et tuerie de masse. Au-delà de l'extrémisation politique, le mouvement masculiniste présente un risque plutôt élevé de radicalisation pouvant amener certains adeptes, poussés par leur haine envers les femmes, à commettre des attentats et des tueries de masse. À titre d'exemples :

- Elliot Rodger est devenu une icône de la mouvance suite à la tuerie d'Isla Vista en Californie en 2014, qu'il a qualifié de « jour du châtiment » lui permettant de prendre sa « revanche sur l'humanité » et particulièrement sur les femmes[18] ;
- Jake Davison, auteur de la fusillade de Plymouth au Royaume Uni, adhérait quant à lui à la culture incel et à l'idéologie de la pilule noire[19].
- En France, Timothy G., un jeune homme de 18 ans, a été arrêté le 27 juin 2025 près de son lycée de Saint-Etienne en possession de couteaux. Ce dernier avait la volonté de « tuer des femmes » et s'identifiait aussi à la mouvance incel[20].

---

[17] *Ibid.*

[18] Le Monde. (24 mai 2024). « Le fils d'un réalisateur annonce « le jour du châtiment » et tue 6 personnes en Californie ». *Le Monde*. https://www.lemonde.fr/ameriques/article/2014/05/24/au-moins-sept-morts-dans-une-fusillade-en-californie_4425200_3222.html

[19] Mitchell, S. (13 août 2021). « Drame. L'ombre « incel » plane sur la tuerie de Plymouth, la pire depuis onze ans au Royaume-Uni ». *Courrier international*. https://www.courrierinternational.com/article/drame-lombre-incel-plane-sur-la-tuerie-de-plymouth-la-pire-depuis-onze-ans-au-royaume-uni

[20] Ayad, C. (2 juillet 2025). « Projet d'attentat masculiniste déjoué : une première en France, où la menace « incel » est émergente ». Le Monde. https://www.lemonde.fr/societe/article/2025/07/02/projet-d-attentat-masculiniste-dejoue-une-premiere-en-france-ou-la-menace-incel-est-emergente_6617439_3224.html

2 - Développement de la culture masculiniste

Eléments constitutifs d'une sous-culture. Le mouvement masculiniste a développé une véritable culture qui lui est propre, constituée d'éléments interconnectés : un champ lexical spécifique, un idéal physique et psychique de la masculinité authentique, des modes de diffusion particuliers, des thématiques récurrentes articulées à l'idéologie du mouvement, des procédés de rassemblement communautaire (en ligne comme hors-ligne) et des répertoires d'action caractéristiques de la manosphère*. Cette structuration culturelle cohérente permet à la fois l'identification des membres entre eux et la diffusion efficace de l'idéologie auprès de nouvelles recrues[64].

Société de la jeune fille
La société actuelle aurait transformé les hommes en jeunes filles, à savoir des êtres dépourvus de virilité, naïfs, superficiels, narcissiques et écervelés.

Prendre la red pill
Allusion au film Matrix et aux pilules bleues et rouges. Prendre la pilule rouge permet de se réveiller et de prendre conscience que le monde subit une crise de la masculinité

PPP
Abréviation des termes protéger, procréer et pouvoir. rôles fondamentaux de l'homme dans les sociétés traditionnelles qu'il ne peuvent plus tenir du fait des féministes (l'homme ne protège plus) et des homosexuels (l'homme ne procrée plus).

VMS
Abréviation de valeur sur le marché sexuel. La VMS des hommes est calculée en fonction de bonus tels que les SHV (Signes de Hautes Valeur) ou des malus tels que les SFV (Signes de Faible Valeur).
Exemples : la calvitie est perçue comme un SFV, un beau costume est quant à lui un SHV. En outre, la VMS d'une femme décline après le cap des 30 ans et est également fonction de son bodycount[21].

Cuck
Un homme faible qui croit aux théories du patriarcat et qui pense devoir se faire pardonner pour.
Exemple : une personne qui croit aux inégalités salariales est asservie à la société et donc aux femmes.

[21] Manosphère : un ensemble de communautés en ligne se présentant comme un soutien aux hommes confrontés à des difficultés dans leur vie. Mais derrière cette façade se dissimulent bien souvent des discours toxiques, des conseils nuisibles, et une rhétorique fondée sur la défiance envers les femmes. Comme le rappelle le rapport du Secrétaire général des Nations Unies sur les violences faites aux femmes et aux filles, ces groupes partagent une hostilité commune au féminisme et propagent l'idée fausse selon laquelle les hommes seraient les « victimes » du contexte sociétal actuel. ONU FEMMES FRANCE

Nawalt/Awalt
Abréviations des expressions :
› Not all women are like that (Toutes les femmes ne sont pas ainsi)
› All women are like that (Toutes les femmes sont ainsi)

Alpha, Beta, Lambda, Mega
Hiérarchie sexuelle déterminée en fonction de l'apparence et de la richesse mettant en compétition les hommes entre eux.

Social justice warrior
Expression anglaise péjorative désignant une personne qui défend des causes progressistes, notamment le féminisme*.

Soy boy ("homme-soja")
Terme péjoratif utilisé pour qualifier un homme ayant des traits physiques ou psychologiques attribués à la féminité.

Homme alpha et normativité corporelle. L'homme « alpha » constitue, selon l'idéologie masculiniste, le dominant absolu, l'idéal masculin à atteindre. Une série de critères physiques et psychologiques a été codifiée comme nécessaire pour accéder à ce statut. Si certaines caractéristiques varient selon les discours, d'autres sont systématiquement valorisées et dépassent même parfois les cercles masculinistes pour s'ancrer dans la culture dite *mainstream*. La mâchoire carrée est ainsi perçue comme un marqueur biologique de virilité, donnant lieu à de nombreuses publicités et vidéos ciblant principalement de jeunes garçons et promouvant des produits ou exercices permettant de développer cette caractéristique physique. L'homme alpha doit également présenter une musculature très développée, faire preuve d'une assurance inébranlable et bénéficier d'une indépendance financière totale. Cette construction normative de la masculinité idéale produit des effets disciplinaires sur les corps masculins et contribue à naturaliser des rapports de domination fondés sur des critères arbitraires présentés comme biologiquement déterminés.

Dissimulation des discours violents. Les influenceurs masculinistes recourent fréquemment à des stratégies de dissimulation permettant de masquer la radicalité de leurs discours derrière des contenus apparemment anodins ou inoffensifs. Ces contenus servent pourtant activement l'enracinement de leurs idéologies dans l'esprit des jeunes utilisateurs des réseaux sociaux. Les thématiques abordées – musculation, investissement financier, relations sociales entre hommes et femmes – paraissent à première vue neutres. Les influenceurs se présentent ainsi comme coachs sportifs, experts en cryptomonnaies, coachs de séduction ou coachs de développement personnel.

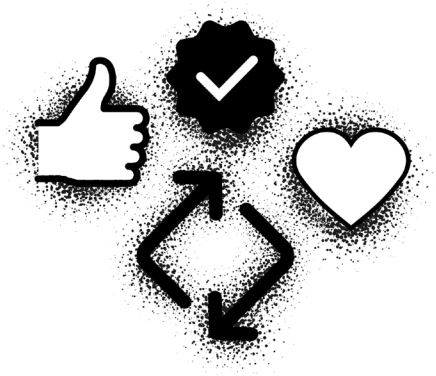
Instrumentalisation de l'humour. De nombreux contenus produits par ces influenceurs masculinistes présentent également un caractère humoristique délibéré, permettant ainsi – sous couvert de second degré – d'invisibiliser la violence structurelle portée par leurs propos. L'usage massif de mèmes et les références constantes à la culture populaire constituent des vecteurs privilégiés de ce procédé. Le discours masculiniste s'arme ainsi d'humour pour tourner en dérision les revendications féministes, discréditer les militant·es progressistes et mépriser les hommes qui refusent de jouer le jeu de la masculinité hégémonique. Ces techniques de dissimulation des discours radicaux et de minimisation des violences faites aux femmes permettent une radicalisation progressive et insidieuse des internautes exposés à ces contenus, d'autant plus efficace qu'elle emprunte des codes culturels contemporains.

Violence collective et organisée. Au-delà de la production de contenus idéologiques, les masculinistes ont développé des pratiques permettant le rassemblement communautaire et l'entraînement mutuel vers un extrémisme toujours plus prononcé, notamment en matière de haine envers les femmes. La création de groupes sur certaines plateformes – WhatsApp, Telegram, Discord – exclusivement réservés aux partisans de l'idéologie constitue l'un de ces dispositifs. Ces espaces fermés fonctionnent comme de véritables foyers de propagation et de radicalisation, échappant largement à la modération et permettant une intensification progressive de la violence discursive. Ils sont également instrumentalisés pour établir des listes comportant les noms de personnes identifiées comme cibles à « abattre » et pour coordonner des raids de cyberharcèlement massif à l'encontre de ces victimes désignées.

Exemples. Typhaine D., comédienne et metteuse en scène engagée pour la cause féministe, a ainsi subi des vagues de cyberharcèlement organisé suite à la diffusion sur les réseaux sociaux d'une vidéo présentant une œuvre artistique dont elle est l'autrice : la Langue de la Féminine universelle – création littéraire et militante visant à démontrer la masculinisation historique de la langue française depuis le XVIe siècle[22]. Les violences subies se sont traduites par des milliers de messages extrêmement violents comportant insultes, menaces de violences physiques, menaces de mort et menaces de viol, contraignant finalement la victime à quitter son lieu de vie et à se réfugier en province pour garantir sa sécurité physique. De même, Léa, répondante de la Grande Enquête sur les Cyberviolences Sexistes et Sexuelles, a vécu une situation similaire après avoir affirmé ses convictions féministes sur Instagram. Elle a subi plusieurs vagues de cyberharcèlement d'une violence extrême après que son nom a été diffusé au sein de groupes masculinistes, illustrant ainsi le caractère systématique et organisé de ces violences coordonnées.

[22] « Violence en ligne, quelle action internationale ? », Délégation aux droits des femmes, intervention de Madame Typhaine D, accessible via : https://videos.assemblee-nationale.fr/video.17380945_68e51e78ef741.delegation-aux-droits-des-femmes---violences-en-ligne-quelle-action-internationale----7-octobre-2025

3 – Epanouissement des mouvances masculinistes sur les plateformes



Implication des plateformes. Les mouvances masculinistes se sont développées avec une rapidité alarmante depuis l'avènement des réseaux sociaux. Cette expansion fulgurante, criante depuis ces dernières années, s'explique non seulement par l'existence d'une interconnexion instantanée et généralisée à l'échelle mondiale – rendant l'échange d'informations immédiat et affranchissant ces discours de toute limite géographique – mais également, et de manière déterminante, par le fonctionnement des plateformes qui favorise la propagation de ces idéologies sur leurs services.

Programmation algorithmique. Chaque réseau social est doté d'un algorithme analysant en continu les données issues de l'activité des utilisateurs – likes, partages, commentaires, durée de visionnage des vidéos, réactions aux stories – afin d'établir la pertinence de chaque contenu et d'identifier ceux susceptibles de générer le plus d'interactions. Des travaux de recherche ont démontré que ces algorithmes sont programmés de manière à proposer préférentiellement des contenus masculinistes, sexistes et misogynes aux comptes identifiés comme appartenant à des adolescents de genre masculin[23]. Ainsi, une dizaine de minutes suffirait pour qu'un contenu masculiniste soit proposé à un compte TikTok nouvellement créé et identifié comme appartenant à un adolescent[24]. Cette orientation algorithmique ne relève pas d'un dysfonctionnement technique mais d'une logique économique privilégiant l'engagement au détriment de la qualité des contenus diffusés.

Monétisation des contenus violents. Les contenus violents bénéficieraient par ailleurs d'une mise en avant algorithmique privilégiée sur les plateformes. Lorsqu'un contenu génère un volume élevé d'engagements – likes, commentaires, partages –, il peut être récompensé financièrement ou par une visibilité accrue. Une étude publiée fin 2025 analyse précisément les mécanismes économiques utilisés par les influenceurs publiant des contenus violents, notamment sexistes et misogynes, pour obtenir une rémunération substantielle[25].

---

[23] Reset Australia & Institute for Strategic Dialogue (ISD), (avril 2022). *Algorithms as a weapon against women. How YouTube lures boys and young men into the « manosphere »*. https://www.isdglobal.org/wp-content/uploads/2022/04/Algorithms-as-a-weapon-against-women-ISD-RESET.pdf

[24] Ferrari, P. (2023). *Formés à la haine des femmes*, Éditions du Seuil. Paris.

[25] Daniele, F., Bucher, L., Servida, G., Gilman, R. (17 décembre 2025). « Monetising Misogyny: Engagement Farming and the Tactics Behind Incendiary Online Content. ». Global Network on Extremism Technology. https://gnet-research.org/2025/12/17/monetising-misogyny-engagement-farming-and-the-tactics-behind-incendiary-online-content

› Paul Elam, fondateur du groupe suprémaciste masculin *A Voice for Men* qui promeut l'idée que le féminisme opprime les hommes ;

› Nick Fuentes, nationaliste chrétien d'extrême droite à l'origine du mouvement « Ton corps, mon choix »,

› Andrew Tate, boxeur s'affirmant ouvertement misogyne et défendant une idéologie de domination masculine, sont cités comme cas d'étude emblématiques.

Ces trois figures opèrent sur plusieurs réseaux – X (anciennement Twitter), Telegram, YouTube, Discord – où leurs publications génèrent des millions d'interactions et redirigent stratégiquement vers des plateformes privées non modérées. Sur ces espaces fermés, l'utilisateur pénètre dans un écosystème monétisé où sont sollicités dons, abonnements payants et achats de produits dérivés[26], générant ainsi des bénéfices financiers considérables pour ces créateurs de contenus. Cette économie politique de la violence transforme la misogynie en modèle économique viable et récompense financièrement la production de discours haineux.

Écueils de la modération. Les techniques de modérations mises en place par les différentes plateformes favorisent aussi la prolifération des contenus masculinistes et violents. La modération des contenus circulant sur une plateforme est aujourd'hui opérée par des systèmes automatisés. Si l'être humain pourrait être capable de déceler le caractère misogyne ou sexiste d'un contenu, une machine peinera lorsque le contenu est contextuel ou codé par exemple. En outre, et comme démontré précédemment, la modération automatique entraîne la suppression, des contenus relatifs aux violences sexuelles, à la santé sexuelle, aux récits de traumas ou aux témoignage de survivantes et invisibilise les causes défendues par les féministes sur les réseaux[27].

Implication des dirigeants. Sur certaines plateformes, les dérives inhérentes aux pratiques de modérations ont même plutôt tendance à s'aggraver. Depuis l'investiture de Donald Trump :

› Mark Zuckerberg a annoncé la fin des programmes de fact-checking sur les plateformes Meta (Facebook et Instagram)[28].

› Elon Musk, a profondément remanié son équipe de modération de sorte que les effectifs sont désormais très faibles en comparaison au nombre d'utilisateurs de la plateforme[29]. La Commission européenne a par ailleurs infligé une amende de 120 millions d'euros à la plateforme pour violations de ses obligations de transparence au titre du Digital Services Act[30].

---

[26] *Ibid.*
[27] Voir *infra*, Partie 2, I, A, 2.
[28] Le Monde. (7 avril 2025). « Meta » met fin à son programme de fact-checking aux États-Unis ce lundi », *Le Monde*. https://www.lemonde.fr/pixels/article/2025/04/07/meta-met-fin-a-son-programme-de-fact-checking-aux-etats-unis-ce-lundi_6592305_4408996.html
[29] Duffaut, M. (11 janvier 2024). « Depuis Elon Musk, Twitter/X a licencié plus d'un tiers de ses employés dans la modération et la sécurité ». Radio France.
[30] Commission Européenne. (5 décembre 2025). « La Commission inflige à X une amende de 120 millions d'euros au titre du règlement sur les services numériques ». Communiqué de presse. Bruxelles. https://digital-strategy.ec.europa.eu/fr/news/commission-fines-x-eu120-million-under-digital-services-act

Focus.
YouTube, laboratoire des masculinités oppressives

Mainstreamisation du masculinisme. L'éloge d'une masculinité que la sociologue australienne Raewyn Connell qualifie d'« hégémonique » – en ce qu'elle configure des « pratiques de genre » visant à assurer la perpétuation du patriarcat et la domination des hommes sur les femmes – trouve aujourd'hui pleinement à s'exprimer sur des plateformes telles que YouTube. Une frange importante de l'extrême droite nationaliste et identitaire a investi ce thème de manière récurrente, parvenant à attirer un public essentiellement masculin s'accroissant de jour en jour.

Des créateurs tels que

- **Le Raptor** dissident (753 000 abonnés) ;
- **Baptiste Marchais** (280 000 abonnés) ;
- **Papacito** (200 000 abonnés avant la fermeture de sa chaîne en 2023) ou ;
- **Julien Rochedy** (140 000 abonnés)

produisent des vidéos dépassant régulièrement le million de vues et cherchent explicitement à former la culture politique d'un public jeune. Là où Ugo Gil Jimenez – alias Papacito – use ouvertement de la provocation et de la polémique pour véhiculer ses idées, Julien Rochedy – ancien président du Front national de la jeunesse – se pare d'une rigueur intellectuelle apparente pour s'étendre sur des sujets qu'il juge problématiques au rang desquels figure le « post-féminisme ».

Stratégie de diffusion et normalisation idéologique. Dans un registre évolutif mais demeurant fondé sur l'humour – dont le caractère déresponsabilisant permet d'éviter la censure et les poursuites judiciaires – et l'irrévérence – fonctionnant comme stratégie subversive formelle –, une myriade de vidéastes de droite radicale a fait son apparition sur YouTube. Reprenant les codes de l'*alt-right* états-unienne, ces nouvelles figures de l'extrême droite ont réussi à fidéliser un public qui ne cesse de s'élargir. Loin des caricatures, le chercheur Benjamin Tainturier estime pour sa part qu'il serait erroné de penser que l'internaute s'enfoncerait inexorablement dans un tunnel de vidéos de plus en plus réactionnaires, qui ne pourraient que le convaincre de l'existence d'un « grand remplacement ». La force de l'extrême droite sur la plateforme réside plus subtilement dans la création d'un réseau de vidéos aux thématiques vraisemblablement diversifiées et dont le contenu est insidieusement présenté comme neutre et apolitique. Cette stratégie de normalisation idéologique par dilution thématique et déni de la dimension politique des contenus s'avère particulièrement efficace auprès d'audiences jeunes encore peu familiarisées avec les codes du discours politique radical.

Rhétoriques victimaires. Dans sa vidéo-conférence de deux heures consacrée aux distinctions entre masculinité et féminité, Julien Rochedy affirme ainsi : « En à peine trente ans, une importante révolution anthropologique et morale a eu lieu. Vouloir être un homme, ce que tous nos pères voulurent, devient subitement suspect, ridicule, coupable. Désormais, dans tous les médias, à l'université [...] règne cette idéologie déconstructiviste et culpabilisatrice ». Cette rhétorique victimaire, caractéristique du discours masculiniste, procède par inversion systématique des rapports de domination réels.

Réalités objectives. Or, les données statistiques disponibles contredisent frontalement cette supposée oppression masculine. Les inégalités salariales demeurent de l'ordre de 29,5 % entre hommes et femmes (9 % à postes et compétences égales) et 78 % des emplois à temps partiel sont occupés par des femmes. Ces dernières restent quasi inexistantes dans les instances de décision des entreprises du CAC 40[31] et demeurent surreprésentées dans la réalisation du travail domestique, largement dévalorisé et toujours non rémunéré dans nos sociétés. Face à ces faits établis, nul doute quant au fait de savoir si ces créateurs de contenus ignorent volontairement ces réalités ou s'ils procèdent délibérément à leur occultation en se fondant en vérité davantage sur des ressentis individuels et hautement subjectifs que sur l'état des rapports de force structurant le monde social.

La « crise de la masculinité » constitue donc bien moins une réelle perturbation venant bouleverser les rapports de force entre femmes et hommes qu'un discours performatif visant à défendre, voire à consolider, un système de domination qui continue de profiter structurellement à une partie spécifique de la population.

Nécessité d'une réponse éducative structurelle. L'analyse de la genèse, de la structuration culturelle et de la diffusion algorithmiquement facilitée des mouvances masculinistes révèle un phénomène d'ampleur systémique qui ne saurait être appréhendé comme une simple dérive marginale des espaces numériques. La sophistication des stratégies de dissimulation idéologique, la professionnalisation de l'économie politique de la haine et l'implication directe des infrastructures numériques dans la propagation de ces discours antiféministes témoignent d'une transformation profonde de l'écologie informationnelle contemporaine. Face à cette structuration massive de la violence idéologique en ligne, les seules réponses répressives ou techniques – modération renforcée, sanctions judiciaires, régulation des algorithmes – bien que nécessaires, s'avèrent insuffisantes. La persistance et l'amplification de ces phénomènes appellent une transformation plus radicale portant sur les conditions mêmes de socialisation aux rapports de genre dans l'espace numérique. C'est précisément dans cette perspective que l'éducation à la vie affective, relationnelle et à la sexualité, intégrant explicitement la dimension numérique des interactions sociales contemporaines, apparaît comme un levier stratégique permettant à la fois de déconstruire les représentations véhiculées par les idéologies masculinistes et de valoriser les pratiques émancipatrices portées par les mouvements féministes. Poser ces bases éducatives dès le plus jeune âge constitue ainsi une condition nécessaire pour transformer durablement notre culture du numérique.

[31] SKEMA Business School. (23 février 2026). CAC 40 : *plus de femmes, mais toujours pas au sommet*. https://www.skema.edu/fr/communique-de-presses/cac-40-plus-de-femmes-mais-toujours-pas-au-sommet

C - La transversalité des enjeux d'éducation au numérique à la vie affective, relationnelle et sexuelle (EVARS)

Pédagogie. L'un des axes de travail le plus important reste celui de la pédagogie, qu'elle concerne les personnes mineures comme les personnes majeures. Dans un contexte de numérisation de plus en plus poussée de nos sociétés et au regard de la place proéminente des outils numériques dans nos espaces de vie et surtout de l'accès précoce aux espaces en ligne, il n'est plus envisageable de penser une éducation excluant le prisme du numérique. Au contraire, le numérique devient un objet d'apprentissage à part entière.

Éducation au numérique. Incluant la citoyenneté numérique[32], elle peut et doit être appréhendée dans sa globalité dès le plus jeune âge. Outre le fait de transmettre des savoirs, c'est aussi permettre aux individus de percevoir les espaces numériques comme des outils d'émancipation et de vivre-ensemble. À l'ère du numérique, le concept de faire société ensemble se trouve bouleversé face au nouveau contrat social qu'internet propose. Bien naviguer en ligne implique des connaissances à propos de soi et des autres, des moyens de protection, un respect d'autrui et surtout un esprit critique. L'éducation au numérique peut prendre des formes bien diverses et être abordée sous de nombreux angles. Toutefois, lorsque l'on s'intéresse aux enjeux de haine en ligne et de relations humaines, il y a bien un domaine dans lequel inclure ces espaces et pratiques numériques qui semble incontournable dans le but de décloisonner nos représentations et surtout de considérer le continuum des violences : l'EVARS.

Programme EVARS. L'un des volets de l'action publique dont l'envergure est à la hauteur des enjeux en présence est l'intégration des pratiques liées au numérique dans le programme d'Éducation à la Vie Affective, Relationnelle et à la Sexualité (EVARS). Attendu pendant 24 ans, le programme EVARS a été publié en février 2025 par le Ministère de l'Education Nationale et de la Jeunesse. Il reflète un changement dans les mœurs et la prise en compte de certaines réflexions féministes, abordant ouvertement les questions du rapport au corps, du plaisir, des interactions libres et consenties, mais également « des représentations de la sexualité dans l'espace public »[33], et se propose notamment de « repérer des discriminations issues de stéréotypes, notamment de genre ». L'EVARS se donne en effet pour objectif d'aider les jeunes à mieux comprendre leurs émotions, leurs relations et leur sexualité. Elle leur donne des outils indispensables pour faire des choix responsables et épanouissants, en accord avec soi-même et dans le respect des autres. Cette démarche éducative s'appuie sur des principes essentiels comme l'égalité, l'écoute, la tolérance et l'ouverture aux différences. L'éducation au numérique s'inscrit dans ce programme, dans 3 des 4 cycles scolaires, comme une thématique transversale. Ainsi, nous retrouvons :

> Au 2ème cycle : un apprentissage à « prévenir les risques liés à l'usage du numérique et d'internet ». La capacité de définition des cyberviolences est ici primordiale.

> Au 3ème cycle : celui de « Distinguer vie publique et vie privée, en réfléchissant à ce que signifie la liberté individuelle, en particulier sur les réseaux sociaux. ». Cet objectif replace le consentement au centre, dans un espace qui semble parfois peu saisissable et où il est encore aisé d'échapper à la loi.

> Au 4ème cycle : il s'agit de pouvoir « Se protéger et protéger les autres : l'intimité à l'ère des réseaux sociaux ».

---

[32] La citoyenneté numérique représente une dimension de l'éducation à la citoyenneté qui vise à apprendre aux élèves à travailler, vivre et partager dans des environnements numériques de manière positive. (définition du Ministère de l'Education Nationale)

[33] Ministère de l'Éducation Nationale, de l'enseignement supérieur et de la recherche. (février 2025). *Un programme ambitieux : Éduquer à la vie affective et relationnelle, et à la sexualité.*

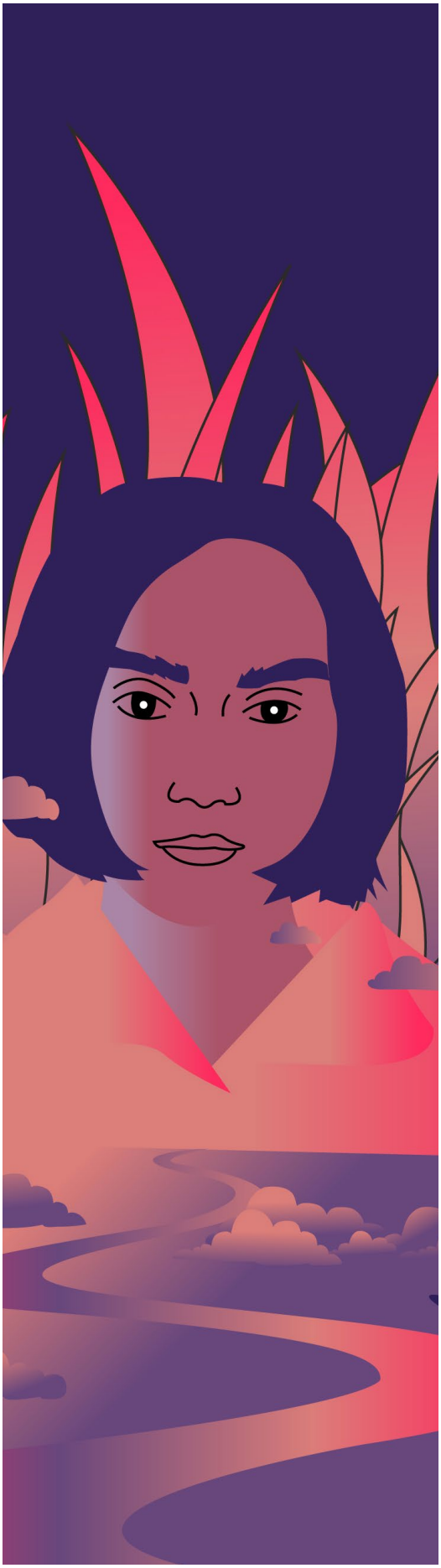
Éducation féministe. Ainsi, les usages et mésusages du numérique sont abordés dans le cadre du troisième axe du programme intitulé : « Trouver sa place dans la société, y être libre et responsable ». La compréhension du cyberespace, des interactions et des violences qui s'y déroulent est ici comprise comme un devoir civique. Selon le rapport Haut Conseil à l'Égalité (HCE) de 2025, 9 Français·es sur 10 disent soutenir l'instauration des séances d'EVARS, perçues comme la mesure la plus efficace contre le sexisme et les violences de genre. L'éducation au numérique sous le prisme du féminisme s'impose ainsi comme une nécessité pour tenter d'endiguer ce transfert de violence, dans des lieux où la frontière entre espace public et privé est d'autant plus friable. La notion de consentement n'a jamais été aussi importante que depuis la généralisation de l'usage du numérique mais sa réalisation suppose un processus de déconstruction des violences qui peuvent y surgir.

Maîtriser pour mieux lutter. Quand les pratiques numériques sont pensées et conçues pour donner du pouvoir d'agir, elles peuvent enrichir l'EVARS et participer à réduire les comportements de haine en ligne. Cet éveil est en effet un des remèdes en ce qu'il permet d'insister sur des messages essentiels et de les diffuser : cultiver l'empathie, respecter l'altérité, accepter la différence. Comme #StopFisha l'écrit dans Combattre le cybersexisme les objectifs doivent être de définir les différentes cyberviolences pour savoir les identifier tout en fournissant les outils aux plus jeunes – et notamment, aux femmes et minorités de genre – pour se protéger et se défendre en ligne. Cela implique de sensibiliser la population aux droits numériques pour faire du net un espace sécurisé permettant l'exercice de toutes nos libertés, pour jouer, créer, former des communautés, apprendre à façonner en toute sécurité son identité numérique et pouvoir jouir, de façon égalitaire, des nouvelles technologies[34]. Pour Anaïs Condomines et Emmanuelle Friedmann, « puisque le cyberharcèlement est le miroir de la société, il faut s'attaquer à la racine de toutes les discriminations. Il faut des politiques publiques, une éducation à la bienveillance et une valorisation de l'empathie »[35]. Ces considérations dûment mises en œuvre, elles permettront l'émergence d'une intelligence émotionnelle numérique collective, c'est-à-dire une capacité partagée à construire de bonnes relations avec les autres en ligne et à leur venir en aide.

[34] Association #StopFisha : Outaik, H., Outaik, H., Bories, J., Reynaud, L., Diogo, L. P., Drillaud, L. G., Janvier, M., Haouari, S., Maclaren, S. C., & Pardo, R.-F. (Coord.). (2021). *Combattre le cybersexisme*. Éditions Leduc. p.152.
[35] Condomines, A. & Friedmann, E. (2019). *Cyberharcèlement. Bien plus qu'un mal virtuel*. Pygmalion.

Démocratisation de l'information. La réciprocité des apports entre l'éducation au numérique et l'EVARS a ainsi été comprise par certaines institutions françaises. Le Conseil national du numérique a publié en 2024 un dossier particulièrement complet consacré à l'usage du numérique dans l'EVARS et intitulé « Éveil à la vie affective, relationnelle et sexuelle. Donner le pouvoir d'agir ». Ce dossier pose la question suivante : Comment les pratiques numériques peuvent-elles être employées pour enrichir l'éveil à la vie affective, relationnelle et sexuelle et participer du même tenant à réduire les comportements de haine en ligne et dans la société en général ? Le parti pris de ce dossier est de considérer les outils numériques comme des espaces entre pairs propices et vertueux et qui pourraient favoriser l'épanouissement affectif, relationnel et sexuel. Ils sont en mesure de répondre à certains besoins en information, exploration ou fournir clés de compréhension et sont complémentaires aux actions pédagogiques traditionnelles. À contre-courant d'une diabolisation des réseaux sociaux, souvent perçus dans l'esprit collectif comme des lieux de haine avant d'être des moyens d'éveil, il nous semble aussi pertinent d'insister sur l'utilité que tiennent ces espaces d'émancipation, d'autonomie et d'apprentissage (par rapport aux familles et aux institutions) en devenant presque une chambre à soi, un espace intime dématérialisé.

Limites. Néanmoins, ce processus d'éducation possède des limites. Par exemple, bien qu'il fasse l'objet d'un portage gouvernemental, l'EVARS se heurte à plusieurs obstacles, notamment le manque de cadrage budgétaire[36] (indemnisation des temps de préparation et Indemnités de Mission Particulière - IMP, budgets alloués à la mise en place des ateliers…), ou encore le temps et les moyens de formations des professionnel·les (infirmier·ères scolaires, enseignant·es, en première ligne). À cette réalité, s'ajoute celle de la baisse des subventions allouées aux associations expertes de ce type d'interventions en milieu scolaire. L'intérêt de faire se rejoindre éveil à la vie relationnelle, affective et à la sexualité et éducation aux médias et à l'information est à la croisée de tous les enjeux précédemment abordés. Cette union est susceptible d'encourager des enseignements plus complets et inclusifs et requiert dès lors de réels investissements. Face à cette nouvelle ère de haine et à la croissance des idéologies masculinistes, l'EVARS s'illustre peut être comme l'une de nos armes les plus précieuses.



[36] Publication conjointe et documentée de NousToutes, Parents & Féministes, Le Planning familial, & #StopFisha. (à partir du 17 juin 2025). *L'EVARS, c'est pour nous toustes* [Publications Instagram en série]. Instagram.

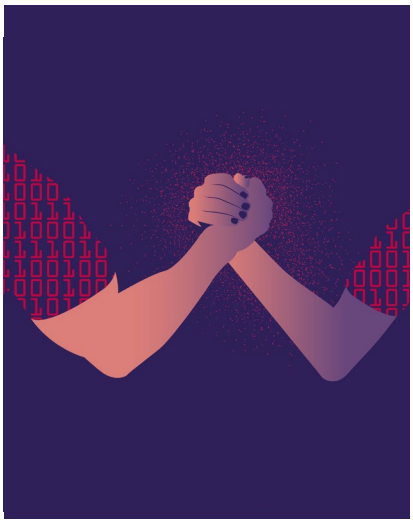
2. Enjeux technologiques

L'illusion de la neutralité. Les outils numériques ne sont ni bons ni mauvais par nature, mais ils ne sont pas neutres pour autant : ces technologies servent les intérêts de leurs concepteurs et sont imaginées, financées, développées et déployées dans un monde déjà structuré par des rapports de pouvoir. Ces outils encodent donc, dans leurs interfaces comme dans leur fonctionnement, des choix sociaux, économiques et culturels. C'est précisément ce que rappelle la chercheuse Isabelle Collet lorsqu'elle insiste sur le fait que le numérique est un enjeu démocratique et non un simple domaine technique réservé à quelques spécialistes ; elle s'inquiète du risque représenté par une transition numérique pensée par une population socialement homogène, et l'effet de miroir grossissant que cela produit sur les biais existants[37]. Cette perspective rejoint un constat central : non contente de refléter les inégalités, la technologie peut aussi les automatiser et les renforcer, notamment lorsque les plateformes sont organisées autour de la captation de l'attention et de la monétisation de l'engagement. En somme, les architectures numériques font davantage que simplement refléter le monde dans lequel elles sont conçues : elles participent activement à le configurer.

A - Conception et usages des services et outils numériques

Faible représentation. La sous-représentation des femmes et, plus largement, des minorités dans les métiers du numérique a des effets directs sur les technologies produites. Lorsque l'innovation est majoritairement pensée depuis des positions masculines, blanches, valides et socialement favorisées, certains usages vont être anticipés et d'autres ignorés, et cela a des conséquences très concrètes sur la sûreté des femmes en ligne.

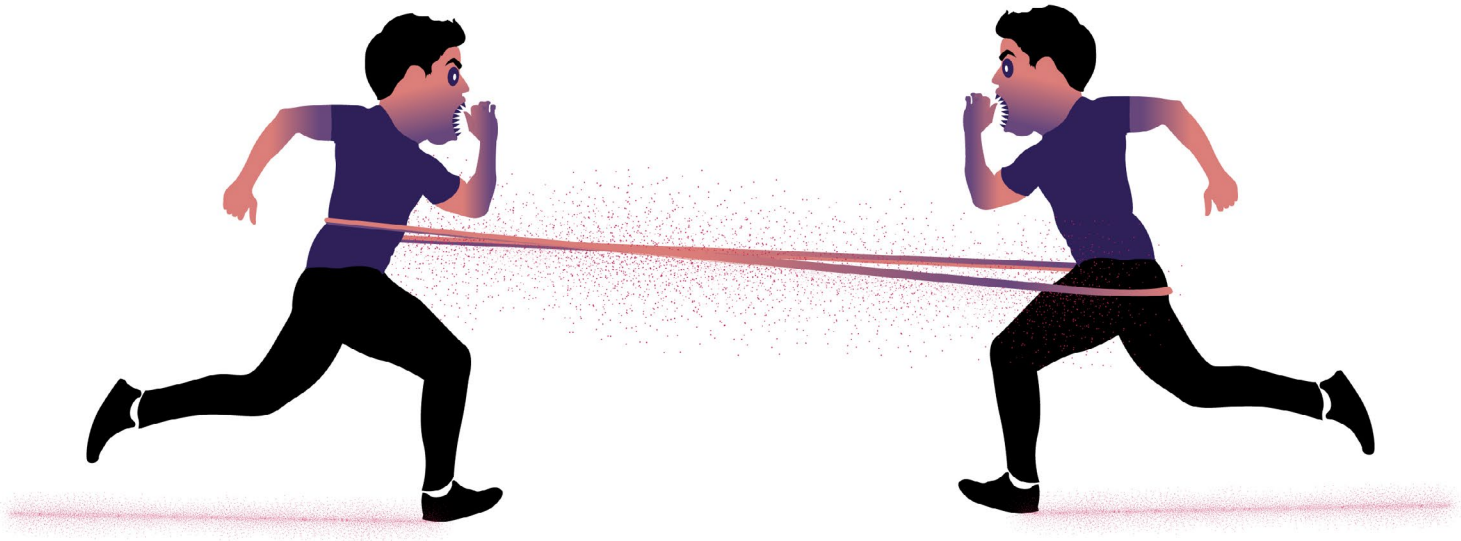
1 - Conception des nouvelles technologies



Reconduction des discriminations. Loin de constituer un espace neutre et émancipateur, le développement de l'intelligence artificielle reproduit et amplifie les rapports de domination sexistes préexistants. Les algorithmes héritent des biais contenus dans les données sur lesquelles ils sont entraînés, transformant ainsi des siècles de discrimination en lignes de code. L'affaire du système de recrutement d'Amazon en 2018 l'illustre parfaitement : entraîné sur une base de CV majoritairement masculins, l'algorithme a mécaniquement discriminé les candidatures féminines[38], automatisant ainsi l'exclusion des femmes. Cette violence algorithmique ne relève pas d'un dysfonctionnement technique mais d'une reproduction des structures patriarcales qui organisent le monde du travail.

[37] Collet, I. (2025). *Le numérique est l'affaire de toutes*. Le Bord de l'eau.
[38] Dastin, J. (2018, 9 octobre). Insight: Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG

Prolongement des stéréotypes de genre. Au-delà de ces violences explicites, l'intelligence artificielle véhicule et renforce les stéréotypes de genre, notamment à travers la conception des assistants virtuels et agents conversationnels. Alexa, Siri, Cortana : la quasi-totalité des IA grand public se voient attribuer des voix féminines, des personnalités dociles et des fonctions de service[39]. Ce choix systématique ne doit rien au hasard. Les études marketing montrent que les voix féminines sont perçues comme plus chaleureuses, rassurantes et dignes de confiance – autant de qualités traditionnellement assignées aux femmes dans les rôles de soin et d'assistance. Cette tendance s'étend aux IA humanoïdes comme l'actrice virtuelle Tily Norwood, la ministre virtuelle albanaise Diella ou la chanteuse Tata Taktumi, chacune conçue selon des canons de beauté conventionnels. Ces créations numériques offrent une version fantasmée et totalement contrôlable de la féminité : malléable à l'infini tant physiquement que psychologiquement, toujours disponible, jamais contestataire. Elles matérialisent le fantasme patriarcal d'un corps féminin parfaitement soumis aux désirs masculins. La sexualisation régulière de ces IA sur les réseaux sociaux et dans les productions culturelles[84] normalise l'objectification des femmes et façonne les représentations collectives, avec des conséquences qui dépassent largement les écrans[40].



La socialisation algorithmique à la haine. Ces environnements ne se contentent pas de reproduire des biais : ils socialisent aussi politiquement celles – et surtout ceux – qui y gravitent. Les contenus masculinistes, réactionnaires et antiféministes circulent de manière transversale entre jeux, forums, réseaux sociaux, vidéos et influenceurs. Les travaux de recherche conduits par Reset Australia et l'Institute for Strategic Dialogue (ISD) montrent ainsi comment les recommandations de YouTube, et surtout de YouTube Shorts, exposent progressivement les garçons autant que les jeunes hommes à des contenus misogynes, antiféministes et produits par la manosphère[41]. On découvre ainsi comment s'organise cette escalade vers des contenus toujours plus radicaux au fil des interactions. Les algorithmes ont des effets très concrets car ils fabriquent des trajectoires d'exposition idéologique via la mise en avant de contenus qui renforcent les logiques de haine et de domination : l'économie de l'attention, en récompensant les contenus clivants, humiliants et haineux par de la visibilité, participe ainsi à diffuser massivement les discours et contenus oppressifs.

---

[39] Courrier international. (octobre 2025). *« Soumises et dociles » : pourquoi les IA humanoïdes sont (presque) toujours des femmes. Courrier international*. https://www.courrierinternational.com/stories/technologie-soumises-et-dociles-pourquoi-les-ia-humanoides-sont-presque-toujours-des-femmes_23629

[40] Des Roches, A. (octobre 2025). *Sexy robots: A perpetuation of patriarchy*. DigitalCommons@CalPoly. https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1244&context=comssp

[41] Morrigan, V. (2022). Patriarchal imaginaries beyond the human: "sex" robots, fetish and fantasy in the domination and control of women. *In* K. Richardson & C. Odlind (Eds.), *Man-made women: Social and cultural studies of robots and AI*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-19381-1_6

2 - Mésusages et détournements des nouvelles technologies

Le business de la *nudification*. Les outils dits de « nudification » en offrent une démonstration particulièrement nette : ils transforment en service commercial une violence sexiste préexistante qui consiste à objectifier les femmes et à disposer de leur corps sans leur consentement. L'IA générative industrialise ces violences en permettant le développement d'applications et de sites dont le but est de produire des *deepfakes* à caractère sexuel, soit des images sexuelles truquées réalisées à partir de photos ordinaires – souvent récupérées sur les réseaux sociaux – sans qu'il n'y ait besoin pour cela de compétence technique particulière. Cela participe à la banalisation de la production d'images sexuelles non consenties, d'autant plus que des travaux de recherche montrent l'existence d'un écosystème commercial structuré d'outils de nudification en ligne, facilement accessibles[42]. Dans le champ des cyberviolences, cela vient confirmer une tendance déjà largement constatée : l'innovation technologique est régulièrement instrumentalisée à des fins de contrôle, d'humiliation et de sexualisation forcée des femmes et des filles.

Grok : quand l'intelligence artificielle de X produit des contenus pédocriminels et déshabille des femmes sans leur consentement

Grook*
*Crook= escroc, malhonnête

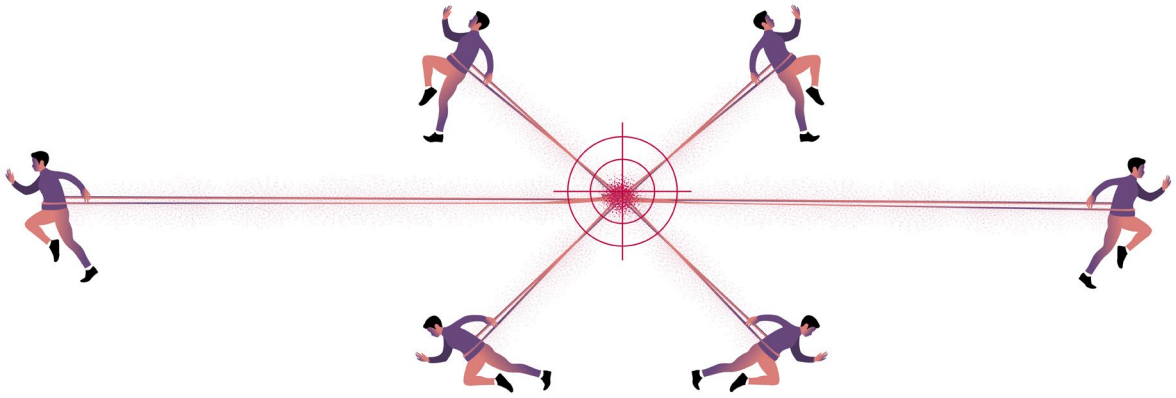
L'intelligence artificielle Grok, développée par la plateforme X et avec laquelle il est possible d'interagir à la vue de tous sur le réseau social, illustre de manière particulièrement préoccupante l'instrumentalisation des outils d'IA générative pour produire des contenus à caractère sexuel abusifs et parfois illicites.

Début 2026, la plateforme X s'est trouvée inondée d'images sexualisées générées par Grok et représentant des femmes et des mineur·es, révélant l'absence de garde-fous techniques permettant de prévenir la production de contenus inappropriés. L'affaire a pris une dimension particulièrement insoutenable lorsque, suite à l'incendie tragique de Crans-Montana (Suisse) le 1er janvier 2026, certains utilisateurs ont instrumentalisé Grok pour générer des deepfakes sexualisés à partir de photographies des victimes décédées, demandant à l'IA de « mettre en bikini » ou dénuder des personnes. Restés en ligne malgré des signalements effectués par le signaleur de confiance Point de Contact, ces contenus ont poussé la Commission Européenne à ouvrir une nouvelle enquête contre la plateforme X en ciblant ces contenus au titre de la réglementation européenne sur les services numériques (RSN/DSA).

Grok ne constitue évidemment pas un cas isolé : LES technologies d'IA générative, lorsqu'elles sont conçues sans protocoles de sécurité suffisants ou lorsque ces protocoles sont délibérément contournés, présentent un risque structurel de détournement à des fins de violences sexuelles. Ces cas soulèvent des questions centrales au sujet de la responsabilité des concepteurs dans l'anticipation des usages malveillants, les choix techniques et l'efficacité des dispositifs de modération face à des technologies dont la sophistication croissante démultiplie les possibilités d'abus.

[42] Gibson, C., Olszewski, D., Brigham, N. G., Crowder, A., Butler, K. R. B., Traynor, P., Redmiles, E. M., & Kohno, T. (2024). *Analyzing the AI Nudification Application Ecosystem*. arXiv. https://arxiv.org/html/2411.09751

Surveillance et cyberviolences. Les dispositifs de surveillance constituent un autre versant des cyberviolences, souvent moins visible que les insultes ou les campagnes de harcèlement. L'inventivité des agresseurs est hélas sans limites et, dans les contextes de violences au sein du couple et intra-familiales, les technologies numériques sont fréquemment détournées par les auteurs des violences pour prolonger et intensifier l'emprise qu'ils exercent sur les victimes. Or cela n'est que rarement pensé ou anticipé lors de la conception de ces appareils afin de garantir une utilisation qui soit sûre, notamment pour les femmes et les minorités. Ainsi, de nombreux logiciels et périphériques connectés simples à utiliser et faciles à se procurer permettent de surveiller et de contrôler à distance les faits et gestes d'une personne. Les technologies numériques deviennent alors, aux mains des agresseurs, des instruments rêvés pour priver leurs victimes de toute autonomie et produire un climat d'insécurité permanent[43].



Des technologies détournées pour contrôler. Les outils mobilisés sont multiples. Il peut s'agir de logiciels espions installés sur un téléphone, de traceurs GPS glissés dans une voiture, dans une poussette ou dans un sac, d'applications de géolocalisation imposées sous prétexte de sécurité, ou encore de caméras connectées – parfois dissimulées – servant à surveiller les victimes. Les objets connectés les plus ordinaires (alarmes, ampoules, thermostats, systèmes domotiques) peuvent eux aussi être instrumentalisés pour intimider et désorienter, par exemple en éteignant les lumières à distance ou en actionnant les volets roulants. La violence tient ici à la fois au contrôle effectif et à l'effet psychique produit : la victime peut finir par douter d'elle-même et de sa perception, voire de sa santé mentale.

La banalisation de la surveillance. Au-delà des violences exercées dans le cadre du couple ou de la famille, les dispositifs de surveillance s'inscrivent dans un système plus vaste où la collecte de données est devenue un principe ordinaire de fonctionnement. Les plateformes, les applications et les services connectés enregistrent en continu nos traces : déplacements, habitudes, recherches, horaires, interactions, achats, etc. Ces informations, qui ont une valeur économique considérable, alimentent des modèles fondés sur la prédiction de nos comportements[44]. Il ne s'agit évidemment pas de confondre ce capitalisme de surveillance avec l'activation d'un logiciel espion par un·e partenaire violent·e, mais ces deux réalités se déploient au sein d'un même environnement technique : un espace où la surveillance, la traçabilité et l'accès aux données sont banalisés. Et c'est précisément cette banalisation qui rend ces violences plus faciles à exercer, mais aussi plus difficiles à dénoncer. Le contrôle n'apparaît plus toujours comme une violence ; il peut prendre la forme d'une option de géolocalisation activée par défaut, d'un logiciel de contrôle parental, d'une application de santé, d'un historique accessible, d'un compte partagé ou d'un objet connecté. La frontière entre la surveillance exercée par un individu, celle instaurée par un État ou encore celle déployée par une entreprise à des fins de collecte de données devient alors plus poreuse qu'on ne le croit.

---

[43] Salmona, L. (2025). *15 idées reçues sur les cyberviolences et le cyberharcèlement*. Le Cavalier Bleu.
[44] Zuboff, S. (2022). *L'Âge du capitalisme de surveillance : le combat pour un avenir humain face aux nouvelles frontières du pouvoir*. Zulma.

B - Renouvellement des approches au numérique

Politiser la fabrique du numérique. Les développements qui précèdent en attestent : l'innovation technologique elle-même reste marquée par un manque de diversité, avec des effets très concrets sur la manière dont chacun·e fait l'expérience du numérique. Le problème naît donc des conditions mêmes de production des technologies numériques : la composition des équipes, les imaginaires techniques dominants, les modèles économiques des plateformes et les architectures algorithmiques qui organisent la circulation des contenus. Une lecture féministe du numérique nécessite donc d'interroger, mais aussi de politiser, les conditions de production de ces outils : qui les conçoit et pour quels usages, avec quels impacts sur les populations.

Prévenir les cyberviolences dès la conception. Face à ces violences, il apparaît nécessaire de transformer la manière dont les technologies sont conçues. Une approche de type « *safety by design* » – ou ici plus précisément féministe et anti-surveillance by design – devrait être intégrée dès la conception des appareils, applications et services connectés. Cela implique de penser en amont les usages abusifs et violents possibles : quelles alertes sont envoyées lorsqu'un compte est espionné, quels paramètres sont activés par défaut, et comment une personne peut reprendre rapidement le contrôle de ses outils. Pour concevoir des technologies plus sûres, il est essentiel de reconnaître que les rapports de domination structurent les usages réels du numérique. Une telle approche suppose aussi de renforcer la transparence des plateformes et des fabricants, d'imposer des normes et des obligations de protection des personnes les plus exposées, et de développer des standards de sécurité qui intègrent explicitement les risques de violences intra-familiales et sexistes. C'est seulement en repensant de fond en comble la conception de ces outils, afin d'empêcher les agresseurs de transformer impunément des objets du quotidien en instruments de contrôle, qu'il sera possible de combattre ces violences à la source.

Encadrer le développement de l'IA. Loin de freiner l'innovation technologique, la réglementation des modèles d'intelligence artificielle constitue elle aussi un impératif démocratique dont la réalisation peut advenir en mobilisant les instruments existants[45]. Le Conseil de l'Europe propose à ce titre d'instaurer une « présomption de biais algorithmique »[46] : tout algorithme serait présumé biaisé tant que ses concepteurs n'auraient pas démontré avoir mis en place des mesures concrètes pour prévenir et corriger ces biais. Cette inversion de la charge de la preuve responsabiliserait davantage les entreprises en les contraignant à l'anticipation plutôt qu'à la réaction. Par ailleurs, le droit doit cesser d'appréhender le féminisme comme une simple opinion politique pour l'intégrer comme grille d'analyse structurante. Cela implique l'adoption systématique d'une approche intersectionnelle, l'usage d'un langage inclusif et la prise en compte des besoins des groupes marginalisés lors de l'élaboration des réglementations sur l'IA[47].

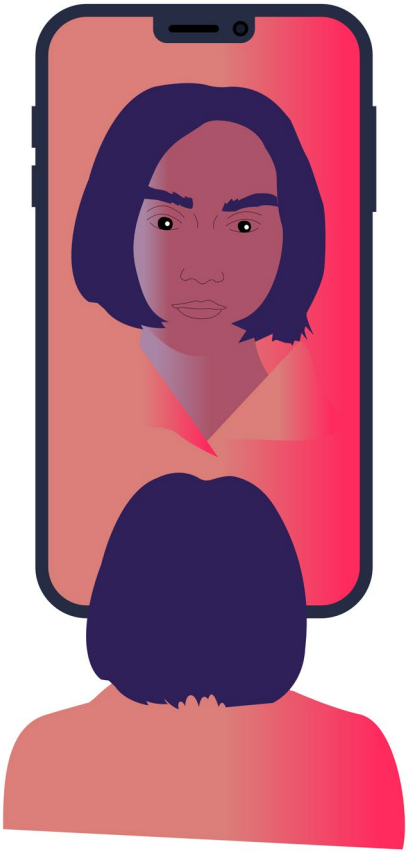
---

[45] Albrengues, A., & Lu, L. (octobre 2025). *Weight of gender in artificial intelligence models' implementation in the European Union non-discrimination laws*. ELSP. https://kclpure.kcl.ac.uk/portal/en/publications/weight-of-gender-in-artificial-intelligence-models-implementation

[46] Bartoletti, I. and Xenidis R., «Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination», (2023) Gender Equality Commission (GEC) and The Steering Committee on Anti-discrimination, Diversity and Inclusion (CDADI), Octobre 2025: https://rm.coe.int/study-on-the-impact-of-artificial-intelligence-systems-their-potential/1680ac99e3

[47] Guevara-Gómez A.,de Zárate-Alcarazo L.O., Ignacio Criado J., «Feminist perspectives to artificial intelligence: Comparing the policy frames of the European Union and Spain» (2021) 26(2) Information Polity, 173-192

Féminiser le développement technologique. Augmenter la représentation des femmes, des personnes trans et des minorités racisées dans le secteur technologique n'est pas qu'une question de justice sociale : c'est une condition nécessaire pour que les usages et les besoins de ces populations soient anticipés dès la conception[48]. Cette diversification implique le développement de bonnes pratiques en matière de coopération avec la société civile et une responsabilisation accrue des entreprises qui développent et déploient ces technologies[49] [50]. Établir des standards communs en matière de représentation et de prise en compte des voix marginalisées pourrait à cet égard éviter les stratégies de contournement réglementaire.



Nouveaux paradigmes. En écho au concept de *safety by design*, l'approche dite de l'« *equality by design* » – littéralement « l'égalité dès la conception » – propose d'intégrer dès l'origine du processus de développement une réflexion sur les rapports de pouvoir que les technologies risquent de reconduire ou d'amplifier. Concrètement, cela implique d'interroger systématiquement la structure des plateformes, les modèles économiques qui les sous-tendent et les choix techniques opérés par les développeur·ses pour identifier et corriger les biais potentiels avant qu'ils ne se transforment en violences effectives. L'*equality by design* propose notamment d'auditer les bases de données utilisées pour entraîner les algorithmes, d'en éliminer les biais identifiés et d'en diversifier radicalement les sources[51]. C'est dans cette lignée que s'inscrit le mouvement du "*data feminism*" ou « féminisme de la donnée » offre des outils méthodologiques prometteurs mais ce type d'approche reste toutefois marginal, faute de recherche suffisante et de volonté politique concomitante[97]. Une approche véritablement féministe exige d'assumer explicitement le projet politique d'une technologie conçue pour servir l'égalité et l'émancipation plutôt que pour reconduire les hiérarchies sociales existantes[52] [53] [54] [55] . Cela suppose de dépasser à la fois la simple reproduction des discriminations préexistantes et l'illusion d'une neutralité technique qui invisibilise les rapports de domination au lieu de les combattre.

---

[48] UN Women, «Accelerating efforts to tackle online and technology-facilitated violence against women and girls», 2022, Octobre 2025: https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls.

[49] S Yeung K. for the Council of Europe, «Responsibility and AI – A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework» (2019), Octobre 2025: https://rm.coe.int/responsability-and-ai-en/168097d9c5.

[50] Bartoletti I. and Xenidis R., «Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination», (2023) Gender Equality Commission (GEC) and The Steering Committee on Anti-discrimination, Diversity and Inclusion (CDADI), Octobre 2025: https://rm.coe.int/study-on-the-impact-of-artificial-intelligence-systems-their-potential/1680ac99e3.

[51] Equal Rights Trust. (2025). *Principles on equality by design in algorithmic decision-making*. https://www.equalrightstrust.org/sites/default/files/ertdocsPrinciples%20on%20Equality%20by%20Design%20in%20Algorithmic%20Decision%20Making_0.pdf

[52] Ganesh M.J., Moss E. (2022). « Resistance and refusal to algorithmic harms: Varieties of 'knowledge projects' », 183(1) Media International Australia, 90-106.

[53] Cummings R. (2022) « This is how AI can support diversity, equity and inclusion », World Economic Forum, Octobre 2025: https://www.weforum.org/agenda/2022/03/ai-support-diversity-equity-inclusion

[54] Eubanks V. (2018). « Automating inequality: How high-tech tools profile; police and punish the poor », (2018), St Martin's Press Inc.

[55] Pradhan A., Erete S., Chopra S., Upadhyay P., Sule O., et al. (2025). « No; not that voice again! »: Engaging older adults in design of anthropomorphic voice assistants (2025), 9(2), Proceedings of the ACM on human-computer interaction, Octobre 2025: https://dl.acm.org/doi/pdf/10.1145/3711039.

[56] Equality Now. (2025). A Call For An Intersectional Feminist Informed Universal Declaration On Digital Rights, Octobre 2025: https://equalitynow.org/news_and_insights/universal-declaration-on-digital-rights.

3. Enjeux sociaux

Normalisation des violences. Les espaces numériques ne se contentent pas de reproduire des rapports de domination préexistants : ils génèrent également leurs propres cultures de la violence, leurs codes et leurs modes de socialisation. Ces dynamiques socioculturelles se manifestent à la fois dans des environnements spécifiques où la masculinité hégémonique structure les interactions, mais également à travers des pratiques d'humiliation publique de masse visant à contrôler et sanctionner les femmes et les minorités qui transgressent les normes sociales. L'amplification algorithmique de ces tendances virales et l'efficacité relative des dispositifs de modération facilitent une impunité structurelle qui accentue les inégalités de genre au sein des espaces numériques.

A - Des espaces d'hégémonie masculine

Le *boys' club* du jeu vidéo. Le secteur du jeu vidéo incarne la quintessence d'un environnement social où la masculinité hégémonique structure les interactions. Les espaces de jeu en ligne restent fortement marqués par la normalisation des comportements agressifs et du harcèlement dans la structuration des échanges ; la violence est considérée comme une composante normale de la participation et les femmes et les minorités y sont dès lors surexposées aux insultes sexistes, aux menaces, aux violences sexuelles et aux campagnes de harcèlement coordonnées. Les cas de streameuses visées par des attaques répétées[57] montrent que ces violences poursuivent un but, celui de régir ces espaces numériques en rappelant sans cesse quelles sont les catégories de population considérées comme légitimes à évoluer dans ces univers – à savoir les hommes cisgenres blancs et hétérosexuels – et lesquelles ne le sont pas[58].

Attaques concertées. Il arrive parfois que des campagnes d'humiliation publique et de dénigrement soient organisées et coordonnées par des groupes essentiellement masculins via des canaux moins exposés ou alternatifs, tels que les exemples suivants :

- **de la Ligue du LOL** groupe actif à partir de 2009 et révélé publiquement en 2019[59] ;
- **du forum 18-25 de Jeuxvideo.com**[60] connu pour ses campagnes de cyberharcèlement organisées mêlant menaces et insultes et ciblant souvent des profils féminins ;
- **le Gamergate** en 2014[61] ;
- **l'usage des *bots* en temps réel sur Twitch** pour cibler des individus marginalisés[62].

---

[57] Trois hommes condamnés par la justice pour le cyberharcèlement de la streameuse Ultia, Le Monde,12 février 2025. https://www.lemonde.fr/pixels/article/2025/02/12/trois-hommes-condamnes-par-la-justice-pour-le-cyberharcelement-de-la-streameuse-ultia_6543805_4408996.html

[58] Salmona, L. (2025). *15 idées reçues sur les cyberviolences et le cyberharcèlement*. Le Cavalier Bleu.

[59] En France, la Ligue du LOL, un groupe principalement masculin de journalistes et communicants, a été exposé pour avoir mené des campagnes coordonnées de harcèlement en ligne contre des femmes et d'autres cibles, notamment sur Twitter.

[60] Condomines, A. (2017, 5 janvier). *Cyberharcèlement et «raids» antiféministes sur le forum 18-25 de JeuxVideo.com : «cela a assez duré». TF1 Info.* https://www.tf1info.fr/societe/cyberharcelement-et-raids-antifeministes-sur-le-forum-18-25-de-jeuxvideo-com-ca-a-assez-dure-2020332.html?

[61] Le Gamergate (#Gamergate) était une campagne de harcèlement sexiste et antiféministe visant des femmes journalistes et développeuses de jeux vidéo. La controverse portait sur la déontologie des journalistes, la censure et le sexisme dans le milieu du jeu vidéo. Le terme regroupe la polémique et les attaques qui ont eu lieu en août 2014.

[62] Cai, J., Chowdhury, S., Zhou, H., & Wohn, D. Y. (2023). Hate raids on Twitch: Understanding real-time human-bot coordinated attacks in live streaming communities. Proceedings of the ACM on Human-Computer Interaction, 7(CSCW2), Article 342, 1-28. https://arxiv.org/pdf/2305.16248

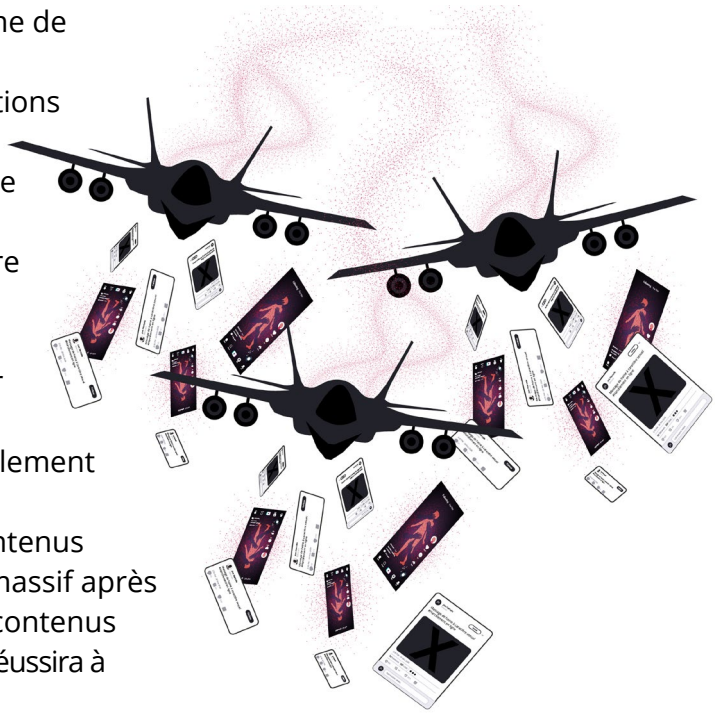
B - Des mécaniques d'humiliation publique

***Public* et *slut-shaming* : définitions et finalités.** Le *public-shaming** – humiliation publique – et le *slut shaming* – humiliation spécifiquement dirigées à l'encontre des sexualités des femmes et des minorités sexuelles – constituent des mécanismes de violence symbolique visant à sanctionner publiquement les comportements perçus comme transgressifs des normes sociales établies. L'expression *slut-shaming* se traduirait littéralement par « couvrir de honte les salopes », révélant ici la dimension profondément misogyne de cette pratique. Ces deux formes d'humiliation publique poursuivent des objectifs convergents : intimider les personnes visées, attaquer leur réputation, les censurer et les exclure des espaces publics numériques. Discréditer, humilier voire punir discrétionnairement et publiquement les individus dont les habitudes et pratiques sexuelles sont jugées inadaptées constitue un moyen éprouvé d'assurer le contrôle social sur les corps et leur soumission aux normes dominantes.

Cibles privilégiées et asymétries de genre. Ces pratiques violentes et profondément discriminantes visent principalement les femmes qui ne se conformeraient pas aux normes et injonctions sociales relatives à leur activité sexuelle, mais également les minorités de genre, d'orientation sexuelle et de pratiques sexuelles. Si la fréquence des rapports ou la nature des pratiques sexuelles sont bien souvent la cible du *slut-shaming*, celui-ci s'attaque également à l'apparence – tenues vestimentaires jugées provocantes, maquillage –, à la manifestation d'autres attributs – argent, statut social, position de pouvoir –, voire à leur simple présence en ligne. Qu'importe la notoriété et la visibilité, être une femme ou minorité de genre actif·ve en ligne expose systématiquement à de la violence : ici réside la profonde asymétrie de genre qui conditionne les conséquences d'une simple présence numérique.

Banalisation linguistique de la violence. L'emploi systématique du mot « pute » constitue une illustration particulièrement éloquente de ces violences. Au regard de la fréquence à laquelle ce terme est mobilisé sur les réseaux sociaux – que ce soit dans les publications, leurs commentaires ou les messages privés –, son usage semble aujourd'hui banalisé, alors même qu'il matérialise une forme de violence profondément sexiste et misogyne. Cette banalisation linguistique normalise l'insulte et la disqualification des femmes sur la base de leur sexualité, réelle ou supposée.

Victimes en France. Des personnalités publiques françaises, influenceuses et créatrices de contenus, ont été et continuent d'être massivement cyberharcelées sur les réseaux sociaux. Les internautes ont pris l'habitude de désigner certaines vagues de harcèlement massif par le terme « sauces », une euphémisation qui oblitère la nature violente et structurelle du cyberharcèlement. Parmi les victimes françaises figurent notamment :



- Léna Mahfouf, influenceuse régulièrement victime de *body- shaming** et de *slut-shaming*[63] ;
- Chloë Gervais, influenceuse ciblée pour ses positions féministes et victime de *slut-shaming*[64] ;
- Barbara Butch, DJ et militante LGBTQ+, victime de harcèlement lesbophobe et grossophobe[65] ;
- Aya Nakamura, chanteuse victime de misogynoire lors de sa participation à la cérémonie d'ouverture des Jeux Olympiques et Paralympiques de Paris[66] ;
- Hoshi, chanteuse lesbienne attaquée après avoir embrassé une danseuse sur scène[67],
- Salomé Saqué, journaliste victime de cyberharcèlement sexiste et *deepfakes* à caractère sexuel[68] ;
- Baghera Jones et Manon Lanza, créatrices de contenus toutes deux victimes d'un harcèlement misogyne massif après plusieurs vidéos mises en ligne par le créateur de contenus Squeezie (GP Explorer 2114, GP Explorer 3115, « Qui réussira à stopper le train ? »[69]) ;
- Sarah Bouchamama, créatrice de contenus et militante cyberharcelée pour avoir alerté sur l'expression problématique « beurette à khel »[70] ;
- Ranelle Brown, influenceuse et créatrice de contenus victime de raids d'insultes racistes et sexistes ainsi que de *doxing* via des lives TikTok pouvant durer des heures.[71]

---

[63] Courret, M. (2025, 21 mars). Elsa Bois, Léna Mahfouf, Chloé Gervais… : les compagnes de YouTubeurs, cibles constantes des masculinistes d'Internet. Marie-Claire. https://www.marieclaire.fr/elsa-bois-lena-situations-chloe-gervaispetites-copines-exs-youtubeurs-influenceurs-victimes-sexisme-masculinisme-cyberharcelement,1489220.asp

[64] *Ibid*.

[65] Le Monde avec AFP. (2025, 6 octobre). La DJ Barbara Butch cible d'une nouvelle campagne de cyberharcèlement, selon la Ville de Paris. Le Monde. https://www.lemonde.fr/societe/article/2025/10/06/la-dj-barbara-butch-cible-d-unenouvelle-campagne-de-cyberharcelement-selon-la-ville-de-paris_6644861_3224.html

[66] Le Monde avec AFP. (2024, 15 mars). Polémique Aya Nakamura aux JO : le parquet de Paris ouvre une enquête après un signalement de publications racistes visant la chanteuse. Le Monde. https://www.lemonde.fr/culture/article/2024/03/15/polemique-aya-nakamura-aux-jo-le-parquet-de-paris-ouvre-une-enquete-apres-un-signalement-de-publications-racistes-visant-la-chanteuse_6222236_3246.html

[67] FranceInfo. (2023, 13 janvier). La chanteuse Hoshi victime de cyberharcèlement homophobe : plusieurs suspects mineurs identifiés en plus de la personne renvoyée en procès. FranceInfo. https://www.franceinfo.fr/societe/homophobie/info-franceinfo-la-chanteuse-hoshi-victime-de-cyberharcelement-homophobe-plusieurs-suspects-mineurs-identifies-en-plus-de-la-personne-renvoyee-en-proces_5600837.html

[68] Forgar, S. (2024, 30 novembre). «Tarée», «morue», «journalope» : quand Salomé Saqué dénonce son cyberharcèlement. Madame Figaro. https://madame.lefigaro.fr/societe/actu/taree-morue-journalope-quand-salome-saque-denonce-son-cyberharcelement-20241130

[69] Mariani, M. (2024, 20 juillet). Manon Lanza, seule face au sexisme de la Gen Z. Radio France. https://www.radiofrance.fr/franceinter/podcasts/mentionne-e/mentionne-e-7697864

[70] Melty. (2025, 7 octobre). Baghera victime de cyber harcèlement pendant le GP Explorer. Melty. https://www.youtube.com/shorts/xX2iW6eKyJc

[71] Konbini. (2025, 20 décembre). "Beurette de luxe", "Beurette de Science Po" : Sarah BOUCHAMAMA témoigne. Konbini. https://www.youtube.com/shorts/4bsFn2Fi_tY

[72] Interview Sam Zirah. (2025, 3 janvier). Ranelle BROWN a été menacée par des hommes. https://www.youtube.com/watch?v=jDPRubnGvUI

Victimes anonymes. Ces pratiques peuvent aussi toucher des internautes qui n'avaient pas de popularité particulière en ligne ou hors ligne avant de subir une vague de cyberharcèlement. À titre d'exemple, une participante à la vidéo du créateur de contenu Squeezie en date du 17 avril 2023 intitulée « Ils nous ont insulté en ligne, on les confronte IRL (ft Gotaga & Kameto) » a subi une vague de cyberharcèlement lancée par plusieurs internautes au cours de laquelle elle a reçu des messages insultants ciblant sa prise de parole.

Intimider pour réduire au silence. Les espaces numériques sont devenus des lieux au sein desquels les insultes sexistes et les attaques misogynes, l'intimidation des minorités et le dénigrement ciblé sont minimisés voire encouragés. Les normes de genre et les rapports de pouvoir sont particulièrement renforcés en ligne, d'une part du fait des dynamiques de contrôle et de surveillance permises par la commission continue de violences genrées, mais aussi grâce à la censure fréquente des contenus féministes et LGBTQIA+. En imposant ce qui est considéré comme acceptable ou non pour certains groupes, en réprimant leurs comportements et en les rendant invisibles dans les espaces numériques, ces pratiques contribuent à renforcer des inégalités déjà profondément ancrées dans le monde réel.

C - Des tendances virales vectrices de stéréotypes

Concept et diffusion des *trends*. Au climat d'intimidation et d'humiliation existant dans certaines sphères sociales et culturelles en ligne, s'ajoute l'existence de *trends* – ces "tendances numériques" qui rendent virales la production de contenus similaires ou portant sur un même sujet – manifestement sexistes partagées massivement par certains utilisateurs et agissant dès lors comme « une arme de construction massive des stéréotypes de genre, en les relayant et les amplifiant dès le plus jeune âge »[73]. Ces tendances émergent notamment des plateformes de partage de vidéos (TikTok, Instagram Reels, Youtube Shorts, ...) et mettent en avant des contenus profondément stéréotypés, ancrant petit à petit des préjugés misogynes voire masculinistes dans l'esprit des jeunes utilisateurs. À cet égard, TikTok doit faire l'objet d'une particulière attention dans la mesure où il a été identifié comme le réseau social de prédilection de la génération Alpha[74].

84 %

En 2024, 84 % des Français·es ayant entre 12 et 17 ans consultent quotidiennement leurs comptes de réseaux sociaux ou de plateformes vidéo[75].

[73] Beaune, C. (mai 2025). Stéréotypes femmes-hommes : un retour en arrière préoccupant chez les jeunes, un combat à amplifier ». In De Montaignac, M. Jolly, C. & Furic, P. *Lutter contre les stéréotypes filles-garçons. Quel bilan de la décennie. quelles priorités d'ici 2030 ?* [Edito].
[74] Qustodio. (2024, 19 août). *Apps through the ages: A Qustodio study on kids' tech use in the USA*. Qustodio.
[75] De Montaignac, M., Jolly, C., & Furic, P. (2025, mai). *Lutter contre les stéréotypes filles-garçons. Quel bilan de la décennie, quelles priorités d'ici 2030 ?*

1 – Le *bodycount*, un outil de hiérarchisation et de contrôle du corps féminin

Définition et viralité. La tendance dite du *bodycount* connaît une large popularité auprès des jeunes internautes. Mobilisée dans le cadre de microtrottoirs, les contenus vidéo sont abondamment likés, commentés et republiés par les internautes. *Bodycount* signifie littéralement « décompte de corps » en anglais. À l'origine utilisée pour désigner le nombre de victimes lors d'un accident ou d'une catastrophe naturelle, l'expression a été détournée par les influenceurs. Aujourd'hui, lorsqu'un·e jeune demande à un·e autre son *bodycount*, cela signifie qu'iel lui demande de chiffrer la totalité de ses partenaires sexuels. Ce détournement sémantique lui-même est révélateur : il assimile les partenaires sexuels à des « corps » comptabilisés, objectifiant ainsi les relations intimes et les réduisant à une logique comptable.

Double standard sexiste. À première vue, cette tendance, bien que profondément intrusive dans l'intimité des personnes interrogées, pourrait sembler relativement anodine. Pour autant, l'analyse des contenus portant le hashtag bodycount sur la plateforme TikTok révèle rapidement son caractère profondément sexiste et misogyne. Quelques clics suffisent à constater un double standard systématique : les femmes ayant un *bodycount* jugé élevé sont dénigrées et insultées ;

- « Tous les jeunes d'aujourd'hui, sachez que vous allez marier des te-pu quand vous serez plus grands. Je vous plains »[76],
- « Je m'éloigne un peu, je veux pas choper une MST »[77].

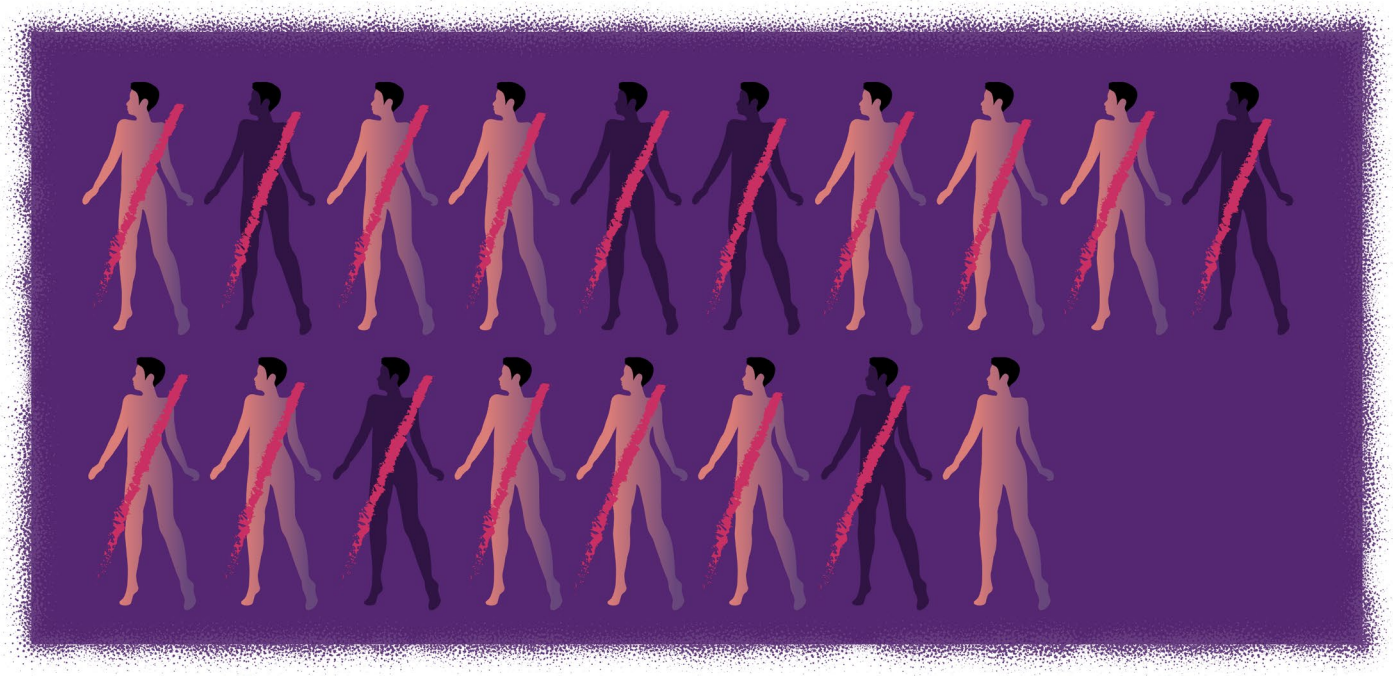
Les hommes sont quant à eux félicités voire glorifiés pour le même comportement. Ce double standard reproduit une norme patriarcale ancienne selon laquelle la sexualité masculine constitue un signe de virilité valorisé tandis que la sexualité féminine doit rester contenue sous peine de discrédit social.

Hiérarchisation des femmes. De nombreux dérivés tout aussi préoccupants de cette tendance circulent sur les réseaux sociaux. Ainsi, certains utilisateurs vont mobiliser le concept du *bodycount* afin de mesurer la « valeur » d'une femme sur le « marché de la séduction » et ainsi pousser l'audience masculine à opérer des distinctions hiérarchiques entre les femmes. Le créateur de contenus Alex Nwa a par exemple proposé la catégorisation suivante[78] :

NOMBRE DE PARTENAIRES SEXUELS	CATÉGORIE
1 à 3	**Zone d'or : la femme a pratiqué sans être une « pute ».**
6 à 9	**La femme peut encore se « repentir », le nombre de partenaires sexuels serait dû à des erreurs causées par des traumas, des peines de cœur, etc.**
10 à 20	**La femme est une pute et cela est sûrement causé par des traumas issus de sa relation avec son père.**

Cette grille de lecture pathologise systématiquement la sexualité féminine – en lui attribuant des causes liées à la survenance de traumas psychologiques – tout en naturalisant la domination masculine et le contrôle du corps des femmes.

[76] @kheyos_plus. (s. d.). *Vidéo sur le « body count »* [Vidéo TikTok]. TikTok. https://www.tiktok.com/@kheyos_plus/video/7560034847511760150
[77] @hugo_tournier. (s. d.). *Vidéo sur le « body count »* [Vidéo TikTok]. TikTok. https://www.tiktok.com/@hugo_tournier/video/7485020322819738902
[78] Fourneau, L. (10 août 2023). Qu'est-ce que le body count, une tendance sur TikTok au sexisme décomplexé. 20 minutes.



Fondements pseudo-scientifiques. Le *bodycount* est également utilisé comme marqueur permettant d'évaluer la capacité d'une femme à être fidèle, stable dans une relation et « mariable ». Certaines de ces théories se parent d'un vernis scientifique et sont parfois relayées par des femmes elles-mêmes, illustrant l'intériorisation de ces normes. Thaïs d'Escufon, ancienne porte-parole du mouvement d'extrême droite Génération identitaire, affirme ainsi sur les réseaux sociaux que les femmes libéreraient de l'ocytocine – « hormone de l'amour » – lors de relations sexuelles, ce qui ne serait pas le cas des hommes[79]. Selon elle, la production d'ocytocine serait altérée à chaque rapport sexuel, rendant les femmes ayant eu de nombreux partenaires moins aptes à s'attacher et plus susceptibles de divorcer. Elle conseille dès lors aux hommes de se renseigner sur le *bodycount* d'une femme car il serait un indicateur pertinent pour estimer stabilité relationnelle future. Ce type de discours, qui mobilise abusivement des références biologiques pour naturaliser des normes sociales, s'inscrit dans une longue tradition de pseudo-sciences mises au service de l'idéologie patriarcale. Ces contenus sont régulièrement utilisés par leur autrice comme vecteur de monétisation et pour justifier des programmes politiques sécuritaires ou racistes, rejoignant ainsi les pratiques de personnalités telles qu'Andrew Anglin, Paul Elam ou Nick Fuentes[80].

Dimension hétéronormative. Au-delà de son caractère profondément misogyne, cette tendance revêt également une dimension homophobe structurante. De nombreux contenus affirment qu'une femme ayant eu des relations sexuelles uniquement avec des femmes aurait un *bodycount* égal à zéro[81]. En d'autres termes, pour qu'une relation sexuelle « compte », il faudrait nécessairement qu'il y ait eu pénétration avec un pénis dans le cadre d'une relation hétérosexuelle. Cette assertion nie l'existence même de la sexualité lesbienne et bisexuelle féminine, tout en révélant une conception phallocentrée de la sexualité où seul le rapport hétérosexuel pénétratif constituerait une relation sexuelle valide et légitime.

---

[79] D'Escufon, T. (s. d.). *Vidéo publiée sur TikTok* [Vidéo TikTok]. TikTok. https://www.tiktok.com/@thaisdescufon/video/7232320892255096090

[80] Voir supra, Partie 2, I, B, 3.

[81] @camk798. (s. d.). *Critique de la trend « bodycount »* [Vidéo TikTok]. TikTok. https://www.tiktok.com/@camk798/video/7388167566260194593

2 - Les “tanas”

Émergence et définitions. Le concept de « tana » a émergé sur les réseaux sociaux, en particulier TikTok, et foisonne désormais dans les commentaires de vidéos et photos postées par des femmes. Cette insulte possède plusieurs acceptions, allant de la femme qui, du fait de son attitude en ligne jugée excentrique, provocatrice ou très expressive, « se fait trop remarquer », à un pur synonyme du terme « pute ». Le fait que des jeunes femmes soient moquées, insultées ou attaquées en ligne en raison de leur simple apparence, de leur attitude ou de leur manière de s’exprimer constitue une manifestation explicite du sexisme ordinaire et de la police sociale exercée à l’égard des femmes dans l’espace public numérique.

Stratégies de réappropriation. Face à cette violence linguistique, un contre-mouvement s’est massivement réapproprié le terme au sein des espaces numériques[82], parvenant à en inverser partiellement la charge négative et à transformer un terme insultant en outil d’affirmation de soi et de lutte contre le sexisme en ligne. Cette réappropriation illustre les stratégies de résistance et de subversion déployées par les femmes et les minorités pour retourner les instruments de leur oppression, selon une logique comparable à celle observée historiquement avec la réappropriation du terme « queer » par les communautés LGBTQIA+. Toutefois, cette stratégie de réappropriation reste débattue au sein des mouvements féministes, certain·es y voyant un risque de banalisation et de dilution de la charge violente initiale du terme.

3 - Les comptes fisha

Concept. Les dynamiques misogynes en ligne prennent souvent une forme organisée, rassemblant plusieurs personnes poursuivant des desseins communs. À l’image des groupes masculinistes qui organisent des raids de cyberharcèlement à l’encontre de femmes, les comptes dits fisha suivent une logique similaire : ils centralisent, diffusent et relaient des contenus visant à humilier, intimider ou harceler des jeunes en lien avec un lieu particulier - un établissement scolaire, une ville, un département, etc. Ils prennent souvent la forme d’un compte dédié sur un réseau social (Instagram, Snapchat) ou d’un canal de discussion (Telegram).

Fonctionnement. Ces comptes fisha constituent des espaces de violences coordonnées dédiés au partage de photos, de vidéos et d’informations personnelles concernant une ou plusieurs personnes, dans l’écrasante majorité des cas sans leur consentement. Ces contenus s’accompagnent de commentaires insultants, sexistes ou discriminatoires, alimentant une dynamique de haine collective parmi les membres du groupe. Les « fisheurs » s’arrogent une position de juges détenant le pouvoir symbolique d’évaluer la « valeur » des victimes, de les culpabiliser et de les réprimer pour des propos ou comportements jugés inadaptés. Cette pratique s’apparente à une forme de tribunal populaire numérique où s’exercent simultanément surveillance, jugement et sanction.

Actions de #StopFisha. En 2020, le hashtag #StopFisha[83] a dénoncé la multiplication de comptes et canaux *fisha* ciblant principalement des jeunes filles et des minorités sur diverses plateformes - Telegram, Snapchat et Instagram notamment, mettant en lumière le harcèlement sexiste, la divulgation d’informations privées (ou *doxing*) et la diffusion non consentie de photos ou vidéos représentant les victimes.

---

[82] Radio France (2025, 13 septembre). Tanaland : nouvelle expression du féminisme 2.0. France Inter. https://www.radiofrance.fr/franceinter/podcasts/zoom-zoom-zen/zoom-zoom-zen-du-lundi-15-septembre-2025-1141794

[83] Nasi, M. (2022, 24 mai). *Les comptes « fisha » sur les réseaux sociaux, nouvelle plaie du cybersexisme. Le Monde.* https://www.lemonde.fr/campus/article/2022/05/24/notre-corps-est-massivement-partage-les-comptes-fisha-sur-les-reseaux-sociaux-nouvelle-plaie-du-cybersexisme_6127391_4401467.html

4 - Usages d'emojis à des fins de harcèlement

Fonctions initiales et détournements. Les emojis constituent aujourd'hui un langage universel permettant d'exprimer des sentiments et des émotions de manière visuelle et immédiate. Cette pratique, partagée par l'ensemble des internautes quelle que soit leur localisation géographique, participe de la communication numérique contemporaine. Toutefois, cette pratique a également fait l'objet de détournements : certains emojis, dévoyés de leur sens initial, servent désormais à véhiculer des messages d'intimidation, de menace ou de violence.

Contournement de la modération. Cette substitution des mots aux images crée un véritable langage codé permettant aux auteurs de propos violents de contourner plus facilement les outils de modération automatisée – chose qui serait plus difficile si les mots étaient écrits en toutes lettres. Ce phénomène a notamment été documenté par la campagne de sensibilisation d'Allianz[84], laquelle explique comment des symboles apparemment anodins peuvent être exploités pour propager la violence, le harcèlement et le *slut-shaming* en ligne. Cette stratégie révèle les limites intrinsèques de la modération automatisée fondée sur la détection de mots-clés et témoigne de la capacité d'adaptation des auteurs de violences face aux dispositifs de régulation mis en place par les plateformes.

Exemples. Sans prétendre à l'exhaustivité, l'on peut ici faire état d'usages particulièrement populaires au sein des jeunes générations de certains émojis pour illustrer le sens qui leur est désormais dévolu.

Emoji	Signification contemporaine en ligne
	L'expression "Cheese Pizza" a les mêmes initiales que child *porn* (CP). Cet emoji est un indicateur destinés aux pédocriminels afin de leur indiquer la présence de contenus d'exploitation sexuelle de mineurs.
	Cet emoji sert à remplacer le mot viol (VIOLet).
	Cet emoji fait référence à la « pilule rouge » du film Matrix et est réutilisé par les adeptes des mouvances masculinistes pour signifier qu'il est nécessaire de « se réveiller » et de prendre conscience que le monde subirait une crise de la masculinité du fait des femmes particulièrement, et plus généralement de toute personne n'adhérant pas aux normes sociales genrées et hétéronormatives.

[84] Allianz. (2025, mai). *Nos actions contre le cyberharcèlement*. https://www.allianz.fr/qui-est-allianz/allianz-s-engage/dans-la-societe/nos-actions-contre-le-cyberharcelement.html

Emoji	Signification contemporaine en ligne
	Cet emoji s'oppose au précédent et constitue la « pilule bleue » de Matrix. Il représente les personnes qui n'auraient pas eu cette prise de conscience, en d'autres termes toute personne n'adhérant pas aux idéologies masculinistes.
	Cet emoji illustre la théorie dite des « 80/20 » : 80 % des femmes seraient attirées par uniquement 20 % des hommes. Dès lors, un homme s'estimant lésé dans le cadre de sa vie sexuelle ou romantique serait légitime à piéger des femmes afin d'obtenir toute forme d'avantage. Cette rhétorique légitime ainsi la violence et entretient la culture du viol.
	Cet emoji permet de s'identifier, ou d'identifier quelqu'un, comme étant incel.
	Cet emoji, lorsqu'il est associé à une femme ou à ses propos, indique que l'on est en train de se moquer d'elle et de la qualifier de stupide. Cette représentation est issue d'une vidéo de Team Fortress 2.[85]
	Cet emoji a été utilisé pour désigner « les pires gauchos de France » au cours de vagues de cyberharcèlement survenues en 2021.[86]

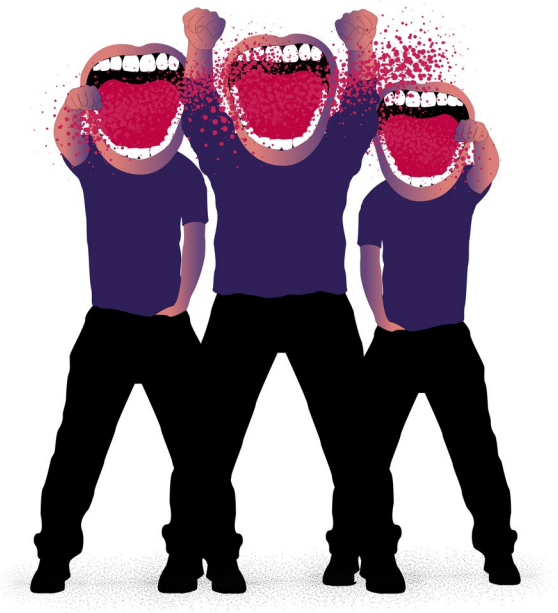
[85] youtube.com/watch?v=OXzMdhtzhbc&feature=youtu.be
[86] Antidote Magazine. (2021, 20 avril). Pourquoi les masculinistes inondent certains comptes Instagram avec des émojis médaille ? *Antidote Magazine*.

III. CADRE NORMATIF

Un arsenal en mouvement. Les cyberviolences sexistes et sexuelles posent au droit un défi redoutable : celui de saisir des comportements qui évoluent plus vite que les textes qui les répriment, qui traversent les frontières sans s'y arrêter, et dont la nature même — immatérielle, diffuse et parfois anonyme — éprouve les catégories juridiques traditionnelles. Appréhender ce phénomène suppose d'emblée de clarifier ce qu'il recouvre, d'identifier les instruments mobilisables à chaque échelon normatif et d'évaluer la distance qui sépare les dispositifs existants de leur effectivité réelle. Car si le droit s'est progressivement adapté — en France comme en Europe, cette adaptation demeure partielle, fragmentée et souvent en retard sur des pratiques violentes que la généralisation des usages numériques rend toujours plus accessibles à leurs auteurs et toujours plus difficiles à fuir pour leurs victimes.

Réalités plurielles. Les cyberviolences sexistes et sexuelles ne se laissent pas aisément circonscrire : elles recouvrent un spectre large de comportements – insultes sexistes, diffusion non consentie de contenus intimes, deepfakes sexuels, menaces de viol, sextorsion, grooming, proxénétisme numérique*, doxing – dont le point commun est de porter atteinte à la dignité, à la sécurité et à la vie privée des personnes qui en sont victimes. Si nul n'est à l'abri de ces violences, les données disponibles attestent qu'elles ciblent de manière structurellement disproportionnée les femmes et les minorités de genre et d'orientation sexuelle. Cette réalité n'est pas le fruit du hasard : elle s'enracine dans des rapports de pouvoir préexistants que l'environnement numérique ne crée pas, mais amplifie, prolonge et rend plus difficiles à combattre. Les victimes y sont exposées à des attaques souvent répétées, parfois collectives, fréquemment anonymes, dont les conséquences – psychologiques, sociales, professionnelles, sexuelles – peuvent se révéler dévastatrices et durables.

Réponse juridique en construction. Face à cette réalité, le droit a progressivement évolué. En France, si la Loi pour la confiance dans l'économie numérique de 2004 posait les premières fondations d'une adaptation du cadre juridique à l'ère numérique, il a fallu attendre le milieu des années 2010 pour que le législateur se penche véritablement sur les cyberviolences en tant que telles – en créant des infractions spécifiques, en étendant le champ d'application d'incriminations préexistantes et en reconnaissant l'usage des outils numériques comme circonstance aggravante. Au niveau européen, cette dynamique s'est traduite par l'émergence d'un corpus normatif ambitieux, articulant droits fondamentaux, droit du numérique et instruments de coopération internationale, dont la directive de 2024 sur la lutte contre les violences faites aux femmes constitue l'expression la plus récente. Pour autant, la multiplication des textes applicables n'a pas nécessairement produit la lisibilité et l'efficacité attendues : le cadre juridique demeure fragmenté, ses dispositions dispersées entre plusieurs codes et logiques d'incrimination, et ses défauts d'application persistent à chaque stade de la chaîne de protection. Le temps de la justice reste un obstacle structurel face à l'instantanéité des communications numériques et à la viralité des contenus illicites.



Périmètre de l'analyse. C'est dans ce contexte que s'inscrit la cartographie qui suit. Elle entend d'abord rendre compte du cadre juridique applicable – en droit français, où les violences sont appréhendées selon la nature du discours, de l'image ou du mécanisme d'emprise qu'elles mobilisent, mais aussi en droit européen, qui articule protection des droits fondamentaux et régulation sectorielle du numérique via des instruments tels que le DSA, le RGPD ou l'AI Act, et en droit international, à travers les Conventions de Budapest et d'Istanbul. Elle examine ensuite la manière dont les plateformes numériques – premières gardiennes des contenus en circulation – traduisent ces obligations dans leurs règles d'utilisation et, surtout, dans leurs pratiques concrètes de modération : c'est en effet à ce niveau opérationnel que se joue, en dernière instance, la réalité de la protection offerte aux victimes.

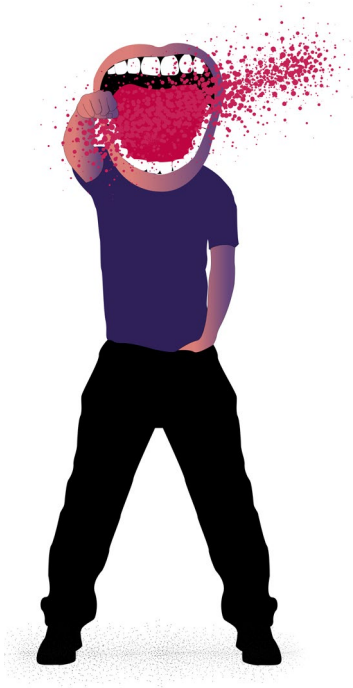
1. Le cadre juridique

A - Perspective française

1 - La répression des cyberviolences sexistes et sexuelles

Fondements et évolutions. Dès 2004, la Loi pour la confiance dans l'économie numérique (LCEN) pose certes les fondements d'une nécessaire adaptation du droit français à la révolution numérique, mais il faudra attendre le milieu des années 2010 pour que le législateur se penche véritablement sur les difficultés liées à ces nouveaux usages en créant des infractions s'inscrivant spécifiquement dans ce cadre. Aussi, le champ d'application de certaines infractions préexistantes est étendu ou modifié afin de couvrir la dimension technologique des violences qu'elles punissent. L'utilisation de moyens de communication numériques est ainsi explicitement reconnue comme une modalité de commission ou comme une circonstance aggravante de plusieurs incriminations – harcèlements, atteintes à la vie privée, violences conjugales, etc.

Lisibilité du droit. Face à la multiplication des nouvelles infractions mobilisables pour appréhender les cyberviolences sexistes et sexuelles et aux innombrables modifications opérées sur le droit existant, le cadre juridique en devient fragmenté, ses dispositions dispersées en différents codes et répondant à plusieurs logiques d'incriminations. Afin d'en faciliter la compréhension et l'appropriation, le présent rapport propose une lecture systématisée de ce corpus, en regroupant ces infractions au sein de trois grands ensembles, construits à partir de la nature et des modalités concrètes de la violence et de ses effets sur les victimes. Cette approche permet d'identifier et de distinguer les violences fondées sur la parole ou le discours, celles liées à l'imagerie intime et sexuelle et enfin celles reposant sur des mécaniques interpersonnelles de domination et d'exploitation.



Les violences fondées sur la parole et le discours

Délimitation du sujet. Les violences sexistes et sexuelles exercées par le biais du langage et des messages en ligne recouvrent un ensemble d'infractions relevant de régimes juridiques distincts. Certaines sont appréhendées par le droit de la presse, qui encadre historiquement les atteintes portées par les propos publics, telles que l'injure, la diffamation ou l'incitation à la haine. D'autres relèvent du droit pénal commun et sanctionnent des comportements attentatoires à la dignité, à la sécurité ou à la santé psychique des personnes, comme le cyberharcèlement, les menaces ou l'outrage sexiste*. Cette distinction structure l'analyse des infractions fondées sur le discours, tout en révélant la singularité et la complémentarité des outils juridiques mobilisables face aux violences commises dans l'espace numérique.

Injures à caractère sexiste

Dimension sexiste d'une incrimination préexistante. L'infraction d'injure est une création ancienne de la loi du 29 juillet 1881[1], qui protège la réputation et la dignité contre les expressions outrageantes ou méprisantes ne comportant pas l'imputation d'un fait précis. La loi n°2004-1486 du 30 décembre 2004[2] a introduit de nouvelles circonstances aggravantes en cas d'injure ou de diffamation à caractère discriminatoire, élargissant le champ des discriminations réprimées, notamment à raison du sexe, de l'orientation sexuelle, de l'identité de genre ou du handicap. Cet ajout permet ici d'appréhender le volet sexiste ou misogyne de termes injurieux, qu'ils soient verbaux, écrits, visuels ou symboliques.

Définition légale. Sur le plan juridique, l'injure est définie par l'article 29 de la loi de 1881 et suppose un propos outrageant - oral, écrit ou visuel - ayant un caractère public et visant une personne identifiable ou le groupe auquel elle appartient. Lorsqu'elle est commise sur les réseaux sociaux, la publicité est caractérisée dès lors que les contenus sont accessibles à un public indéterminé. Lorsque l'injure revêt un caractère discriminatoire, qu'elle ne vise pas seulement la personne prise pour cible, mais tend à porter atteinte à l'ensemble du groupe auquel elle est rattachée, elle est plus sévèrement réprimée.

→ L'auteur d'une injure sexiste encourt un an d'emprisonnement et 45 000 euros d'amende.

Violences numériques incriminées. Cette incrimination permet donc de sanctionner les propos visant à rabaisser une personne sur la simple base de son sexe, de son identité de genre ou de son orientation sexuelle – réels ou supposés. Dans le contexte numérique, elle constitue un outil de protection face aux phénomènes de *slut-shaming*[3] ou de *victim-blaming**[4], formes contemporaines d'humiliation publique et d'atteinte à la réputation.

Diffamation à caractère sexiste

Définition légale. La diffamation, contrairement à l'injure, suppose l'imputation d'un fait précis portant atteinte à l'honneur ou à la considération d'une personne identifiable, que ce soit de manière directe ou implicite, et ce, indépendamment du ton employé[5]. La dimension sexiste de l'infraction, elle aussi introduite à l'occasionnde la loi du 30 décembre 2004, s'applique lorsque l'allégation vise une personne à raison de son sexe, de son orientation sexuelle, de son identité de genre ou de son handicap, conformément à l'article 32 alinéa 3 de la même loi.

[1] Loi du 29 juillet 1881 sur la liberté de la presse.
[2] Loi n° 2004-1486 du 30 décembre 2004 portant création de la Haute Autorité de lutte contre les discriminations et pour l'égalité (HALDE).
[3] Comportement consistant à critiquer, rabaisser ou stigmatiser une personne – le plus souvent une femme – en raison de son apparence, de ses vêtements ou de son comportement perçu comme sexuellement provocant ou « immoral ».
[4] Tenir une victime (d'agression, de violence, notamment sexuelle) pour partiellement ou totalement responsable du préjudice qu'elle a subi.
[5] Article 29 de la loi n°1881-29 du 29 juillet 1881 sur la liberté de la presse, *op.cit.*

Circonstance aggravante. Comme pour l'injure, la diffamation est une infraction considérée par la loi comme étant plus grave lorsqu'elle revêt un caractère sexiste ou LGBTphobe. En d'autres termes, la peine encourue par l'auteur est plus lourde. L'objectif de cette aggravation est de réprimer la propagation publique de fausses informations portant atteinte à la réputation dès lors que cette atteinte repose sur un motif discriminatoire, notamment sexiste.

→L'auteur de diffamation sexiste ou à caractère sexuel encourt un an d'emprisonnement et 45 000 euros d'amende.

Incitation à la haine sexiste*

La légitimation de la restriction de la liberté d'expression. Ce dispositif s'inscrit dans une logique de prévention des discriminations et vise à encadrer l'exercice de la liberté d'expression dans la mesure où celui-ci peut porter atteinte à la dignité et à l'égalité entre les personnes. La jurisprudence européenne reconnaît la légitimité de telles restrictions à la liberté d'expression au regard de l'article 10 de la Convention européenne des droits de l'homme[6]. Les juges européens considèrent en effet que l'on peut estimer nécessaire, au sein de sociétés démocratiques, de sanctionner, voire de prévenir, toutes les formes d'expression qui propagent, incitent, promeuvent ou justifient la haine fondée sur l'intolérance. Dans d'autres décisions, la Cour rappelle qu'un discours de haine ne requiert pas nécessairement un appel explicite à la violence : la simple propagation de propos discriminatoires peut suffire à justifier une sanction dès lors qu'elle porte atteinte aux droits et libertés d'autrui[7].

Outil contre le sexisme en ligne. L'infraction d'incitation à la haine sexiste constitue ainsi un instrument juridique central pour prévenir la diffusion de propos misogynes, sexistes, LGBTQI+phobes ou masculinistes dans l'espace numérique et garantir un environnement d'expression conforme aux principes démocratiques et de respect de l'égalité de genre.

Liberté d'expression et propos sexistes dans l'art

La jurisprudence française tend à accorder une protection renforcée à la liberté d'expression artistique lorsqu'elle est confrontée à des propos sexistes ou violents intégrés à une œuvre de création. Ainsi, dans une affaire visant le rappeur Orelsan, l'auteur avait été condamné en première instance pour certaines paroles, avant d'être relaxé en appel (CA Versailles, 18 févr. 2016, n° 15/02687), les juges considérant que les propos incriminés relevaient de la fiction artistique et ne traduisaient pas une volonté d'inciter à la haine ou à la violence envers les femmes. Cette tendance jurisprudentielle illustre la difficulté d'articuler la répression des discours sexistes avec la protection de la liberté d'expression, et contribue à expliquer la rareté des condamnations définitives en matière d'incitation à la haine ou de propos sexistes lorsqu'ils s'inscrivent dans un cadre artistique.

[6] Cour européenne des droits de l'homme. (2006, 6 octobre). *Erbakan c. Turquie* (n° 59405/00).
[7] Cour européenne des droits de l'homme. (2009, 16 juillet). *Féret c. Belgique* (n° 15615/07).

Cyberharcèlement à caractère sexuel

Définition légale. Le harcèlement sexuel est défini à l'article 222-33 du Code pénal comme le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste portant atteinte à sa dignité ou créant une situation intimidante, hostile ou offensante. Depuis la loi du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes[8], le texte prévoit expressément que le harcèlement peut être constitué même lorsque les propos sont diffusés par plusieurs personnes successivement ou de manière concertée, reconnaissant ainsi juridiquement les phénomènes collectifs caractéristiques du harcèlement en meute.

Circonstance aggravante. La loi de 2018 a également introduit l'usage du numérique en tant que circonstance aggravante de l'infraction. En d'autres termes, lorsque les faits sont commis via un service de communication au public en ligne ou au moyen d'un support numérique, la peine est aggravée.

→ L'auteur de cyberharcèlement sexuel encourt deux ans d'emprisonnement et 30 000 euros d'amende.

Considération de la dimension cyber. Cette modernisation du droit reflète la reconnaissance par le législateur que la diffusion instantanée, massive et durable des contenus amplifie le préjudice psychologique, l'isolement et l'atteinte à la dignité, et que le numérique peut transformer des interactions éparses en un effet cumulatif et dévastateur pour la victime. Elle témoigne de la volonté de garantir la protection de l'intégrité psychique dans l'espace numérique et d'englober l'ensemble des violences contemporaines.

T. corr. Paris, 10 nov. 2025

Condamnation de neuf hommes pour le cyberharcèlement de Typhaine D. Le tribunal souligne que même un seul message, isolé, devient un acte de harcèlement dés lors qu'il s'inscrit dans une dynamique collective déjà en cours.

Menaces de mort, de viol ou d'agression

Définition légale. Les articles 222-17 et suivants du Code pénal incriminent les menaces de commettre un crime ou un délit contre les personnes. La menace est punie à deux conditions :

- lorsqu'elle est proférée par écrit ou matérialisée par une image, un objet, **ou**
- lorsqu'elle est répétée

La loi différencie la menace assortie d'une condition à remplir par la victime ainsi que la menace de mort - quelle que soit sa forme - en aggravant les peines encourues par l'auteur.

[8] Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes.

Matérialisation de la menace numérique. Dans le contexte numérique, les menaces diffusées via un service de communication au public en ligne sont considérées comme matérialisées du fait de leur transmission écrite ou visuelle. Elles constituent un instrument courant d'intimidation, notamment à l'encontre de femmes journalistes, militantes ou personnalités publiques, la menace de viol ou de mort y jouant un rôle dissuasif marqué[9].

→ L'auteur d'une menace proférée au sein de l'espace numérique encourt ainsi au minimum 6 mois d'emprisonnement et 7 500 euros d'amende.

Menace conjugale. La loi du 9 juillet 2010 relative aux violences au sein du couple[10] a étendu la répression aux menaces et violences psychologiques commises dans le cadre conjugal en renforçant l'arsenal répressif en la matière. Par ce biais, la menace proférée par le conjoint, le concubin ou le partenaire lié par un PACS à la victime, est punie plus sévèrement, quelle qu'en soit sa forme.

Outrage sexiste

Évolution. L'outrage sexiste - qu'il serait plus exact de qualifier d'outrage sexiste ou sexuel - a été introduit en 2018[11] pour renforcer la lutte contre les violences sexuelles et sexistes. Initialement prévu à l'article 621-1 du Code pénal, il constituait une contravention sanctionnant les propos ou comportements à connotation sexuelle ou sexiste imposés à une personne et portant atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, ou créant une situation intimidante, hostile ou offensante. L'article 621-1 a été abrogé en 2023[12].

Outrage sexiste simple. Aujourd'hui, deux textes coexistent. L'article R.625-8-3 du Code pénal, issu d'un décret du 30 mars 2023, réprime l'outrage sexiste simple sous la forme d'une contravention de cinquième classe, punie d'une amende de 1 500 euros.

Outrage sexiste aggravé. L'article 222-33-1-1 du Code pénal, créé en 2023[13], érige en délit l'outrage sexiste lorsqu'il est commis dans l'une des circonstances aggravantes prévues par le texte, notamment lorsque la victime est mineure ou vulnérable ou lorsque les faits sont commis en raison de l'orientation sexuelle ou de l'identité de genre.

→ L'auteur d'un outrage sexiste aggravé encourt 3 750 euros d'amende.

Champ d'application. Cette incrimination permet de sanctionner des faits isolés, sans nécessité de répétition ni de diffusion publique, comblant ainsi un angle mort du droit pénal entre l'injure et le harcèlement sexuel. Elle vise en particulier les manifestations de sexisme ordinaire et les comportements d'intimidation de faible seuil et réaffirme que le respect de la dignité et du consentement s'impose dans tous les espaces sociaux.

---

[9] D'après une enquête mondiale menée par l'UNESCO et l'International Center for Journalists auprès de plus de 1 200 journalistes, 73 % des femmes journalistes interrogées ont déclaré avoir été confrontées à des violences en ligne liées à leur activité professionnelle, comprenant notamment des menaces de violence physique ou sexuelle, du harcèlement et des attaques de sécurité numérique. Posetti, J., & Shabbir, N. (Éds.). (2022). *The chilling: A global study of online violence against women journalists. International Center for Journalists & UNESCO*. https://www.icfj.org/our-work/chilling-global-study-online-violence-against-women-journalists

[10] Loi n° 2010-769 du 9 juillet 2010 relative aux violences faites spécifiquement aux femmes, aux violences au sein des couples et aux incidences de ces dernières sur les enfants.

[11] Loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, op.cit.

[12] Loi n°2023-22 du 24 janvier 2023 visant à mieux lutter contre les violences intrafamiliales et sexistes.

[13] Ibid.

STOP à l'utilisation de l'expression "revenge porn"

Les pratiques de diffusions non consenties de contenus intimes en ligne ont fait l'objet d'une importante médiatisation sous l'appellation revenge porn. Cette terminologie devrait toutefois être abandonnée dans la mesure où l'usage de cette expression invisibilise la diversité des contextes de commission de ces violences et qu'elle participe aussi largement à la culpabilisation des victimes.

› L'emploi du terme ***revenge*** laisse entendre que les images sont publiées à des fins de vengeance, mais en réalité, les motivations de l'auteur peuvent varier. D'autres mobiles peuvent conduire à de telles diffusions : menacer, extorquer ou faire taire la victime ciblée sur la base de la détention de ces images. Les contenus à caractère sexuel détenus peuvent également être diffusés à des tiers qui composent l'entourage proche ou lointain de l'agresseur – du groupe de camarades aux communautés en ligne. De plus, l'utilisation de ce terme est hautement culpabilisant pour la victime. Une vengeance intervenant en réponse à un acte préalable, parler de *revenge porn* revient donc à désigner la victime comme première responsable de la violence qu'elle subit – sous-entendant que si elle avait correctement agi, alors l'auteur n'aurait pas publié ses photos ou vidéos.

› L'emploi du terme ***porn*** efface enfin la distinction entre les contenus sexuels produits dans un cadre intime et les contenus issus de l'industrie pornographique. Il ne s'agit pas ici de contenus sexuels diffusés avec l'accord des personnes en scène, mais bien d'une atteinte à leur vie privée et à leur dignité. En outre, le terme *porn* ne différencie pas les contenus d'adultes de ceux qui impliquent des mineur·es et par conséquent son usage invisibilise les situations où ces actes d'exploitation sexuelle sont commis à l'encontre de mineur·es.

Un type de violence en plein essor

Origine et développement contemporain. La diffusion non consentie de contenus sexuels, communément appelée à tort revenge porn, est une violence sexuelle et sexiste de plus en plus fréquente. Facilitée par le développement des technologies telles que l'IA, cette forme de violence, reposant principalement sur l'humiliation via l'exposition forcée de l'imagerie intime, n'est pas nouvelle. L'essor de l'usage d'Internet et des réseaux sociaux, impliquant une facilité de circulation extrêmement rapide des informations, vient toutefois banalisé a donné son ampleur actuelle à cette forme de violence.

Diversité formelle. Si cette cyberviolence peut prendre la forme caricaturale de publication sur un réseau social d'une photo intime de son ex-petit·e ami·e suite à une rupture mal digérée, elle revêt toutefois des dimensions bien plus complexes dans de nombreux cas. Parfois utilisée à des fins politiques, comme dans le cas de l'affaire Griveaux[14], cette cyberviolence peut aussi prendre la forme d'une diffusion massive de contenus visant une ou plusieurs célébrités, comme par exemple lors de l'affaire Celebgate. En 2014, plus de 60 stars ont été victimes d'un piratage informatique[15] suivi de la diffusion de plus de 300 contenus (photos et vidéos) à caractère intime ou sexuel les représentant[16].

Industrialisation de la violence. Des procédés particuliers à la commission de cette violence ont même vu le jour. Le phénomène des comptes fisha en est un exemple[17] Ce phénomène n'est pas nouveau, il existait déjà sur d'anciens sites de blogging, tels que Skyblog[18], mais a pris une envergure nouvelle du fait de l'utilisation massive des réseaux sociaux et des messageries instantanées au cours des années 2010. Dans la même dynamique, des sites entièrement dédiés à la diffusion des contenus sexuels prolifèrent largement sur internet.

Contenus virtuels et IA. En outre, l'émergence de nouveaux outils permet désormais de semer le doute chez les internautes quant à la diffusion de contenus réels alors même que ceux-ci sont artificiellement modifiés ou générés de toute pièce : les deepfakes sexuels. En d'autres termes, cela consiste le plus souvent à faire un montage photo ou vidéo en apposant le visage de la victime sur le corps d'une autre personne nue ou impliquée dans un acte sexuel ou, à l'inverse, utiliser des outils dits de nudification pour altérer une photo anodine au départ mais qui sera sexualisée une fois modifiée. Ce procédé implique l'utilisation d'un outil d'intelligence artificielle, laquelle rend le photomontage suffisamment réaliste pour induire en erreur toute personne non avertie.

[14] Le Monde. (2023, 11 octobre). Affaire Griveaux : l'artiste russe Piotr Pavlenski condamné à une peine de six mois de prison ferme aménageable. *Le Monde*.
[15] Le Monde. (2014, 1er septembre). Des photos piratées de Jennifer Lawrence et plusieurs autres stars nues mises en ligne. *Le Monde*.
[16] Zeid, J. (2014, 1er septembre). Le Cloud à l'épreuve du #CelebGate. *France Info*.
[17] Voir le paragraphe sur les comptes Fisha, parmi les *trends* dangereuses.
[18] Nasi, M. (2022, 24 mai). Les comptes « fisha » sur les réseaux sociaux, nouvelle plaie du cybersexisme. *Le Monde*.

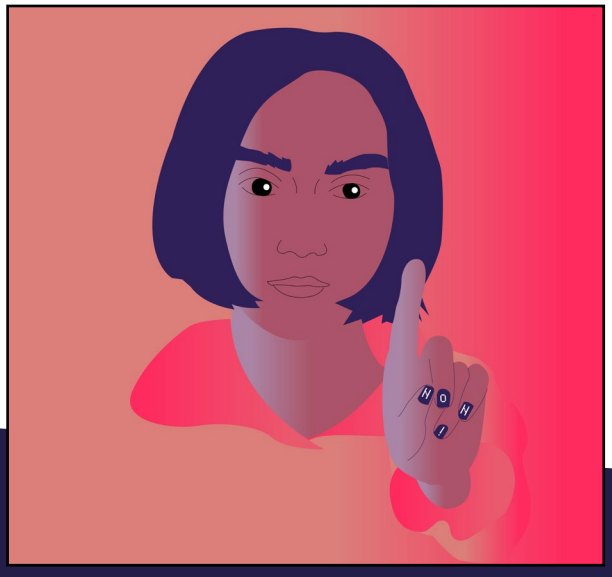
Un droit pénal français lacunaire jusqu'en 2016

Atteinte à la vie privée. La diffusion non consentie de contenus sexuels est une cyberviolence qui va de pair avec l'usage du numérique. Toutefois, le droit pénal français ne s'en est saisi que tardivement. En effet, avant 2016, l'unique fondement juridique permettant de réprimer le fait de diffuser le contenu sexuel d'autrui était l'atteinte à la vie privée, ce sur la base des articles 226-1 et 226-2 du Code pénal.

Définition légale. L'article 226-1 du Code pénal réprime les atteintes volontaires à la vie privée par captation, fixation, enregistrement ou transmission des paroles ou de l'image d'autrui, lorsque la victime se trouvait dans un lieu privé, ou a prononcé ces paroles à titre privé, et qu'elle n'y avait pas consentie. L'article 226-2 réprime quant à lui le fait de diffuser ces contenus au public. La loi considère à ce titre qu'il y a diffusion dès lors que l'auteur a transmis le contenu à une autre personne.

Angles morts. Si cette incrimination permettait de réprimer certains cas de diffusion non consentie de contenus sexuels, elle est loin d'envisager toutes les formes que cette violence peut prendre.

› En effet, concernant la diffusion d'une image, celle-ci doit avoir été prise dans un lieu privé. En d'autres termes, si la personne visible sur le contenu diffusé ne se trouvait pas dans un lieu privé au moment où la photo ou la vidéo a été prise, alors l'auteur de la diffusion ne pouvait pénalement pas être sanctionné[18]. Ainsi, une personne ayant filmé sous la jupe d'une personne dans la rue et diffusant ensuite la vidéo sur internet ne pouvait pas être poursuivie pénalement.

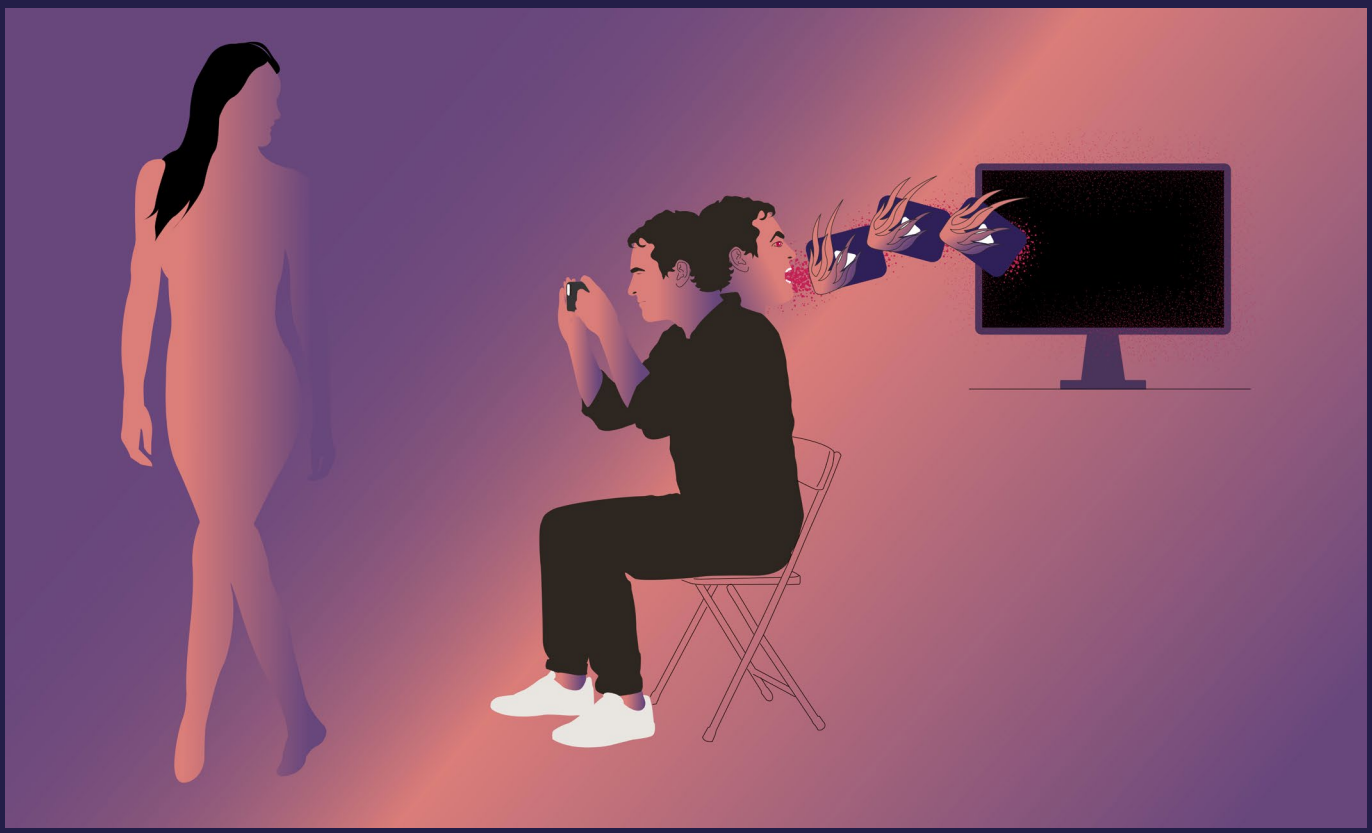


de l'infraction de l'article 226-1 est l'absence de consentement de la victime lors de la fixation de l'image ou captation des paroles[19]. Comme cela a déjà pu être évoqué, publier le *nude* de son ex-petit·e ami·e est une forme fréquente de diffusion non consentie de contenus sexuels. Ces photos ou vidéos étant envoyées volontairement par la victime durant sa relation avec l'agresseur, leur diffusion ultérieure – bien que potentiellement non consentie par la victime – n'était donc pas interdite par la loi. Il en était de même pour la diffusion non consentie d'une sextape réalisée de manière consentie par la victime. Dans ces deux exemples, les personnes à l'origine de la diffusion ne pouvaient pas être poursuivies pénalement car la victime avait donné son accord pour réaliser les contenus ou les avait initialement transmis de manière volontaire.

[18] Parizot, R., & Perrier, J.-B. (2017). Chronique législative. *Revue de science criminelle et de droit comparé, 2017*(2), 378. Dalloz.
[19] *Ibid.*

Jurisprudence. En 2016, il a été explicitement affirmé par la Cour de cassation que l'article 226-1 du Code pénal – et par ricochet l'article 226-2 – ne pouvaient être appliqués à une affaire où les images avaient été prises avec le consentement de la victime. La Cour a retenu que « n'est punissable que si l'enregistrement ou le document qui les contient a été réalisé sans le consentement de la personne concernée »[20], et qu'ainsi « n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement »[21]. Force a donc été de constater que de nombreuses situations préjudiciables n'étaient pas couvertes par la loi française, cette dernière n'étant plus adaptée aux évolutions des violences perpétrées dans les sphères numériques et qu'il existait donc un réel vide juridique en la matière.

Recours civil. Toutefois, il est important de préciser que la victime avait toujours la possibilité de passer par un recours civil sur le fondement du droit à la vie privée, prévu par l'article 9 du Code civil, pour obtenir la reconnaissance du préjudice subi et un dédommagement en conséquence. Ainsi, en 2015, le Tribunal de Grande Instance de Bobigny a jugé qu'effectivement, il n'était pas possible de réprimer pénalement les faits (diffusion non consentie d'images obtenues avec le consentement de la victime), mais a tout de même condamné l'agresseur à payer des dommages et intérêts à la victime.



[20] Cour de cassation, chambre criminelle, 16 mars 2016, n°15-82.676.
[21] *Ibid.*

La mise à jour du droit pénal français via la loi du 7 octobre 2016 pour une République numérique

Mise à jour législative. Le 7 octobre 2016, la loi pour une République numérique est promulguée, créant ainsi de nouveaux droits au bénéfice des victimes de cyberviolences[22]. Le législateur s'est alors saisi de la question de la diffusion non consentie de contenus à caractère sexuel et de la protection jusqu'à lors insuffisante qu'offrait le droit pénal. L'article 226-2-1 du Code pénal vient ainsi spécifiquement criminaliser la diffusion sans accord préalable de la personne représentée.

Nouveaux apports. Plusieurs constats peuvent être tirés à la lecture de ce nouvel article :

> Spécificité du caractère sexuel. Le droit en vigueur avant le 7 octobre 2016 prévoyait des peines indifférentes au domaine violé de la vie privée[23]. Le premier alinéa de l'article 226-2-1 crée ici une circonstance aggravante aux infractions définies aux articles 226-1 et 226-2 dans le cas où le contenu (photo, vidéo, enregistrement de paroles) présente un caractère sexuel. Cette spécificité du caractère sexuel est marquée par l'aggravation de la peine encourue par l'auteur.

> Élargissement du champ d'application. Le champ d'application de l'infraction d'atteinte à la vie privée par la diffusion de contenus à caractère sexuel a été élargi aux espaces publics. Au-delà de couvrir davantage de situations, cela permet concrètement aux juges chargés d'appliquer cet article de ne plus s'interroger sur le lieu où les contenus ont été fixés ou enregistrés – un enjeu qui pouvait notamment survenir lorsque la photo avait été truquée ou l'arrière-plan flouté par exemple.

> Indifférence de l'origine du contenu. Cet article s'applique aux situations dans lesquelles les contenus ont été réalisés avec le consentement de la victime ou envoyés volontairement par celle-ci. L'absence de consentement doit désormais être appréciée uniquement au regard de la diffusion des contenus, et non de la manière dont ils ont été obtenus.

[22] CNIL. (2016, 16 novembre). *Ce que change la loi pour une République numérique pour la protection des données personnelles.*
[23] Detraz, S. (2016). Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple. Commentaire de l'article 226-2-1 du Code pénal issu de la loi n° 2016-1321 du 7 octobre 2016. *Revue de science criminelle et de droit pénal comparé, 2016*(4), 741–753. Dalloz.

Notion de caractère sexuel. Si le législateur a su adapter le droit pénal français aux nouvelles formes et modalités de la violence à l'ère du numérique, la rédaction de l'article 226-2-1 a malgré tout pu être questionnée sur plusieurs points. La notion de caractère sexuel n'a par exemple pas été précisée, tout comme les conditions permettant d'apprécier l'absence de consentement de la victime.

Question prioritaire de constitutionnalité. Ces interrogations ont d'ailleurs donné lieu à une question prioritaire de constitutionnalité, demandant au Conseil Constitutionnel de statuer sur la conformité de l'article à la Constitution française[24]. Le Conseil, dans une décision du 30 septembre 2021, a coupé court aux débats en affirmant qu'il « appartient aux juridictions compétentes d'apprécier le caractère sexuel des paroles ou images diffusées ainsi que l'absence de consentement de la personne à cette diffusion »[25]. Ainsi, la rédaction de l'article 226-2-1 apparaît suffisamment claire et précise.

Acception souple. Le fait qu'il n'existe pas de définition légale de la notion de caractère sexuel permet une plus large application de la loi. En effet, donner une définition stricte d'un contenu à caractère sexuel risquerait d'exclure un certain nombre de contenus n'entrant pas dans les limites posées par celle-ci. Au contraire, l'acceptation large de la notion de caractère sexuel ouvre la possibilité que des juridictions puissent considérer des contenus ne présentant pas une activité sexuelle explicite comme relevant malgré tout du champ d'application de l'article 226-2-1.

→ L'auteur encourt 2 ans d'emprisonnement et 60 000 euros d'amende si les contenus diffusés sont à caractère sexuel.

Réalité des condamnations. Dans les faits, les peines prononcées sont toutefois bien inférieures à celles encourues. À titre d'exemple, dans l'affaire Jean Paul Dupré[26], la mise en cause a été condamnée à deux mois d'emprisonnement avec sursis et 800 euros d'amende en première instance, puis à six mois d'emprisonnement avec sursis et 800 euros d'amende en appel et en cassation.

CA Metz, 6 octobre 2015 : Condamnation à 2 ans de prison ferme pour diffusion non consentie de contenus intimes. L'auteur avait publié de photos intimes sur internet et inscrit son ex-femme sur des site de rencontres libertins.

T. corr. Orléans, 17 janvier 2024 : Condamnation pour diffusion non consentie de contenus intimes à 8 mois de prison avec sursis, 1500 euros d'indemnisation au titre du préjudice moral et interdiction de contacter la victime ou paraitre à son domicile pendant 3 ans.

[24] Cour de cassation, chambre criminelle, 23 juin 2021, n° 2180682.
[25] Conseil constitutionnel, 30 septembre 2021, n° 2021-933.
[26] Le Parisien. (2017, 23 juin). Aude : le maire de Limoux s'excuse après la fuite d'une sex-tape. *Le Parisien*.

Deepfake sexuel

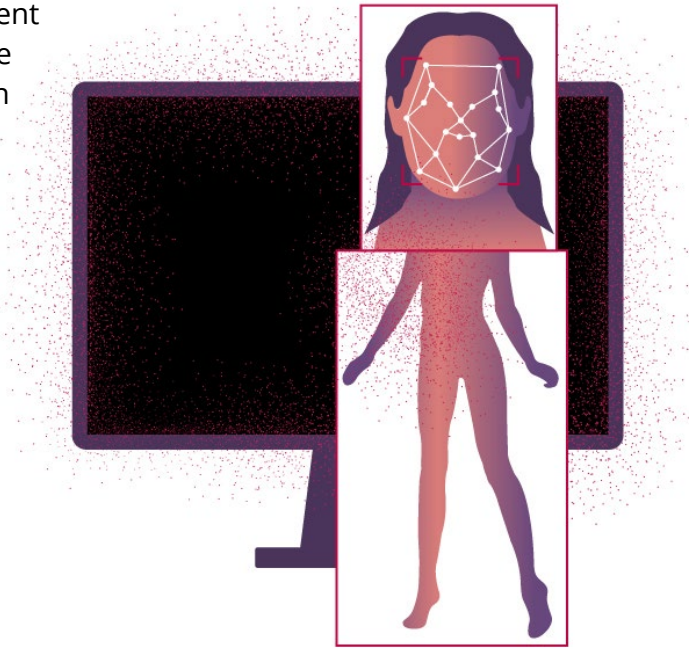
Adaptation du droit. Face à l'essor des outils d'intelligence artificielle et à la multiplication des contenus manipulés numériquement, la France a créé en 2024[27], sous l'impulsion de la directive européenne sur la régulation de l'espace numérique, une incrimination spécifique réprimant les *deepfakes* à caractère sexuel.

Définition légale. Cette infraction, désormais codifiée à l'article 226-8-1 du Code pénal, sanctionne la diffusion de montages ou contenus générés par traitement algorithmique utilisant l'image ou la voix d'une personne sans son consentement. Le texte incrimine ainsi une forme nouvelle de violence numérique qui altère, falsifie ou crée de toute pièce la sexualité supposée de la personne visée.

→ L'auteur de la diffusion d'un deepfake sexuel sans que la personne représentée n'y ait consenti et qui utilise un service de communication publique en ligne encourt 3 ans d'emprisonnement et 75 000 euros d'amende.

Conséquences particulières.
Les *deepfakes* à caractère sexuel constituent une forme de violence numérique particulièrement insidieuse, permettant de créer des images ou vidéos montrant une personne dans des situations sexuelles. La spécificité de cette cyberviolence réside dans la capacité à générer des contenus entièrement fictifs, de manière rapide et à grande échelle. À l'instar de la diffusion non consentie de contenus sexuels, la viralité et la diffusion massive des contenus via les services de communication en ligne multiplient le nombre de personnes susceptibles de les visualiser et prolongent l'exposition de la victime, anéantissant tout contrôle qu'elle peut exercer sur son image. Cette exposition imposée contribue à effacer toujours davantage la frontière entre la sphère intime et l'espace public. L'environnement numérique devient ainsi un lieu où les atteintes à la vie privée et à la dignité des personnes visées s'inscrivent dans la durée.

T.corr. Coutance, 14 mai 2025 : Condamnation à 2 ans de prison avec sursis pour avoir réalisé des montages à caractère sexuel impliquant des mineurs.



[27] Loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, JORF n°0117 du 22 mai 2024.

Contenus pédocriminels

Définition légale. L'article 227-23 du Code pénal vise à lutter contre l'exploitation sexuelle de mineurs en ligne, notamment via la diffusion d'images pédocriminelles en sanctionnant l'ensemble de ses formes, y compris lorsqu'elles sont virtuelles ou simulées. La loi définit ce type de contenu comme étant l'image ou la représentation d'un mineur à caractère pornographique.

Modalités de commission. L'article 227-23 à un champ d'application plutôt large et couvre plusieurs situations : la fixation, l'enregistrement et la transmission de contenus pédocriminels, en vue de sa diffusion si le mineur a 15 ans ou plus ; la commission des actes précités sans qu'il y ait une volonté de diffusion de la part de l'auteur, si le mineur à moins de 15 ans ; la consultation habituelle d'un service de communication au public en ligne mettant à disposition des contenus pédocriminels ; la consultation payante d'un même service ; l'achat de contenus pédocriminels, leur détention et leur diffusion.

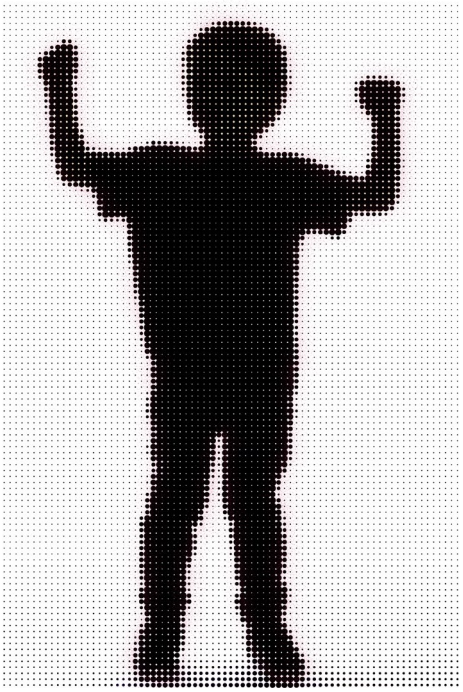
→ L'auteur d'un de ces actes encourt cinq ans d'emprisonnement et 75 000 euros d'amende.
→ Les peines encourues pour la diffusion commise via un réseau de communications électroniques.

Accroître la protection de l'enfance.

Cette infraction incarne la volonté constante du droit français et européen de garantir une protection absolue de l'enfance contre toute forme d'exploitation sexuelle.

Au-delà de prévoir une sanction pénale, elle réaffirme un principe fondamental : le corps, l'image et la représentation sexualisée de l'enfant ne peuvent jamais être monétisés, partagés, échangés ou consommés, quels que soient les outils technologiques utilisés.

En s'appliquant également aux représentations dont l'aspect physique correspond à celui d'un mineur, la loi rappelle avec force que la dignité et l'intégrité de l'enfant constituent des limites infranchissables à la liberté d'expression, de création ou de circulation des images dans l'espace numérique.



T.corr. Dijon, 16 mai 2025 : Condamnation à 3 ans de prison avec sursis et interdiction à vie d'exercer une activité avec les mineurs pour détention d'images pédocriminelles.

T. corr. Bordeaux, 15 avril 2025 : Condamnation pour avoir échangé de nombreux contenus pédocriminels sur le réseau social Telegram.

T. corr. Alençon, 30 janvier 2025 : Condamnation à 4 ans de suivi socio-judiciaire pour consultation habituelle de contenus pédocriminels.

Captation non consentie d'images intimes (upskirting)

Définition légale. Créée par la loi du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes[28], l'article 226-3-1 du Code pénal réprime le fait de filmer ou photographier, sans consentement, les parties intimes d'une personne dissimulée par ses vêtements. En d'autres termes, ce texte permet d'incriminer le fait de filmer sous la jupe ou la robe des victimes.

Évolution du droit. Cette incrimination vise à combler un vide juridique : auparavant, ces comportements échappaient souvent à la qualification d'atteinte à la vie privée, faute d'image captée dans un lieu privé. En reconnaissant l'infraction même dans l'espace public, le droit affirme que la protection de l'intimité s'attache à la personne et non au lieu. Cette évolution témoigne d'une conception renouvelée du consentement à l'image et s'inscrit dans la reconnaissance de l'inviolabilité et de l'intégrité du corps humain, juridiquement protégées contre toute captation, manipulation ou diffusion non consentie.

→ L'auteur de cette infraction encourt deux ans d'emprisonnement et 30 000 euros

Happy-slapping*

Définition légale. L'article 222-33-3 du Code pénal réprime le fait d'enregistrer et/ou de diffuser volontairement des images relatives à la commission de violences physiques, y compris sexuelles. Il est toutefois fait exception des situations où les violences sont enregistrées et diffusées en tant que preuves ou par une personne dont la profession est relative à l'information du public

T.corr. Carcassonne, 17 octobre 2025 :
Condamnation à 6 mois de prison pour avoir filmé et diffusé une scène de viol.

→ L'auteur de la diffusion de telles images encourt 5 ans d'emprisonnement et 75 000 euros d'amende.

Risque de revictimisation. Filmer, photographier ou diffuser des scènes de violences contribue à l'atteinte subie par la victime et peut en aggraver les effets. Ces pratiques accroissent le risque de revictimisation et exposent la personne à l'humiliation, à la stigmatisation et à des conséquences psychologiques durables. Le téléphone ou la caméra deviennent ainsi des moyens de pression, transformant l'acte violent en contenu diffusé à grande échelle sur les réseaux sociaux, souvent à des fins de moquerie ou de menace.

[28] Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, JORF n°0177 du 4 août 2018.

Les violences fondées sur la domination, l'exploitation et l'emprise

Sextorsion (chantage à la diffusion de photos/vidéos intimes)

Définition légale. La sextorsion est incriminée par l'article 312-10 du Code pénal. Cette infraction vise les situations dans lesquelles une personne menace de révéler ou de diffuser des contenus à caractère sexuel représentant ou impliquant la victime – photographies, vidéos, enregistrements ou messages – afin d'obtenir une contrepartie, qu'elle soit financière, sexuelle ou matérielle. Il est important de souligner que le consentement initial de la victime à la création du contenu utilisé ensuite pour la faire chanter est indifférent. En d'autres termes, l'infraction est constituée même si la victime était d'accord pour réaliser le contenu, ou l'avait elle-même transmis à la personne auteure du chantage. En effet, l'usage de la menace pour contraindre constitue en soi une infraction pénale.

Adaptation du droit. Ce comportement se situe au croisement de plusieurs infractions. Avant 2023, il ne faisait pas l'objet d'une incrimination autonome, mais pouvait être réprimé dans la mesure où il relevait de différents interdits pénaux, comme le chantage, l'extorsion ou le harcèlement sexuel. Face à l'ampleur croissante du phénomène, la loi pour la sécurisation et la régulation de l'espace numérique (SREN) du 7 juillet 2023[29] a expressément consacré la sextorsion au sein de l'article 312-10 du Code pénal, en la qualifiant de forme aggravée de chantage.

→ L'auteur de sextorsion encourt 7 ans d'emprisonnement et 100 000 euros d'amende.

T. corr. Paris, 2 novembre 2023 :
Condamnation à 3 ans de prison dont 1 an ferme pour sextorsion. Des milliers d'adresses mails, achetées sur le darkweb, avaient reçu un message d'extorsion, prétendant les avoir filmés via la webcam de leur ordinateur en train de se masturber.

[29] Loi n° 2023-566 du 7 juillet 2023 pour la sécurisation et la régulation de l'espace numérique (SREN).

Grooming (pédopiégage, corruption de mineur)

Définition légale. Le grooming peut être défini comme la sollicitation sexuelle d'un·e mineur·e de 15 ans par un majeur. Cette violence peut passer par le pédopiégeage, un procédé dont la répression est prévue à l'article 227-22-1 du Code pénal et qui se définit comme le fait pour un adulte de faire des propositions sexuelles à un enfant de moins de 15 ans en passant par un moyen de communication électronique - réseau social, sms, forum, etc. La corruption de mineur·es est aussi une technique de grooming utilisée par les pédocriminels. Cette forme d'exploitation est également réprimée par l'article 227-22 du Code pénal.

Réalités plurielles. Le grooming se caractérise par le fait qu'un adulte entre en contact avec un·e mineur·e sur Internet afin de créer une relation de confiance en vue d'obtenir de lui des images à caractère sexuel, des échanges explicites ou une rencontre physique. Ce comportement, souvent progressif et fondé sur la manipulation émotionnelle, s'inscrit dans une stratégie d'emprise visant à contourner la vigilance de l'enfant et de son entourage.

→ L'auteur de propositions sexuelles encourt 2 ans d'emprisonnement et 30 000 euros d'amende et 5 ans d'emprisonnement et 75 000 euros d'amende si ces propositions ont été suivies d'une rencontre physique.
→ L'auteur de corruption de mineur·es encourt 5 ans d'emprisonnement et 75 000 euros d'amende et dix ans d'emprisonnement et 150 000 euros d'amende si la victime a moins de 15 ans.de communications électroniques.

Fondement de l'incrimination.
L'objectif est d'intervenir en amont de la commission d'actes sexuels, d'agressions ou de production de contenus pédocriminels, en sanctionnant les comportements préparatoires et la construction de l'emprise. Le grooming illustre ainsi la capacité du droit à appréhender la prévention des violences sexuelles avant leur matérialisation : le simple fait de manipuler un·e mineur·e à ces fins suffit à caractériser l'infraction, il n'est pas nécessaire qu'il y ait effectivement eu commission d'actes sexuels, envoi de photos, etc. Par cette approche, la loi consacre une protection renforcée des mineurs dans l'espace numérique, reconnaissant leur vulnérabilité face à des formes de prédation adaptées aux modes de socialisation en ligne.

Cass. Crim. 25 janv. 1983, n°81-91.203 :
Le fait d'adresser à un(e) mineur(e) des correspondances érotiques et des dessins pornographiques qui l'incitent à une sexualité perverse relève de la corruption de mineur.

T. corr. de Colmar, 29 mai 2012 :
Le fait d'inciter à un(e) mineur(e) à exhiber et dévoiler sa poitrine et son sexe au moyen d'utilisation d'un réseau de communication électronique relève de la corruption de mineur.

Proxénétisme numérique

Définition légale. Le proxénétisme est défini par l'article 225-5 du Code pénal comme le fait d'aider, d'assister ou de protéger la prostitution d'autrui, d'en tirer profit, ou encore de recruter, d'entrainer ou de détourner une personne en vue de l'exploiter sexuellement. La loi française retient une conception large du proxénétisme. Ainsi, l'article suivant assimile au proxénétisme le fait de mettre en relation une personne en situation prostitutionnelle et un proxénète ou d'aider un proxénète à justifier les revenus tirés de la prostitution. Le fait de vivre avec quelqu'un en situation prostitutionnelle et de ne pas pouvoir justifier de ses ressources ou d'entraver l'action de structures destinées à accompagner et aider les personnes en situation de prostitution est aussi assimilé au proxénétisme..

Numérisation de l'organisation prostitutionnelle. Historiquement centré sur l'exploitation physique seule, le délit de proxénétisme s'est adapté à l'organisation contemporaine de la prostitution et aux nouvelles pratiques des réseaux d'exploitation. En effet, les réseaux de proxénétisme se développent aujourd'hui principalement sur internet – utilisation des réseaux sociaux et sites d'annonces spécialisées, tant pour le recrutement que la mise en relation avec les clients ou la recherche d'hébergement.

C. assises Val d'Oise, 26 septembre 2025 : Condamnation à 15 ans de réclusion criminelle pour proxénétisme aggravé. Les victimes, placées à l'aide à l'enfance, étaient mineures. Les rendez-vous étaient organisés en ligne.

→ L'auteur encourt 7 ans d'emprisonnement et 150 000 euros d'amende.

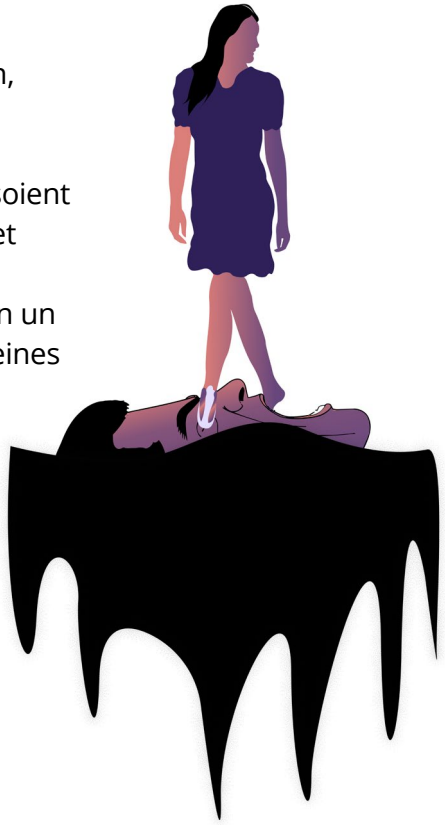
→ Lorsque la victime est mineure et a moins de 15 ans, les peines sont aggravées et peuvent atteindre 20 ans de réclusion criminelle et 3 000 000 euros d'amende.

Emancipations relatives. Si une partie des personnes concernées déclare exercer un travail du sexe, la majorité des personnes concernées par la vente de services et contenus sexuels le font dans un cadre de contrainte et de violences. Le proxénétisme numérique – à l'instar de son volet tangible – repose ainsi bien souvent sur des mécanismes de domination, de contrainte, de dépendance économique ou d'abus de vulnérabilité. Il s'inscrit dans la continuité des infractions de traite des êtres humains et de cyberexploitation sexuelle, en rappelant que la médiation technologique ne minore ni la réalité de l'exploitation, ni son impact sur les victimes.

Plateformes de contenus privés. L'achat de services sexuels virtuels personnalisés s'est significativement développé depuis la crise sanitaire sur des plateformes de partage de contenus tels qu'OnlyFans ou MYM. Au-delà de l'accès à des contenus à caractère sexuel moyennant paiement ou abonnement, ces plateformes, qui permettent la commande de contenus produits à la demande, sont en partie investies par des proxénètes. Des contenus sont parfois récupérés par des clients qui vont à leur tour les diffuser et générer un profit subsidiaire illégitime. Cette monétisation indirecte alimente une logique de profit sur autrui et contribue aux situations d'exploitation et d'abus.

Nouveaux projets d'encadrement légal.

Dix ans après la loi 2016 qui pénalise les clients de la prostitution, une proposition de loi a été déposée au Parlement pour traiter spécifiquement du proxénétisme numérique. Le projet entend interdire l'achat de services sexuels virtuels personnalisés, qu'ils soient produits en direct ou enregistrés sur commande, en assimilant cet achat à une infraction, à l'instar de la pénalisation du recours à la prostitution. Il vise alors à sanctionner les « proxénètes 2.0 » selon un régime proche de celui du proxénétisme traditionnel, avec des peines prévues allant jusqu'à sept ans d'emprisonnement et 100 000 € d'amende, et jusqu'à dix ans d'emprisonnement et 150 000 € d'amende lorsque les faits concernent un mineur ou sont commis en bande organisée. En parallèle, une proposition de loi pour une reconnaissance effective des droits fondamentaux des travailleurs et travailleuses du sexe a été déposée au Sénat le 13 avril 2026 par Anne Souyris, sénatrice écologiste de Paris.



Cyberviolences conjugales (stalking, harcèlement moral entre partenaire, atteintes numériques)

Définition légale. Les cyberviolences conjugales désignent l'ensemble des comportements de surveillance, de contrôle ou d'intimidation exercés par un·e conjoint·e, un·e ex-conjoint·e ou un·e partenaire au moyen d'outils numériques. Cette forme de violence recouvre des pratiques telles que : la géolocalisation non consentie, l'espionnage de messages, l'accès frauduleux aux comptes personnels, l'installation de logiciels-espions, l'usurpation d'identité en ligne, le contrôle de la vie numérique, les menaces ou pressions répétées par téléphone ou via les réseaux sociaux. Ces pratiques prolongent souvent les violences conjugales commises dans le monde physique et permettent à l'agresseur d'instaurer une emprise durable qui n'est plus contrainte par des limites physiques, géographiques ou temporelles.

Incriminations pénales. Sur le plan juridique, les cyberviolences conjugales se trouvent à la croisée de plusieurs incriminations différentes et sont souvent comprises comme des circonstances aggravantes.

› **Harcèlement.** Ces agissements peuvent être qualifiés de harcèlement moral au sein du couple et tombés sous le coup de l'article 222-33-2-1 du Code pénal lorsqu'ils causent une dégradation des conditions de vie de la victime et altèrent sa santé psychique ou physique.

› **Incrimination spécifiques au numérique.** Ces actes peuvent également constituer des infractions spécifiques aux usages numériques, telles que la violation du secret des correspondances (article 226-15 du Code pénal), l'usurpation d'identité en ligne (article 226-4-1 du Code pénal), la captation ou l'utilisation frauduleuse de données personnelles (article 226-18 du Code pénal), ou encore l'envoi réitéré de messages ou d'appels malveillants (article 222-16 du Code pénal).

› Atteintes à la vie privée. Les pratiques de surveillance technique relèvent également des atteintes à la vie privée et aux systèmes numériques : la géolocalisation d'une personne sans son consentement, notamment par l'installation de balises ou de traceurs GPS, est réprimée par l'article 226-1 du Code pénal ; l'accès frauduleux à des téléphones, messageries ou comptes en ligne, ainsi que l'installation ou la détention de logiciels espions, relèvent des infractions d'atteinte à un système de traitement automatisé de données prévues aux articles 323-1, 323-3 et 323-3-1 du Code pénal.

→ Lorsque le harcèlement sur partenaire, sur conjoint·e ou ex-conjoint·e a conduit la victime à se suicider ou à tenter de se suicider, les peines sont portées à 10 ans d'emprisonnement et 150 000 euros d'amende.

Notion de contrôle coercitif. Selon un rapport de la Miprof[30] (Mission interministérielle pour le protection des femmes contre les violences et la lutte contre la traite des être humains) : une femme sur trois déclare avoir subi des cyberviolences au sein du couple, notamment par le biais de la surveillance numérique ou du contrôle exercé via un téléphone, un GPS ou les réseaux sociaux. La reconnaissance successive des violences psychologiques au sein du couple en 2010[31], puis l'intégration explicite du numérique dans les infractions de harcèlement en 2018[32] ont chacune permis d'établir que les nouvelles technologies peuvent servir d'instrument de contrôle et de domination au sein du couple. À ce titre, la proposition de loi relative au renforcement de la lutte contre les violences sexuelles, déposée à la fin de l'année 2025, mentionne explicitement la notion de contrôle coercitif. Des traces de ce concept se retrouvent notamment dans la jurisprudence de la Cour d'Appel de Poitiers qui, près de deux ans auparavant, en avait déjà fait la démonstration en rendant pas moins de cinq arrêts établissant l'existence d'un mécanisme historique et collectif d'inégalités structurelles[33]. Les esprits optimistes y verront l'une des pistes les plus encourageantes pour permettre l'imbrication des différentes formes que revêtent les violences conjugales.

T.corr. Angers, 25 juin 2025 :
Condamnation pour harcèlement sur conjoint et atteinte à la privée pour avoir placé un traceur GPS dans la voiture de son ex-épouse.

T. corr. Nantes, 12 juillet 2024 :
Condamnation à 1000 euros d'amende et un stage de sensibilisation aux violences conjugales pour avoir placé un traceur GPS dans le sac à main de son ex-épouse.

[30] Ministère chargé de l'Égalité femmes-hommes, Observatoire national des violences faites aux femmes. (2024, mars). *Les violences au sein du couple et les violences sexuelles en France en 2022. Lettre de l'Observatoire national des violences faites aux femmes, 19.*
[31] Loi n°2010-769 du 9 juillet 2010 relative aux violences faites spécifiquement aux femmes, aux violences au sein du couple et aux incidences de ces dernières sur les enfants.
[32] Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, JORF n°0177 du 4 août 2018.
[33] Muller, Y. (2024, 7 mars). Consécration de la notion de contrôle coercitif… Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire. *Le Club des juristes*.

Doxing

Définition légale. Le doxing consiste à révéler, diffuser ou transmettre des informations personnelles d'une personne sans son consentement aux fins de lui nuire. Ces informations peuvent inclure l'adresse, le numéro de téléphone, les coordonnées professionnelles, ou tout élément permettant d'identifier ou de localiser la personne. La diffusion de ces informations doit exposer la victime, ses proches ou ses biens à un risque pour leur sécurité. Ces pratiques sont désormais réprimées par l'article 223-1-1 du Code pénal, créé en 2023[176].

→ L'auteur encourt 3 ans d'emprisonnement et 45 000 euros d'amende et 5 ans d'emprisonnement et 75 000 euros d'amende si la victime est mineure.

Endiguer pour protéger. Cette modalité de violence numérique transforme les données personnelles en outils d'intimidation ou de représailles. En quelques secondes, la publication d'une adresse ou d'un nom peut déclencher une campagne de harcèlement collectif, des menaces ou des actes de violence physique. Par cette incrimination, la loi reconnaît explicitement le lien entre sécurité numérique et sécurité physique : l'atteinte à la confidentialité des données devient un vecteur direct de mise en danger, rappelant que la protection des personnes passe aujourd'hui par la protection de leurs informations.

Des cyberviolences aux "contenus illicites". Les développements qui précèdent en attestent : la France dispose effectivement d'un arsenal législatif en mesure de répondre aux enjeux sociaux que soulèvent la commission de violences à caractère sexiste ou sexuelle en ligne. En criminalisant certains comportements, le droit français rend tout aussi illégaux les contenus qui matérialisent ces violences ; il devient donc nécessaire d'interroger le régime juridique applicable à ce qu'il convient de nommer les contenus illicites.

[34] Loi n°2023-22 du 24 janvier 2023 visant à lutter contre le harcèlement scolaire et le cyberharcèlement, JORF n°0021 du 25 janvier 2023.

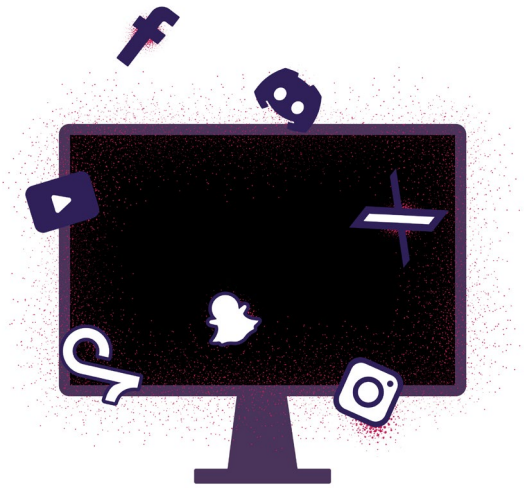
2 - L'encadrement des services numériques

Cadre législatif. Lorsque vient la question de la diffusion de contenus illégaux en ligne, la France dispose depuis de nombreuses années d'un cadre juridique en mesure de répondre à ces problématiques. S'il est effectivement possible, en droit, de faire condamner l'auteur d'infractions pénales mais également de tenir responsable une entreprise qui aurait sciemment permis que cette atteinte se produise, il reste que le temps de la justice est un temps long. Face à l'instantanéité des communications numériques et par ricochet des dommages causés, la réponse judiciaire est souvent perçue comme inadéquate ou lacunaire. Le cadre normatif français s'est donc nécessairement adapté au regard de ces enjeux, notamment en instaurant de nouvelles voies de recours. Toujours est-il qu'un travail d'explication des dispositions en vigueur s'impose afin de clarifier les régimes de responsabilité existants, en particulier au sujet des services numériques.

La responsabilité des hébergeurs dans la diffusion de contenus illégaux

Définition. Un hébergeur est défini comme un acteur dont le rôle consiste « à stocker des informations fournies par un destinataire du service à sa demande »[35]. Cette définition était déjà présente dans la Loi pour la Confiance dans l'économie du numérique (LCEN)[36] de 2004, elle-même transposant les objectifs de la directive e-commerce de l'Union européenne[37].

Rôle. En pratique, les hébergeurs n'assurent que la disponibilité des infrastructures permettant la diffusion de contenus. Ils ne jouent pas de rôle actif dans la production des contenus hébergés et sont considérés comme de simples intermédiaires neutres au regard du droit – à la différence des éditeurs. Engagement de la responsabilité. De ce fait, ils ne sont a priori pas responsables des informations transmises et diffusées sur leurs services. Toutefois, cette immunité disparaît s'ils ont eu connaissance du caractère illégal des contenus diffusés sur leur services et qu'ils n'ont pas agi promptement pour les retirer. Autrement dit, il n'existe pas d'obligation générale de surveillance des contenus diffusés sur les services. Il existe, en revanche, une obligation de diligence dès qu'une entreprise du numérique est au fait d'activités illégales sur ses services.



Précision du Conseil Constitutionnel. En 2004, le Conseil Constitutionnel a précisé que la responsabilité d'un hébergeur n'est pas engagée dès lors que « l'information dénoncée comme illicite ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge »[38].

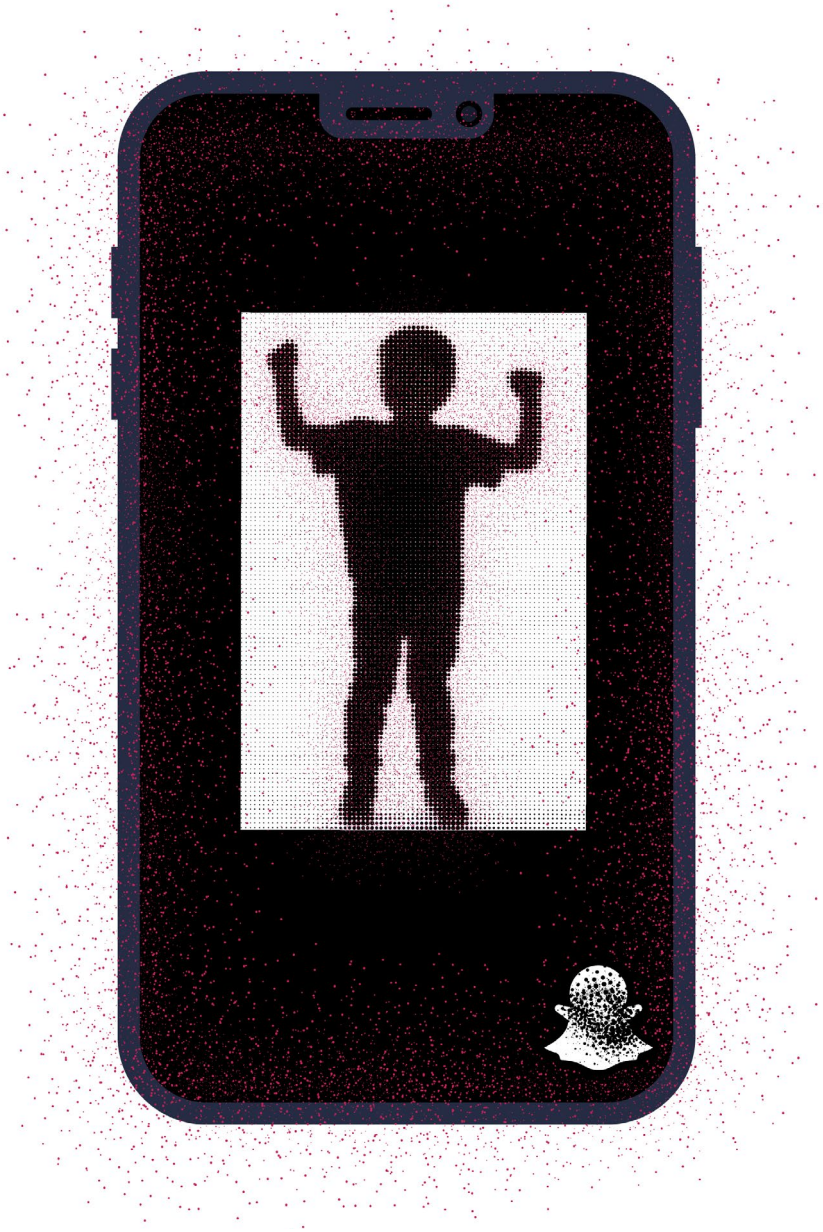
---

[35] Règlement (UE) 2022/2065 du Parlement et du Conseil relatif à un marché unique des services numériques, 19 octobre 2022, Article 3 g) iii).
[36] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[37] Directive 2000/31/CE du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, 8 juin 2000.
[38] Conseil Constitutionnel, Décision n° 2004-496 DC, 10 juin 2004.

Cas des cyberviolences sexistes et sexuelles. Cette interprétation emporte néanmoins de réelles difficultés et complexifie la répression de certaines cyberviolences, particulièrement celles à caractère sexiste et sexuel.En effet, les autorités chargées d'ordonner le retrait de certains contenus peuvent considérer que la diffusion non consentie de contenus à caractère sexuel n'est pas une pratique dont l'illicéité est manifeste, dans la mesure où le consentement n'est pas directement appréciable à l'œil nu. Cette problématique se pose particulièrement pour des sites ou des comptes de type leak ou fisha, dont le titre même fait ouvertement la promotion de contenus sexuels volés ou dont la diffusion n'est pas consentie, distribués en masse.

Équilibre des droits fondamentaux.

Toujours est-il que ce régime est solidement intégré à nos différents systèmes juridiques, qu'il s'agisse du droit français, de l'Union Européenne ou du Conseil de l'Europe. La crainte de porter une atteinte disproportionnée aux libertés d'expression et d'entreprendre en imposant à l'hébergeur une surveillance généralisée de ses services ou en permettant de déclencher sa responsabilité dès la survenance d'un contenu illégal est à ce jour perçue comme suffisamment fondée pour ne pas remettre en cause cet arbitrage.



Hébergeur ou éditeur ?

On ne peut toutefois pas ignorer les débats qui surgissent à intervalles réguliers et qui questionnent la réalité du rôle passif des réseaux sociaux dans la distribution des contenus à ses utilisateurs[39]. Peut-on maintenir, à l'heure où la plupart des plateformes reposent sur des algorithmes de recommandations ultra performants, qu'ils n'ont aucune maîtrise sur les contenus diffusés ?[40]

[39] Sire, G. (2016, 28 octobre). Facebook, YouTube, Twitter : hébergeurs ou éditeurs ? *La Revue des médias*. INA.
[40] Assemblée nationale. (2025, 4 septembre). *Rapport de la commission d'enquête sur les effets psychologiques de TikTok sur les mineurs* (p. 148).

La procédure de l'article 6-3 de la LCEN

Ordonner le retrait de contenus. Si le cadre normatif applicable aux services numériques est donc largement favorable à la libre circulation des informations, cela ne signifie pas pour autant que le justiciable se retrouve totalement désarmé dans le cas où il serait victime de cyberviolences. La LCEN met en place une procédure permettant de solliciter l'intervention d'un juge pour faire cesser un dommage résultant de la publication d'un contenu illégal. Concrètement, cela signifie que toute personne s'estimant victime d'un préjudice du fait de la diffusion en ligne de propos ou d'images peut solliciter l'appui du pouvoir judiciaire, qui statue ensuite selon une procédure accélérée. Bien qu'une telle procédure ait le mérite d'exister, il est utile de préciser qu'elle est loin de constituer une solution miracle.

Type de contenus concernés. Cette procédure contraint le juge à statuer sur le caractère manifeste de l'illicéité du contenu. Le mécanisme ouvert par l'article 6-3 visant principalement les fournisseurs de service[41], et non pas l'auteur·ice du contenu litigieux, la procédure n'ouvre pas de débat contradictoire de sorte que seul un abus caractérisé est de nature à justifier l'intervention du juge[42]. Reste que, eu égard aux développements qui précèdent, les cyberviolences sexistes et sexuelles s'appuient sur des mécanismes de domination et de contrôle et reposent bien souvent sur des images dont l'illicéité ne se caractérise pas au premier abord. Cet état de fait pourrait expliquer l'absence de décision judiciaire en la matière ; le doute reste donc entier quant à la possibilité qu'un juge ordonne le retrait de ce type de contenus sur le fondement de cette procédure.

Absence de réparation. En aucun cas la procédure 6-3 LCEN n'a vocation à réparer le dommage causé par la voie de l'indemnisation. Sa seule fonction étant de prévenir un dommage ou de le faire cesser, il ne faut donc pas escompter obtenir de dommages et intérêts par ce biais. Comme évoqué plus haut, cette voie permet uniquement d'obtenir possiblement le retrait, le blocage ou le déréférencement du contenu. Une demande d'indemnisation du préjudice allégué supposera de mobiliser des voies de recours différentes – mais qui peuvent être engagées en parallèle.

Conclusion. La consécration d'une procédure rapide et précisément dédiée à limiter les conséquences d'une diffusion de contenus illicites n'a manifestement pas été conçue pour répondre aux besoins spécifiques des victimes de violences numériques. En retenant une approche restrictive, cantonnée aux contenus considérés comme les plus graves, le pouvoir judiciaire contraint les victimes à emprunter des voies de droit plus longues et retarde ainsi le retrait effectif de ces contenus.

[41] Question écrite n° 1225 : Application de l'article 6-3 de la loi dite LCEN, 26 aout 2025.
[42] Lyannaz, C. (28 novembre 2025). DSA et article 6-3 LCEN : continuité des principes, proportionnalité des mesures. *Lamy Liaisons*.

B - Perspective européenne

Architecture juridique à double niveau. Le cadre européen applicable aux cyberviolences sexistes et sexuelles repose sur une articulation entre, d'une part, les droits fondamentaux, qui posent des principes structurants de protection contre les discriminations, et, d'autre part, le droit du numérique, qui organise la régulation concrète des contenus et des acteurs en ligne. Cette double approche permet d'appréhender les cyberviolences à la fois comme des atteintes aux droits fondamentaux et comme des phénomènes nécessitant des réponses opérationnelles adaptées aux environnements numériques. Elle structure ainsi un cadre juridique en construction, marqué par une montée en puissance des instruments européens et une volonté d'adapter le droit aux spécificités du cyberespace.

1 - La protection transversale offerte par les droits fondamentaux

Socle structurant. La lutte contre les cyberviolences sexistes et sexuelles s'inscrit, en premier lieu, dans le cadre plus large de la protection des droits fondamentaux au niveau européen. Ces derniers posent des principes généraux – au premier rang desquels le droit à l'égalité et à la non-discrimination – qui irriguent l'ensemble des politiques publiques, y compris celles relatives au numérique. À travers les textes conventionnels, le droit dérivé et leur interprétation par le juge, ils offrent un socle juridique transversal permettant d'appréhender les cyberviolences comme des atteintes aux droits fondamentaux, au-delà de leur seule dimension technique ou sectorielle.

Le droit conventionnel

Textes conventionnels. Les droits fondamentaux sont consacrés et protégés par deux textes européens majeurs, la Charte des Droits Fondamentaux de l'Union Européenne[43] et la Convention Européenne de sauvegarde des Droits de l'Homme du Conseil de l'Europe (Conv.EDH)[44]. De ces textes découle notamment le droit à la non-discrimination – le corrolaire du principe d'égalité – qui constitue une assise solide pour lutter contre les violences à caractère discriminatoire.

Champ d'application. La Charte s'applique aux institutions de l'Union ainsi qu'aux États membres lorsqu'ils mettent en œuvre le droit de l'Union[45]. La Convention européenne des droits de l'homme, quant à elle, s'impose aux 46 États membres du Conseil de l'Europe[46]. En raison de leur portée générale, qui n'affecte toutefois en rien leur caractère contraignant, ces textes offrent un cadre de référence mobilisable pour l'élaboration de réglementations numériques respectueuses de l'égalité de genre. Ils jouent un rôle de principes directeurs ; les réglementations axées sur le numérique sont ainsi tenues au respect de ces dispositions et peuvent s'appuyer sur ce droit fondamental pour affermir la protection dévolue aux minorités et personnes vulnérables[47].

---

[43] Charte des droits dondamentaux de l'Union européenne (2000/C 364/01), (2000, 7 décembre).
[44] Conseil de l'Europe. (1950, 4 novembre). *Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales*.
[45] Commission Européenne (2025). *Types of EU law*.
[46] Conseil de l'Europe. (2025). *Une Convention pour protéger vos droits et libertés*.
[47] Albrengues, A., & Lu, L. (2025, octobre). *Weight of gender in artificial intelligence models' implementation in the European Union non-discrimination laws*. ELSP.

Jurisprudence constante. La portée normative du droit à la non-discrimination a été systématiquement confirmée par le juge européen. La Cour de justice de l'Union européenne a ainsi affirmé de longue date que « l'égalité entre les hommes et les femmes est un principe fondamental de l'Union européenne » et qu'il interdit « toute discrimination fondée sur le sexe », exigeant que « l'égalité entre les hommes et les femmes soit assurée dans tous les domaines »[48], conformément aux articles 21 et 23 de la Charte de l'Union. Cette jurisprudence, largement partagée par la Cour EDH, confère au principe d'égalité une valeur structurante, susceptible d'irriguer l'ensemble des politiques publiques, y compris celles relatives à la régulation de l'espace numérique.

Le droit dérivé

Types de discriminations. Le droit européen distingue deux types de discriminations émergeant de situations dans lesquelles des traitements différenciés sont observés. Le principe sous-tendant ce pan du droit peut être résumé comme tel : à situation égale, traitement égal – sauf à pouvoir justifier de la nécessité et de la proportionnalité d'un traitement différencié. L'Union Européenne consacre ainsi :

- la discrimination directe, qui se fonde explicitement sur un attribut protégé tel que le sexe ou l'orientation sexuelle, et
- la discrimination indirecte, caractérisée par une pratique apparemment neutre mais qui produit un désavantage disproportionné pour un groupe donné[49] [50].

Directives. L'Union européenne a adopté quatre directives anti-discriminations, dont deux portant spécifiquement sur l'égalité entre les genres : la directive sur l'égalité entre les hommes et les femmes et la directive sur l'emploi. Ces textes dépassent l'énoncé abstrait du principe d'égalité en proposant une approche circonstanciée ayant vocation à s'appliquer à des domaines concrets de la vie sociale et économique. En ce sens, ne pas embaucher une femme en raison de sa grossesse doit être considéré comme une dicrimination directe fondée sur le genre et consitue donc une violation de ses droits fondamenaux[51] [52]. La lutte contre les cyberviolences fondées sur le genre peut alors prendre appui sur des directives européennes telles que celles portant sur les discriminations ou celles contre la violence faite aux femmes.

[48] CJUE, Association belge des consommateurs Test-Achats and Others v Conseil des ministres, 2011, C-236/09 ECR I-77.
[49] Directive 2006/54/CE relative à la mise en œuvre du principe de l'égalité des chances et de l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail, 2006, Article 2(1)(b).
[50] Directive 2000/78/EC portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail, 2000.
[51] *Op. cit.*, Directive 2006/54/CE relative à la mise en œuvre du principe de l'égalité des chances et de l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail, Article 2(1)(a).
[52] *Ibid.* Article 14(1)(a).

Applicabilité au numérique. Cette conception permet donc de qualifier de discriminatoires des situations dans lesquelles un traitement défavorable est fondé sur le genre, y compris lorsque ce traitement résulte de pratiques techniques ou organisationnelles. À ce titre, ces principes sont susceptibles de s'appliquer aux environnements numériques, notamment lorsque des outils algorithmiques produisent des effets discriminatoires – par exemple dans les processus de recrutement opérés totalement ou partiellement via des outils numériques[53]. Si l'application du droit à la non-discrimination demeure encore inégale au sein des espaces numériques, ces directives posent néanmoins des fondements normatifs utiles à la protection des droits fondamentaux dans le cyberespace[54].

La lutte contre les violences faites aux femmes dans l'UE

Fondements de la lutte. En Europe, le droit du numérique se révèle être un levier déterminant dans la lutte contre les cyberviolences sexistes et sexuelles. Le mot d'ordre guidant la régulation du contenu et des interactions dans le cyberespace, et particulièrement sur les plateformes numériques, est de rendre illégal sur l'espace numérique ce qui est déjà illégal dans l'espace physique[55].

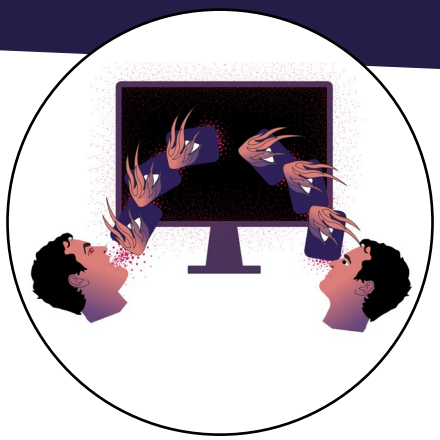
Adaptation de la législation. Cette approche implique l'émergence de nouvelles incriminations pour les comportements ou les contenus perçus comme préjudiciables – soit en transposant ou en élargissant des infractions préexistantes, soit en élaborant des nouvelles infractions pour les comportements spécifiques à l'espace numérique. La réalisation de cette promesse suppose aussi, en France et plus globalement dans l'Union européenne, la régulation des plateformes en ligne en faisant peser sur celles-ci des obligations de retrait de contenus illégaux, de modération de contenus préjudiciables et de transparence sur leurs activités.

Infractions spécifiques. En 2024, quatre infractions spécifiques sont consacrées par la directive sur la lutte contre la violence à l'égard des femmes et la violence domestique[56], le texte européen le plus récent en matière de violences de genres.

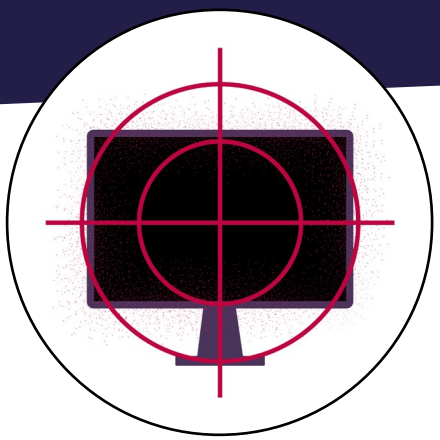
- le partage non consenti de contenus sexuels, réels ou manipulés (article 5),
- la traque furtive en ligne (article 6),
- le cyberharcèlement (article 7) et
- l'infraction d'incitation à la violence ou à la haine en ligne (article 8).

[53] Lütz, F. (2022). Gender equality and artificial intelligence in Europe: Addressing direct and indirect impacts of algorithms on gender-based discrimination. *ERA Forum*.
[54] XENIDIS Raphaële et SENDEN Linda, EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination. In U. Bernitz et al. (Eds.), *General principles of EU law and the EU digital order* (pp. 151–182). Kluwer Law International.
[55] Cluzel-Métayer, L. (2023, mars). Contrôler les contenus ? *Pouvoirs, 185*(2).
[56] Directive 2024/1385 du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 14 mai 2024.

L'INCRIMINATION DES CYBERVIOLENCES PAR LE DROIT EUROPÉEN

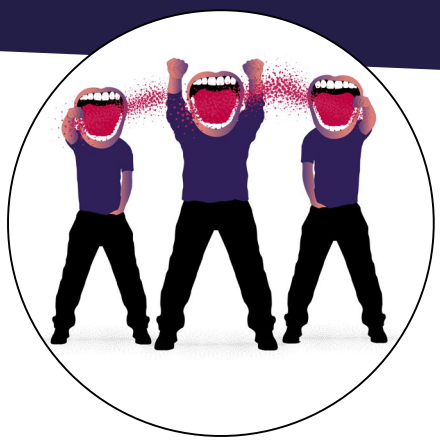


→ Le partage non consenti de contenus sexuels est défini comme étant le fait de publier un contenu à caractère sexuel - images, vidéo ou matériel similaire qu'il soit réel, manipulé, modifié ou produit artificiellement - sans le consentement de la victime et par le biais d'un outil technologique de communication ou d'information. À la différence de la loi française, la directive européenne impose une condition supplémentaire d'application de la disposition, à savoir le fait que cette publication doit risquer d'entraîner un préjudice important pour la personne représentée.



→ La traque furtive en ligne (cyber-stalking) est définie comme le fait d'espionner une personne grâce à l'utilisation de technologies de communication ou d'information. Cette pratique ne doit toutefois pas être occasionnelle ou ponctuelle pour être illégale, mais répétée ou continue. Elle doit aussi permettre à l'auteur de surveiller les déplacements ou les activités de la victime. À l'image du partage non consenti de contenus sexuel, la traque furtive requiert d'entraîner un risque de préjudice important pour être caractérisée. Cette condition n'a pas été retenue par la loi française dans la définition donnée aux différentes pratiques illégales de surveillance technique.

→ Le cyberharcèlement peut être constitué par plusieurs comportements, notamment celui pour l'auteur d'être menaçant ou insultant envers la victime, soit de manière répétée ou continue, soit de manière publique et à plusieurs. L'envoi d'images de parties intimes à une personne ne l'ayant pas sollicité peut aussi constituer une forme de cyberharcèlement, ainsi que le fait de diffuser les informations privées de cette dernière. Ces comportements doivent toutefois amener la victime à craindre pour sa sécurité, risquer de lui causer un préjudice important ou inciter des tiers à lui causer un préjudice - psychologique ou physique. Cette condition s'inscrit dans le prolongement du droit français en ce que l'infraction de harcèlement suppose de provoquer une altération de la santé physique ou mentale de la victime.



→ L'incitation à la violence ou à la haine en ligne est définie comme le fait de diffuser publiquement, au moyen des technologies de communication et d'information, des contenus incitant à la violence ou à la haine et visant un groupe de personnes ou un membre de ce groupe, lorsque cette incitation est fondée sur le genre. L'infraction suppose un acte intentionnel de la part de son auteur. La directive laisse toutefois aux États membres une marge d'appréciation quant à la portée de l'incrimination : ceux-ci peuvent choisir de ne réprimer que les comportements qui risquent de troubler l'ordre public, ou qui revêtent un caractère menaçant, injurieux ou insultant. Contrairement aux trois infractions précédentes, aucune condition tenant à l'existence d'un risque de préjudice important pour une victime individualisée n'est expressément requise, l'infraction étant davantage orientée vers la protection d'un groupe que vers celle d'une personne déterminée.

Surexposition des personnalités publiques. La cyberviolence à l'encontre des femmes s'inscrit directement dans cette conception de la violence de genre. Elle constitue en effet un obstacle à la participation démocratique et à la présence des femmes dans l'espace public en ligne, en exposant particulièrement certaines d'entre elles, notamment les femmes politiques, journalistes ou celles défendant les droits humains, à des attaques et à des risques accrus[57]. Les femmes et minorités de genre engagées dans la vie publique figurent parmi les publics les plus exposés à ces formes de violence. Cela peut avoir pour effet de réduire les femmes au silence et d'empêcher leur participation à la vie démocratique et sociale au même titre que les hommes.

2 - La protection sectorielle offerte par le droit du numérique

Agencement des textes. La régulation européenne du numérique trouve ses premières fondations dans la directive e-commerce du 8 juin 2000[58], laquelle a posé les principes structurants qui gouvernent encore aujourd'hui la responsabilité des intermédiaires techniques. Ce cadre juridique s'est progressivement consolidé sous l'impulsion de la Cour de justice de l'Union européenne, dont la jurisprudence a contraint le législateur français à adapter à plusieurs reprises son droit interne aux exigences européennes. Face à l'évolution des technologies et à la mutation profonde des usages numériques, une refonte d'ensemble s'est révélée nécessaire, aboutissant à l'adoption du règlement sur les services numériques – le *Digital Services Act* (DSA) – lequel réaffirme certaines obligations héritées du droit antérieur tout en renouvelant en profondeur la structure et la philosophie de la régulation. Si le DSA constitue désormais la pierre angulaire du droit numérique européen, il s'inscrit dans un corpus plus large, complété par le règlement général sur la protection des données (RGPD), le règlement sur les marchés numériques (DMA) et, plus récemment, le règlement sur l'intelligence artificielle (*AI Act*).

Le *Digital Services Act*[59] : instrument central de la régulation du numérique

Terminologie renouvelée. Le DSA propose une nouvelle architecture de la régulation, organisée selon une logique pyramidale. Les obligations applicables à chaque fournisseur de services numériques sont graduées en fonction de l'importance de ce dernier, mesurée sur la base du nombre d'utilisateurs mensuels actifs au sein de l'Union européenne : plus l'audience d'un service est élevée, plus les obligations qui lui incombent sont étendues et les instruments de contrôle nombreux. Le règlement distingue ainsi plusieurs catégories de services, allant du simple fournisseur d'accès à internet jusqu'à la très grande plateforme en ligne – telles qu'Instagram, TikTok ou Snapchat.

[57] Sénat, Délégation aux droits des femmes. (2026, 30 avril). Cyberharcèlement, haine en ligne : protégeons les victimes ! [Auditions].
[58] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, 17 juillet 2000.
[59] Digital Services Act (DSA), Règlement (UE) 2022/2065, 19 octobre 2022.

Nature des obligations. Le DSA s'inscrit dans la continuité des principes hérités de la directive e-commerce, tout en y apportant des compléments substantiels. L'absence d'obligation générale de surveillance des contenus est maintenue, mais les fournisseurs de services numériques demeurent tenus d'agir promptement dès lors que des contenus ou activités illicites sont portés à leur connaissance, et de coopérer avec les autorités compétentes des États membres – qu'il s'agisse des régulateurs sectoriels ou des services de police. Le règlement introduit par ailleurs des obligations nouvelles, parmi lesquelles figurent notamment la publication de rapports de transparence périodiques et la mise en place de mécanismes de signalement efficaces et accessibles sur chaque service.

Les plateformes en ligne. Le DSA consacre également la catégorie de « plateforme en ligne » comme une catégorie juridique autonome, dont le périmètre exact reste encore en partie à préciser. Les plateformes en ligne sont soumises à des obligations spécifiques, découlant de la logique de graduation propre au règlement : devoir de coopération avec les signaleurs de confiance et les organes de règlement extrajudiciaire des litiges, niveau élevé de protection des mineurs, transparence renforcée – notamment en matière de publicité ciblée et de fonctionnement des algorithmes de recommandation.

Les très grandes plateformes en ligne. Au sommet de cette architecture se trouvent les très grandes plateformes en ligne (Very Large Online Platforms – VLOP), qui rassemblent les services numériques les plus importants en termes d'audience et de trafic. Elles font l'objet d'un contrôle renforcé, exercé par la Commission européenne et les régulaters nationaux dans lesquels ils sont établis. Ces acteurs sont en particulier tenus d'identifier, d'évaluer et d'atténuer les risques dits « systémiques » que leurs services sont susceptibles de générer, et de permettre aux chercheurs d'accéder à leurs données dans des conditions encadrées.

Architecture de la régulation. En définitive, le DSA répartit les compétences de supervision entre les régulateurs nationaux – chargés de veiller au respect des obligations des fournisseurs établis sur leur territoire – et la Commission européenne, qui exerce une surveillance directe sur les très grandes plateformes. Les manquements aux obligations issues du règlement sont susceptibles d'être sanctionnés par des amendes pouvant atteindre 6 % du chiffre d'affaires mondial annuel du contrevenant.

Lutte contre les cyberviolences.

Dans la perspective de la lutte contre les cyberviolences de genre, le DSA constitue un levier dont la portée est réelle, bien qu'elle demeure conditionnée à son application effective. La répression des contenus susceptibles de relever de la cyberviolence repose en premier lieu sur la vérification de la modération effectuée par les fournisseurs de services numériques eux-mêmes – en particulier sur leur capacité à retirer les contenus illicites de manière rapide et efficace. Par ailleurs, pour les très grandes plateformes, la diffusion de contenus illicites est expressément identifiée par le règlement comme l'une des principales sources de risques systémiques, au même titre que les atteintes aux droits fondamentaux ou à certaines catégories de populations vulnérables. Cette qualification offre, en théorie, un fondement permettant d'exercer une pression régulatoire accrue sur ces acteurs afin qu'ils renforcent la protection de leurs utilisateurs.

Les autres textes de protection des libertés numériques

> RGPD[60]

Champ d'application. Le 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) s'applique à toutes les structures qui collectent ou traitent des données personnelles dans l'UE.

Applicabilité aux cyberviolences sexistes et sexuelles. Le RGPD constitue un levier important dans la lutte contre les cyberviolences, en ce qu'il encadre strictement certaines catégories de données sensibles, telles que les données biométriques, génétiques, ou relatives à la santé. Interprétées de manière large, ces catégories pourraient inclure les données relatives au genre. Si la jurisprudence ne s'est pas encore explicitement prononcée sur cette question, le RGPD reconnaît déjà les libertés et les principes de la Charte de l'UE, et la CJUE a récemment lié genre et RGPD dans l'affaire Deldits (C-247/23).

Droit à la non-discrimination. Dans son arrêt Deldits, la Cour de Justice de l'UE a affirmé que le RGPD obligeait la rectification des données d'identité de genre inexactes afin de garantir la protection des droits et libertés fondamentaux des personnes. Cet arrêt fait directement référence à la Charte de l'UE et confirme que le RGPD ne s'attache pas seulement à protéger les données des individus, mais qu'il peut aussi servir la garantie d'autres droits fondamentaux tels que le droit à la non-discrimination[61].

Cyberviolences et données personnelles. Certaines dispositions du RGPD pourraient ainsi contribuer à lutter contre les cyberviolences, notamment lorsqu'elles sont fondées sur le genre. Par exemple, l'article 22 protège les personnes contre la prise de décision automatisée, y compris les processus de notation de crédit et de recrutement en ligne entièrement automatisés, qui peuvent avoir des conséquences discriminatoires.[62] Diverses autres garanties s'appliquent à ces activités de traitement de données comme l'article 17 qui consacre un droit à l'effacement – appelé aussi droit à l'oubli. Ce droit permet aux victimes de demander la suppression de leurs données personnelles lorsqu'elles sont traitées ou publiées sans leur consentement. L'article 17 assure ainsi une couverture juridique aux victimes de cyberviolences en leur offrant la possibilité de demander la suppression de leurs données personnelles diffusées en ligne[63].

---

[60] 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, dit "Règlement général sur la protection des données (RGPD)", 27 avril 2016.
[61] CJUE, Deldits, C-247/23, 13 mars 2025.
[62] RGPD, *op. cit.*, Article 22.
[63] Garcia Diaz, E., & Méndez, L. (2020, août). L'ère du « cyberbullying » vs la protection des données personnelles. *Village de la Justice*.

L'Artificial Intelligence Act (IA Act)[64]

Champ d'application. Le règlement européen sur l'IA entré en vigueur en 2025, bien qu'imparfait, offre une opportunité pour lutter contre les cyberviolences liées aux algorithmes reposant sur de l'intelligence artificielle. Ce texte s'appuie sur une approche graduée selon le niveau de risque que chaque système présente pour les droits fondamentaux et s'applique, selon son article 2(7), à toute personne qui fabrique, utilise, distribue ou importe une IA dans l'UE.

Applicabilité aux cyberviolences. Bien que l'IA Act ne mentionne pas les cyberviolences directement, il restreint et réglemente certains types de modèles d'intelligence artificielle au regard du principe d'égalité entre les genres, notamment lors des processus de recrutement[65]. L'objectif premier du texte est en effet d' « d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle centrée sur l'homme et digne de confiance »[66]. Ce texte s'inscrit également dans une démarche destinée à assurer un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés par la Charte, au rang desquels l'égalité de genre.

Modalités d'encadrement. Le texte évoque la discrimination et le genre dans son préambule, et interdit certains usages de l'IA. Il interdit notamment certaines pratiques représentant des risques qualifiés d'inacceptables et impose des obligations spécifiques lorsques les systèmes sont considérés comme à haut risque[67], telles que la mise à disposition de la documentation aux autorités, un devoir de correction, ainsi qu'un devoir d'information.

- La notion de « risque inacceptable » se réfère notamment aux modèles d'intelligence artificielle manipulatrices ou qui mettent en place des systèmes de notation sociale.

- Un système est considéré comme « à haut risque » s'il présente une menace significative pour la santé, la sécurité ou les droits des personnes. Ainsi, si une discrimination fondée sur le genre se produit dans des domaines définis par le règlement tels que l'identification biométrique, l'éducation, l'emploi ou l'accès aux services essentiels et présente une menace significative, l'IA pourrait être classée dans la catégorie à haut risque et des obligations spécifiques pourraient s'imposer. Le règlement prolonge cette logique préventive en son article 7.1 (b) en prévoyant la possibilité d'ajouter certaines IA à haut risque à la liste initiale lorsqu'un système présente un risque de préjudice pour les droits fondamentaux, notamment lorsque les personnes ayant potentiellement subi un préjudice se trouvent dans une situation vulnérable par rapport au déployeur d'un système d'IA, par exemple en raison de leur statut ou de circonstances économiques ou sociales[68].

Perspectives d'usage. Bien qu'il soit regrettable que ce règlement, par sa nature horizontale, n'aborde pas spécifiquement les cyberviolences et l'égalité de genre, il fournit des outils utiles pour lutter contre les violences perpétuées par l'IA[69].

---

[64] Règlement (UE) 2024/1689, Artificial Intelligence Act ou « AI Act », 13 juin 2024, *op. cit.*
[65] Article 6, (2) et Annexe III Règlement (UE) 2024/1689 du 13 juin 2024 sur l'intelligence artificielle, *op. cit*.
[66] Article 1er, (1), *Idem*.
[67] Articles 18 et 20, *Idem*.
[68] Règlement (UE) 2024/1689, Artificial Intelligence Act, op. cit. Annexe III.
[69] Lütz, F. (2022). Gender equality and artificial intelligence in Europe: Addressing direct and indirect impacts of algorithms on gender-based discrimination. *ERA Forum*.

B - Perspectives internationales

Engagements des États. Le caractère intrinsèquement diffus des communications numériques et, par extension, de la criminalité qui s'y rapporte rend indispensable la coopération inter-étatique afin de lutter efficacement contre les formes qu'elle peut prendre. Parmi les textes de références portant aussi bien sur la cybercriminalité que sur la lutte contre les violences sexistes, on trouve notamment deux Conventions issues du Conseil de l'Europe que sont la Convention de Budapest et d'Istanbul.

Réponses fragmentées. Si ces instruments posent des bases essentielles en matière de coopération et de reconnaissance des violences, le cadre international demeure fragmenté et insuffisamment adapté à certaines formes spécifiques de cyberviolences sexistes et sexuelles. Cette limite apparaît de manière particulièrement saillante s'agissant de la diffusion non consentie de contenus à caractère sexuel, dont la qualification juridique, les modalités d'incrimination et les niveaux de protection varient d'un État à l'autre. En l'absence d'harmonisation, les réponses apportées restent hétérogènes et parfois incomplètes, ce qui complique la protection effective des victimes dans des environnements numériques par nature transnationaux.

1 - Les conventions internationales

> Budapest

Premier cadre international. La Convention de Budapest[70] est l'un des premiers textes à proposer un cadre normatif international sur les questions de cybercriminalité. Il constitue un instrument fondamental pour la coopération judiciaire en la matière. Son principal intérêt, du point de vue de la protection des victimes de cyberviolences, réside dans ses dispositions procédurales portant aussi bien sur la conservation des données, l'accès aux preuves numériques et l'entraide judiciaire entre Etats.

Objectif. Ces mécanismes répondent à des obstacles documentés auxquels sont confrontées les victimes de violences en ligne tels que l'hébergement des contenus à l'étranger ou les difficultés d'identification des auteurs. En pratique, ils peuvent être mobilisés dans des affaires de diffusion non consentie de contenus à caractère sexuel, de sextorsion ou de harcèlement en ligne, sous réserve que le droit pénal national criminalise ces comportements.

Lacunes et imprécisions. Précisons d'emblée que la Convention de Budapest ne reconnaît toutefois ni la dimension genrée de certaines violences numériques, ni leurs impacts spécifiques sur les victimes. Elle adopte avant tout une approche technique, centrée sur la sécurité des systèmes et des données, sans intégrer les violences fondées sur le genre comme un enjeu autonome de protection des droits fondamentaux. Malgré tout et alors même que la perspective genrée de ces violences n'est jamais explicitement envisagée au sein de ce texte, le Comité adossé à la Convention (T-CY) publiait en 2018 une étude sur les cyberviolences[71] dans laquelle plusieurs documents étaient cités – rapports, enquêtes – comme faisant état de l'exposition particulière des femmes aux violences numériques. Au regard de ces éléments, le Comité a conclu son étude en recommandant aux Etats parties d'adapter leurs droits respectifs de sorte à améliorer et renforcer l'efficacité des mécanismes prévus par la Convention en les conjuguant aux dispositions issues, à titre d'exemple, de la Convention d'Istanbul.

---

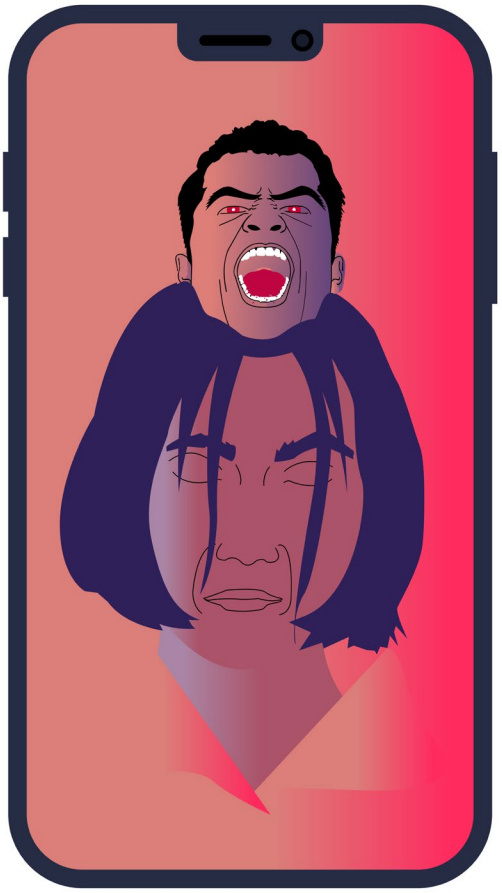
[70] Convention sur la cybercriminalité (STE n° 185), Budapest, 23 novembre 2001 (entrée en vigueur le 1er juillet 2004)
[71] Cybercrime Convention Committee (T-CY). (2018, 9 juillet). *Mapping study on cyberviolence*. Conseil de l'Europe.

› Istanbul

Protection des droits des femmes.

La Convention d'Istanbul constitue le principal instrument international reconnaissant les violences fondées sur le genre comme une violation des droits humains et une forme de discrimination.

(Cyber)Violences genrées. Si elle ne mentionne pas explicitement les espaces numériques, les principes qu'elle établit, tout comme les définitions qu'elle consacre, permettent d'interpréter ses dispositions de manière à inclure les cyberviolences sexistes et sexuelles. Le GREVIO, l'organe indépendant chargé de veiller à la mise en œuvre de la Convention, a confirmé que des comportements tels que le cyberharcèlement ou le *stalking* peuvent relever des infractions prévues par le texte, notamment au titre de la violence psychologique et du harcèlement. Cette interprétation s'inscrit en effet dans le prolongement des analyses sociologiques considérant que les violences en ligne faisant partie d'un continuum des violences sexistes préexistantes, et non pas comme des phénomènes distincts ou secondaires.



Variété des mécanismes de lutte. L'approche pluridimensionnelle de la Convention d'Istanbul, combinant prévention, protection, poursuites et politiques publiques coordonnées, offre un cadre pertinent afin de penser la réponse aux cyberviolences au-delà du seul registre pénal. Elle met notamment l'accent sur l'accès à l'information, l'accompagnement des victimes et la coordination entre acteurs et constitue en ce sens un vivier de mesures favorisant le respect effectif de l'égalité entre les genres.

Absence de force contraignante. Toutefois, la Convention d'Istanbul ne contient aucune obligation explicite concernant les plateformes numériques, la modération des contenus ou la nature de la coopération avec les acteurs privés. Son effectivité au sein des espaces numériques dépend donc largement des instruments complémentaires adoptés au niveau national et européen.

2 - Les législations nationales à travers le monde

Répression inégale. La répression des pratiques de diffusion non consentie de contenus à caractère sexuel est très inégale à travers le monde. En effet, chaque Etat dispose d'une législation qui lui est propre en la matière, plus ou moins protectrice des victimes et plus ou moins sévère envers leurs agresseurs.

Distinction majeur-mineur. Toutefois, cette affirmation n'est valable que lorsque la victime est majeure. En effet, un contenu à caractère sexuel représentant un mineur n'est plus seulement diffusé sans le consentement de la victime, mais est à caractère pédocriminel et donc interdit par la grande majorité des Etats. En 2018, seulement 16 Etats n'avaient pas encore adopté de loi visant à interdire et sanctionner ce type de contenu[72].

> Des méthodes d'incrimination divergentes

C'est lorsque la victime est majeure que les inégalités entre les différentes législations nationales se creusent mais il est cependant possible de dégager deux grandes tendances.

La diffusion non consentie comme infraction autonome

Un certain nombre d'Etats sanctionnent explicitement la diffusion non consentie de contenus à caractère sexuel en l'érigeant en tant qu'infraction autonome au sein d'une loi ou d'un article spécifique de leur code pénal.

Europe. C'est par exemple le cas du Royaume Uni, qui a créé en 2015 une nouvelle infraction visant à réprimer ce type de violence. En effet, la section 33 du Criminal Justice and Courts Act interdit la divulgation de photographies et de films privés à caractère sexuel dans l'intention de nuire[73]. L'Italie quant à elle interdit depuis 2019 la diffusion illicite d'images ou de vidéos à caractère sexuellement explicite au sein des dispositions de l'article 612-ter de son Code pénal[74].

Amérique. De l'autre côté de l'Atlantique, le Code pénal brésilien criminalise, depuis 2018, à l'article 218-C le fait de diffuser par tout moyen une photographie, une vidéo ou tout autre enregistrement audiovisuel à caractère sexuel, lorsque la victime n'y a pas consenti. Une référence spécifique aux cas de deepfakes y est par ailleurs faite, interdisant ces contenus lorsqu'ils ont pour objet le fait d'insérer une personne dans une scène de nature sexuelle ou pornographique, ou le fait de laisser croire à la nudité de cette personne[75].

[72] Panorama Global. (2023). *I didn't consent : a global landscape report on image-based sexual abuse* (p. 22).
[73] Criminal Justice and Courts Act, S. 33, Disclosing private sexual photographs and films with intent to cause distress, Royaume-Uni, 2015.
[74] Code pénal italien, Article 612-ter. (Diffusione illecita di immagini o video sessualmente espliciti), 2019.
[75] Code pénal brésilien, Article 218-C, 2018.

Spécificité canadienne.

Le Canada incrimine cette cyberviolence au sein de l'article 162.1 de son Code pénal. Les dispositions de cet article interdisent spécifiquement le fait de publier, distribuer, transmettre, vendre ou rendre accessible la publication d'une image intime sans le consentement de la personne qui y est représentée. Le droit canadien se démarque des autres législations nationales en matière de champ d'application de l'infraction de diffusion non consentie de contenus à caractère sexuel. En effet, l'infraction peut être constituée même lorsque les contenus n'ont pas encore été diffusés mais que l'auteur·ice en fait la publicité ou la promotion[76].

Asie. Du côté du continent asiatique, certains Etats ont suivi ce format d'incrimination. C'est par exemple le cas du Japon qui interdit la diffusion non consentie de contenus à caractère sexuel au sein d'un article de loi dédié. En effet, l'article 3 de la loi visant à prévenir des dommages causés par "la fourniture d'enregistrements d'images sexuelles privées" interdit le fait d'offrir, de transmettre ou de mettre à disposition un enregistrement d'images sexuelles privées d'une personne identifiable sans que celle-ci n'y ait consenti[77]. C'est aussi le cas de la Corée du Sud, donc la législation nationale visant les crimes de nature sexuelle s'est saisie de la question des « crimes sexuels numériques ». Entre 2023 et 2024, le *Sexual Crimes Punishment Act* a été amendé afin d'être applicable aux situations de diffusion non consentie de contenus à caractère sexuel et de se saisir de la question des *deepfakes* sexuels[78].

Océanie. Enfin, à titre de dernier exemple, la Nouvelle-Zélande criminalise cette cyberviolence au sein de la section 22A du Harmful Digital Communications Act de 2015 par modification de cette loi en 2022. Plus précisément, ces dispositions visent l'acte de publier un enregistrement audiovisuel intime d'une personne lorsque l'auteur sait qu'elle n'y a pas consenti, ou lorsqu'il a été "imprudent" en la matière[79].

[76] Code pénal canadien, Article 162.1, 2015.
[77] Act on the Prevention of Damage by the Provision of Private Sexual Image Records, Article 3, 2014.
[78] Sexual Crimes Punishment Act, Article 14(3), Corée du Sud.
[79] Harmful Digital Communications Act, S. 22A, 2022.

L'interdiction de la diffusion non consentie par le biais d'autres incriminations

D'autres Etats répriment la diffusion non consentie de contenus à caractère sexuel en se fondant sur l'interdiction d'autres atteintes, telles que celle au droit à la vie privée par exemple.

Exemples. C'est par exemple le cas de la Russie qui réprime cette cyberviolence sous l'incrimination d'atteinte à l'inviolabilité de la vie privée[80], de l'Allemagne qui qualifie ces actes d'atteinte à la sphère la plus intime de la vie des personnes (traduction du texte original)[81]. Le Portugal a fait ce choix aussi, mais distingue l'acte de diffuser à l'aide d'un moyen de télécommunication des images ou autre document relatif à la vie privée d'autrui[82] des autres actes relatifs à ces mêmes contenus, comme par exemple celui de capter ou enregistrer[83]. Ce format de répression se rapproche du modèle français. En effet, la diffusion non consentie de contenus à caractère sexuel constitue une forme aggravée de diffusion de contenus à caractère privé, laquelle s'analyse elle-même comme une atteinte à la vie privée, mais est criminalisée par un article spécifique du Code pénal français depuis 2016.

Tendance globale. Toutefois, une tendance générale à prendre en considération cette cyberviolence et les personnes qui en sont victimes se dégage généralement des politiques menées par les différents Etats ces dernières années.

L'incrimination de la diffusion non consentie de contenus à caractère sexuel en Australie

Online Safety Act. En 2021, l'Australie a adopté le *Online Safety Act* afin de responsabiliser les plateformes d'hébergement et réseaux sociaux, et de les impliquer davantage en matière de sécurité des internautes et de protection de leurs droits[84]. L'Etat a aussi mis en place une autorité nationale chargée de la sécurité en ligne des internautes. L'*Office of the eSafety Commissioner* a, en effet, pour mission de protéger les citoyens au sein de l'espace numérique contre les différents abus qui s'y produisent. Créée en 2015, cette autorité était initialement destinée à couvrir les sujets relatifs à la protection des mineurs en ligne. Avec l'adoption du *Online Safety Act* en 2021, son champ de compétence a été élargi et elle est devenue la principale autorité de régulation des contenus circulant en ligne en Australie.

Pouvoirs contraignants du régulateur. Plus particulièrement concernant la diffusion non consentie de contenus à caractère sexuel, cette structure reçoit les plaintes des victimes dont les contenus ont été diffusés sans leur accord, ou menacés de l'être. Elle exige ensuite des plateformes d'hébergement de retirer ces contenus au plus vite, le délai étant fixé à 24 heures. En cas de refus ou d'absence de réponse de la part de ces derniers, l'*Office of the eSafety Commissioner* peut notamment requérir l'attribution d'amendes civiles. L'Office pratique aussi le *naming and shaming* en publiant régulièrement le nom des plateformes n'étant pas coopératives.

---

[80] Code pénal russe, Article 137.
[81] Code pénal allemand (StGB), §201a.
[82] Code pénal portugais, article 193.
[83] *Idem*, article 192.
[84] Panorama Global. (2023). *I didn't consent : a global landscape report on image-based sexual abuse* (p. 24).

Interdiction de la pornographie. Enfin, certains Etats tendent à considérer comme un acte criminel le fait de diffuser des contenus à caractère sexuel alors que la victime n'y a pas consenti, non pas dans le but explicite de protéger cette dernière, mais parce que la diffusion de contenus pornographiques y est tout simplement interdite. C'est par exemple le cas de l'Arabie Saoudite, du Kenya[85] ou encore de l'Afghanistan depuis que le régime Taliban est au pouvoir.

> Un manque d'harmonisation dans la définition de l'infraction

Appréhension des éléments constitutifs. Les droits internes des différents Etats susmentionnés divergent également quant à la définition de ce type de contenu et aux éléments constitutifs de l'infraction de diffusion non consentie de contenus à caractère sexuel. Certains Etats ne définissent d'ailleurs tout simplement pas cette notion, et c'est par exemple le cas de la France qui laisse le soin aux juges de l'apprécier[86].

L'intimité canadienne. Le Canada utilise le terme " image intime " pour désigner ces contenus, qui doit s'entendre comme étant tout enregistrement visuel d'une personne, réalisé par quelque moyen que ce soit, au sein duquel la personne est nue ou expose ses organes génitaux, sa région anale ou ses seins, ou se livre à une activité sexuelle explicite. Le fait que la personne visible sur l'image puisse raisonnablement en attendre à ce qu'elle reste privée est une condition supplémentaire ajoutée à cette définition. Un tel degré de précision est rarement observé au sein de ce genre de dispositions, ce qui rend d'autant plus singulière l'appréhension de cette cyberviolence par le droit canadien.

L'intimité sud-africaine. L'Afrique du Sud retient également l'expression image intime, qui désigne une représentation, réelle ou simulée, faite par quelque moyen que ce soit, dans laquelle la victime est nue, ou ses parties intimes sont visibles, ou si la victime est de genre féminin, sa poitrine est visible. L'Afrique du Sud prend en compte explicitement les personnes transgenres en précisant qu'un contenu est intime si la poitrine est visible et que cette victime est une "*transgender person or intersex person*"[87]. Une image intime devra aussi être regardée comme telle dès lors qu'elle constitue une représentation qui porte atteinte ou offense l'intégrité sexuelle ou la dignité de la victime, ou qui constitue un cas d'exploitation sexuelle.

Du sexuel à l'intime. Certaines définitions légales sont donc plus larges et protectrices que d'autres. En effet, retenir le terme d'image intime permet de dépasser le cadre du contenu strictement sexuel et d'englober d'autres images, telles que des photos sur lesquelles la victime est en sous vêtement, ou habillée mais dans une position sexualisée. Toutes les juridictions ne retiennent toutefois pas ce caractère intime du contenu et se limitent à interdire la diffusion non consentie de contenus représentant la victime engagée dans une activité sexuelle ou montrant ses parties intimes. Or, ces acceptions peuvent se révéler trop restrictives dans la mesure où elles limitent le degré de protection accordé à certains types de contenus jugés insuffisamment explicites. En effet, il n'est pas nécessaire que l'image publiée montre explicitement les parties génitales de la victime pour que celle-ci subisse un préjudice important.

---

[85] *Ibid*, p.26.
[86] Conseil constitutionnel français, 30 septembre 2021, n° 2021-933.
[87] Section 16, 2-b-i-ii, Cybercrime Act, Afrique du Sud.

Souplesse française. La solution adoptée par les juridictions françaises peut donc apparaître comme satisfaisante sur ce point. Ne pas définir rigoureusement les contours de du caractère sexuel permet au juge du fond d'apprécier la notion sans être lié par le principe d'interprétation stricte de la loi pénale et l'image d'une personne posant en sous-vêtements dans un lit, par exemple, pourrait ainsi être considérée comme revêtant un caractère sexuel.

Limites du cadre normatif. L'analyse du cadre juridique applicable aux cyberviolences sexistes et sexuelles – qu'il soit d'origine française, européenne ou internationale – révèle un arsenal normatif réel, dont la densité et la progressivité témoignent d'une prise de conscience croissante des pouvoirs publics face à ces phénomènes. Reste que l'existence de règles de droit ne préjuge pas de leur effectivité. Or, c'est précisément l'effectivité de la protection – et non sa seule existence formelle – qui conditionne la réalité de la sécurité des personnes dans l'espace numérique.

Centralité des plateformes.

À cet égard, les plateformes numériques occupent une position déterminante. Premières destinataires des signalements, premières gardiennes des contenus en circulation et premières interlocutrices des victimes, elles constituent le maillon opérationnel sans lequel aucune protection effective ne saurait être garantie. Ce sont elles qui, au quotidien et en continu, font – ou ne font pas – appliquer les règles qui s'imposent à elles. C'est donc l'analyse de leurs propres règles d'utilisation et de leurs pratiques concrètes de modération qui permet seule de mesurer l'écart entre la norme et la réalité, entre la protection promise et la protection effectivement assurée aux victimes de cyberviolences sexistes et sexuelles.

2. Le cadre d'usage des plateformes

A - Les règles d'utilisation des plateformes

Étude comparative. Les Conditions Générales d'Utilisation (CGU), dont la dénomination varie d'une plateforme à l'autre (Community Guidelines, Rules and Policy, ...) de douze Très Grandes Plateformes En Ligne (VLOPs) ont fait l'objet d'une étude comparative à l'hiver 2025-26 afin d'évaluer les politiques adoptées par ces services en matière de prise en compte des cyberviolences sexistes et sexuelles et de réponses apportées à ces dernières.

Plateformes étudiées. Les plateformes ayant fait l'objet de cette analyse comparative sont les suivantes : Meta (Facebook et Instagram), X, Snapchat, TikTok, YouTube, LinkedIn, Pinterest, Pornhub, Xnxx, Xvideos, Stripchat. À la lecture de leurs CGU respectives, il apparaît que la prise en compte des cyberviolences sexistes et sexuelles par ces plateformes est encore aujourd'hui – trop – inégale.

1 - La reconnaissance des cyberviolences sexistes et sexuelles par les plateformes

> L'absence de prise en compte de la dimension genrée des cyberviolences

Haine de genre. La dimension genrée d'une cyberviolence est souvent abordée dans les CGU des réseaux sociaux lorsqu'il s'agit de discours de haine en ligne, le genre étant l'un des critères protégés mentionnés par les plateformes. C'est par exemple le cas de LinkedIn, Pinterest, Snapchat, TikTok ou encore YouTube. Meta proscrit, par exemple, toute incitation à la violence à l'encontre des femmes et interdit la publication de contenus dévoilant l'identité d'une femme si cela l'expose à des risques de préjudices. Meta interdit notamment certains contenus révélant l'identité de femmes lorsque cette exposition est susceptible de les mettre en danger, par exemple dans des contextes où le fait d'apparaître sans voile peut entraîner des représailles sociales ou judiciaires.

Neutralité des violences sexuelles. Malgré le fait que la haine à l'égard des femmes soit une problématique reconnue presque uniformément par les plateformes et proscrite par ces dernières, le caractère genré des cyberviolences sexistes et sexuelles reste insuffisamment abordé. L'adoption par les réseaux sociaux d'une définition neutre de la diffusion non consentie de contenus intimes, alors même que plus des trois quarts des victimes appartiennent au genre féminin[88], en constitue un exemple flagrant.

[88] Chiffres issus de la Grande Enquête sur les Cyberviolences Sexistes et Sexuelles.

Exceptions. Néanmoins, certaines CGU ciblent spécifiquement des cyberviolences qui, de par leur nature et leur appellation, ciblent davantage les personnes qui s'identifient au genre féminin. C'est par exemple le cas de Meta et de Pinterest, deux réseaux sociaux qui interdisent la diffusion d'images prises via *upskirting*. Du côté des sites pornographiques, Pornhub est le seul à envisager les violences à caractère genré en interdisant également ce type de contenu. Les CGU des trois autres plateformes pornographiques étudiées restent silencieuses à ce sujet.

> L'interdiction de principe des cyberviolences sexistes et sexuelles

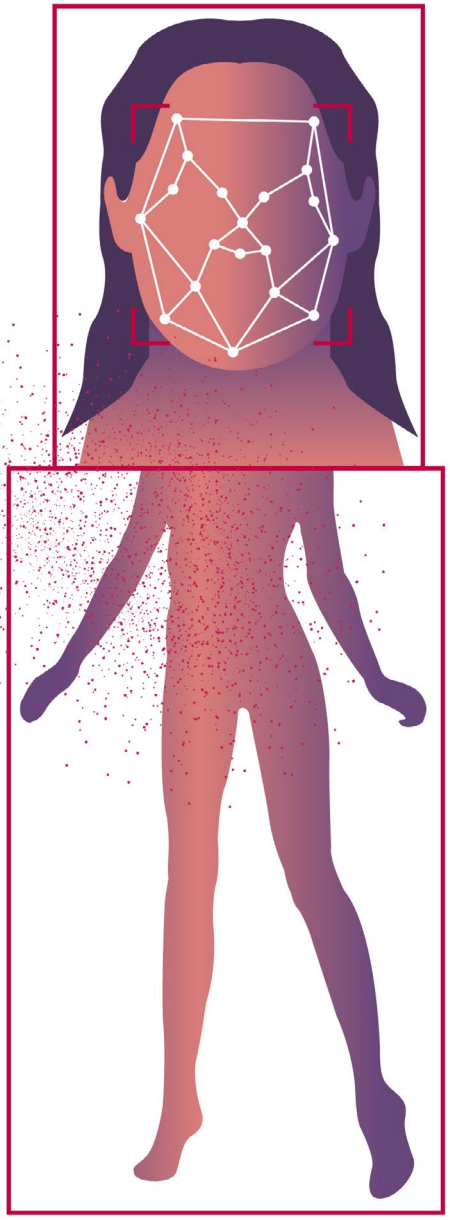
Réseaux sociaux. Les réseaux sociaux tels que Facebook, Instagram, Pinterest, TikTok ou encore Snapchat semblent se positionner sur la question des cyberviolences sexistes et sexuelles avec un certain sérieux.

Diffusions non consenties. À titre d'exemple, la diffusion non consentie de contenus intimes est quasi-systématiquement envisagée et définie dans les conditions générales d'utilisation (CGU) des plateformes étudiées – à l'exception de LinkedIn, qui prévoit une interdiction générale à l'égard de tout contenu présentant un caractère sexuel. Une image intime diffusée sur l'un des réseaux sociaux précités est donc supposée contrevenir aux règles de la communauté et impliquer une mesure de modération de la part du service – *a fortiori* ne pas la retirer déclencherait sa responsabilité pénale.

Plateformes pornographiques. Les quatre plateformes distribuant du matériel pornographique étudiées (Pornhub, Stripchat, Xnxx et Xvideos) interdisent elles aussi la diffusion non consentie de contenus à caractère sexuel. En d'autres termes, les personnes visibles sur les contenus pornographiques diffusés sur ces plateformes doivent avoir expressément accepté leur diffusion. Les CGU du site Xnxx stipulent par exemple que toute personne soumettant un contenu pour diffusion doit disposer du consentement ou la permission écrite à utiliser l'image de chaque personne identifiable. Ainsi, toute « image intime non consensuelle », selon les termes de Xvideos et Xnxx, ou tout "contenu non consensuel", selon les termes de Pornhub, sont contraires aux règles internes de ces plateformes. Il en est de même pour Stripchat qui interdit la diffusion si la personne visible sur le contenu n'y a pas consenti.

Hétérogénéité des définitions. Toutefois, si l'interdiction de diffusion non consentie de contenu intime ou sexuel semble faire consensus au sein des différentes plateformes, à l'instar des législations nationales, la définition précise de cette cyberviolence varie d'une plateforme à l'autre. À titre exemple, les CGU de Meta considèrent comme contraire à leurs règles « le partage, la menace ou la déclaration d'intention de partager, offrir ou solliciter des images intimes non consensuelles ». Pinterest interdit la production, la publication et la reproduction d'images non consentantes, adoptant ainsi une définition proche de celle utilisée par Snapchat. De son côté, X interdit la nudité non consentie, expression désignant le fait de publier ou de partager des photos ou vidéos intimes d'une personne ayant été réalisées ou diffusées sans son accord. Quant à YouTube, la plateforme envisage cette cyberviolence et la proscrit sans proposer toutefois de définition au sein de ses CGU.

Deepfakes sexuels. Certaines plateformes envisagent explicitement d'autres formes de cyberviolences sexuelles contemporaines en admettant qu'une image intime non-consensuelle[89] puisse également s'entendre dans les cas où ladite image est générée artificiellement – supposant l'usage de l'IA. Certains procédés permettant notamment d'accoler le visage d'une personne sur un corps nu ou impliqué dans une activité sexuelle – ou de simplement la déshabiller artificiellement. On parle alors deepfake sexuel. X et Meta reconnaissent cet acte comme une forme de diffusion non consentie de contenus intimes. A l'inverse, les CGU de YouTube ne l'envisagent pas en tant que cyberviolence sexiste et sexuelle et celles de Snapchat n'en font tout simplement pas mention. Pornhub envisage aussi cette question, en considérant qu'un deepfake ou tout autre forme de contenu généré ou manipulé par IA puis diffusé sans le consentement de la personne représentée constitue bien un contenu non consensuel. Xnxx, Xvideos et Stripchat demeurent toutefois silencieux à ce sujet.



Positions équivoques. Si les plateformes étudiées ont chacune admis que garantir des espaces sûrs supposent de lutter contre les cyberviolences à caractère sexiste et sexuel, l'analyse minutieuse de leurs règles d'utilisation met toutefois en évidence une prise en compte limitée, inégale – voire inexistante – de la dimension genrée de ce type de violences. La terminologie employée pour désigner les contenus intimes diffusés illégalement, tout comme les actes matériels constituant une violation des règles, varient selon la plateforme concernée – laissant planer le doute sur les modalités de mise en œuvre de ces règles. Ce constat s'inscrit dans le prolongement des développements précédents au sujet de l'encadrement légal : il n'existe pas de définition universelle de la diffusion non consentie de contenus intimes. Celle-ci fluctue d'une juridiction à l'autre, tout comme elle fait l'objet d'acceptions différentes d'une plateforme à l'autre.

2 - La lutte contre les cyberviolences sexistes et sexuelles par les plateformes

> Les centres d'aide aux victimes

Sanctionner et guider. La prise en considération des cyberviolences sexistes et sexuelles et de leur impact sur les victimes a pu pousser certaines grandes plateformes à dépasser la simple sanction des auteurs – suppression des contenus, suspension des comptes, bannissement – et proposer un système d'accompagnement et de redirection des victimes vers des structures d'aide et, parfois, un espace de sensibilisation des internautes sur ces questions,

[89] Expression utilisée au sein des Conditions Générales d'Utilisation (CGU) de Meta.

Centres d'assistance. À l'image du centre d'aide Soutien aux victimes d'abus sexuels de TikTok[90], Meta propose par exemple un espace d'aide aux victimes[91] qui redirige vers des espaces dédiés comme Stop à la sextorsion, informe la victime des différents moyens de signalement disponibles et liste les actions qu'elle peut prendre afin de limiter la diffusion de ses images intimes via la plateforme *Take It Down* (victime mineure) ou StopNCII.org (victime majeure). Un centre de ressource est aussi disponible et couvre plusieurs sujets, notamment la préservation de la sécurité des femmes en ligne. Il en est de même pour Pinterest qui propose un centre d'assistance à ses utilisateur·ices au sein duquel la procédure de signalement de contenus diffusés sans consentement y est détaillée[92]. La plateforme a d'ailleurs mis en place un formulaire de signalement spécifique à ce type de contenus. Un centre de redirection est aussi mis à la disposition des internautes, leur permettant de trouver des structures d'aide adaptée en fonction de leur situation et des violences subies. Snapchat a adopté un fonctionnement similaire avec la mise en place de l'outil *Here for you* directement accessible sur l'application et la création d'un espace recensant les différentes structures d'aide aux victimes en fonction de la localisation géographique de l'utilisateur·ice. Toutefois, en matière de cyberviolences sexistes et sexuelles, aucune structure n'est mentionnée pour la France.

Judiciariser. En matière de contenus d'exploitation sexuelle de mineur·es, les plateformes YouTube et Pinterest annoncent dépasser l'assistance aux victimes et participer à leur judiciarisation en signalant elle-même lesdits contenus aux autorités compétentes – reste que, aussi important que cela soit de le signifier, ce signalement est en réalité une obligation directement issue de la loi française[93].

> La suspension dès le signalement chez les plateformes diffusant des contenus pornographiques

Suspension préventive. Certaines plateformes pornographiques ont mis en place des systèmes de suspension temporaire de tout contenu signalé. En d'autres termes, le contenu n'est plus accessible dès l'instant où il a été signalé et jusqu'à ce que l'équipe de modération du service concerné ait pris une décision le concernant. Cette pratique permet d'empêcher les utilisateur·ices de pouvoir continuer à visualiser un contenu qui pourrait se révéler illégal. Après examen du signalement, le contenu est définitivement supprimé si son illicéité est conformé par les modérateur·ices ou est remis en ligne dans le cas contraire. Pornhub est la première grande plateforme chez laquelle cette démarche a été observée.

Mises en œuvre différenciées. Les plateformes affirment de manière quasi-unanime et uniforme au sein de leurs CGU proscrire la diffusion non consentie de contenus à caractère sexuel. Toutefois, en pratique, ces plateformes n'accèdent pas toujours aux demandes de retrait de tels contenus formulées par les associations spécialisées telles que Point de Contact ou #StopFisha et les procédures suivies pour en obtenir la suppression peuvent s'avérer longues et fastidieuses. En outre, le contenu et la qualité de la mise en œuvre des CGU de ces plateformes restent largement aux mains des entreprises qui les édictent, ces conditions d'utilisation reposant avant tout sur une logique contractuelle manifestement déséquilibrée. La réalité de leur application en vient mécaniquement à dépendre de la bonne volonté d'une poignée de dirigeants d'entreprises – laquelle s'est effondrée au cours des dernières années.

---

[91] Soutien aux victimes d'abus sexuels, Centre de sécurité de TikTok.
[92] Lutter contre la sextorsion et la divulgation d'images intimes, Centre de sécurité de Meta.
[93] Avis de procédure : combattre les images intimes non consentantes, Centre d'aide de Pinterest.
[94] Loi pour la confiance dans l'économie numérique (LCEN), Article 6, IV, A.

B - Les pratiques de modération des plateformes

Disparité des pratiques.

Les signaleurs de confiance et les associations spécialisées dans les cyberviolences se trouvent en première ligne pour observer et documenter les pratiques de modération des plateformes et hébergeurs de contenus en ligne. Ces pratiques, très hétérogènes, conditionnent directement l'effectivité de la protection des victimes de cyberviolences sexistes et sexuelles, perpétrées massivement sur ces plateformes. Si certaines d'entre elles se conforment à leurs obligations de diligence, d'autres s'illustrent à l'inverse par leurs défaillances, si ce n'est leur défiance à l'égard du droit.

Bonnes pratiques. À ce titre, certaines bonnes pratiques méritent d'être soulignées. Inscrites dans un cadre conforme aux exigences européennes de transparence et de proportionnalité, elles sont de nature à instaurer une relation de confiance entre les plateformes, leurs utilisateur·ices et les organisations de la société civile mandatées pour assurer la protection des victimes.

Suspension des contenus.

Ainsi que les développements précédents en attestent, certaines plateformes procèdent à la suspension immédiate de l'accès aux contenus signalés, dans l'attente de la vérification de leur licéité. Cette mise en quarantaine préventive, opérée sans exiger de démarches excessives de la part des victimes, constitue un exemple de conduites préventives à saluer – dès lors que celle-ci est strictement encadrée.

Mécanismes de signalement.

Dans la même logique, certaines plateformes mettent en œuvre des mécanismes de signalement accessibles et traçables, adressent des accusés de réception aux signaleurs, et notifient leurs décisions motivées dans des délais raisonnables. Bien qu'il s'agisse là d'obligations légales, il est utile de préciser que deux ans après l'entrée en vigueur du DSA, la motivation des décisions de modération constitue encore une exception.

Pratiques préoccupantes. Cependant, l'expérience de terrain révèle également des pratiques alarmantes. Nombreuses sont les plateformes ou services numériques qui opposent aux notifications de contenus illégaux des exigences disproportionnées, telles que la transmission de documents d'identité, de lettres manuscrites ou de photographies de la victime, voire la production d'une décision judiciaire préalable. Ces démarches, qui excèdent largement le cadre fixé par le DSA, constituent des entraves manifestes à la rapidité d'intervention pourtant essentielle à la limitation du préjudice.

Silence des fournisseurs d'hébergement. Dans d'autres cas, les hébergeurs s'abstiennent purement et simplement de répondre, même face à des signalements étayés démontrant la présence de contenus illicites. Certains forums explicitement dédiés au partage de contenus sexuels non consentis illustrent ces manquements : malgré plusieurs dizaines de notifications adressées à leurs hébergeurs – dont une partie est établie en dehors de l'Union Européenne, aucune réponse n'a été apportée et les contenus demeurent en ligne, en violation des obligations de retrait prompt prévues par le droit européen.

Propriété intellectuelle. Plus grave encore, certains opérateurs invoquent abusivement le droit de la propriété intellectuelle pour refuser de retirer des contenus relevant de la diffusion non consentie d'images à caractère sexuel, alors que ces faits relèvent indiscutablement du droit pénal. Ce détournement de fondement juridique traduit une méconnaissance, délibérée ou non, des obligations applicables aux fournisseurs de services d'hébergement lorsqu'ils ont connaissance d'une activité illicite.

Menace des plateformes.

Il convient également de signaler des comportements plus hostiles, observés chez certains hébergeurs, qui adoptent des postures dissuasives ou menaçantes à l'égard des signaleurs, invoquant de prétendues dispositions du Digital Services Act pour justifier leur inaction. Ces pratiques, fondées sur une interprétation erronée du cadre européen, compromettent la coopération indispensable entre acteurs privés et organismes de signalement et participent à la persistance d'une forme d'impunité numérique.

Devoir d'uniformisation. À l'inverse, les exemples positifs démontrent qu'une modération diligente et structurée est possible lorsque les acteurs assument pleinement leurs responsabilités. La systématisation des bonnes pratiques apparaît donc comme une priorité : suspension immédiate des contenus signalés lorsque leur illicéité est manifeste, réponse écrite et motivée aux notifications, archivage des échanges pour assurer la traçabilité, et coopération effective avec les autorités et les organismes de signalement. Ces principes, déjà posés par le Règlement sur les services numériques et la Loi pour la confiance dans l'économie numérique, devraient être considérés non comme des variables de gouvernance interne, mais comme des obligations de diligence et de loyauté inhérentes à la fourniture de services numériques. Une modération rigoureuse, rapide et transparente constitue aujourd'hui l'un des leviers essentiels de la lutte contre les cyberviolences sexistes et sexuelles. Elle garantit la mise en œuvre concrète des droits fondamentaux à la dignité, à la vie privée et à la sécurité des personnes dans l'espace numérique et conditionne, en dernière analyse, la crédibilité de l'ensemble du cadre juridique qui les protège.

Infographie

Loi sur la liberté de la presse du 29 juillet 1881
Répression de la diffamation, de l'injure et de la provocation à la haine

1881

Convention européenne des droits de l'homme (entrée en vigueur 1953)
Adoption de la Convention européenne des droits de l'homme par le Conseil de l'Europe. Elle protège les droits de l'homme et les libertés fondamentales, notamment la vie privée ou la liberté d'expression.

1950

2000

Convention de Budapest sur la cybercriminalité (entrée en vigueur 2004)
Premier instrument international de lutte contre les infractions informatiques (accès frauduleux, atteinte aux systèmes).

2001

Loi n° 2004-1486 du 30 décembre 2004
Renforcement de la lutte contre les propos discriminatoires à caractère sexiste ou homophobe. Introduction d'une circonstance aggravante en cas d'injure ou de diffamation à caractère discriminatoire, notamment à raison du sexe, de l'orientation sexuelle, de l'identité de genre ou du handicap.

2004

2011

Loi n° 2010-769 du 9 juillet 2010
Reconnaissance juridique des violences psychologiques et morales, notamment dans le cadre conjugal. Elle renforce la protection et la prise en charge des victimes et pose les bases pour prendre en compte certaines formes de harcèlement pouvant être amplifiées par le numérique.

2010

2014

Loi n° 2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les hommes
Intégration de disposition visant à mieux prévenir et sanctionner les discriminations, le harcèlement et certaines formes d'atteintes aux droits des femmes.

Règlement général sur la protection des données (RGPD)
Harmonisation des règles de protection des données personnelles dans l'Union européenne, en donnant aux individus un contrôle accru sur leurs informations et en imposant des obligations strictes aux responsables de traitement.

2016

Digital Services Act (DSA)
Adoption du *Digital Services Act* qui modernise le cadre des services numériques en imposant aux plateformes plus de transparence et des obligations de retrait des contenus illicites. Il prévoit des règles adaptées à la taille des acteurs et des mécanismes de signalement tout en protégeant les droits des utilisateur·ices dans l'Union européenne.

2022

Règlement établissant des règles harmonisées concernant l'intelligence artificielle (IA Act)
Régulation des produits d'intelligence artificielle qui sont commercialisés sur le marché européen.

2024

1948

Déclaration des Droits de l'Homme et du Citoyen
Adoption de la Déclaration des Droits de l'Homme et du Citoyen, premier instrument international de protection des droits humains.

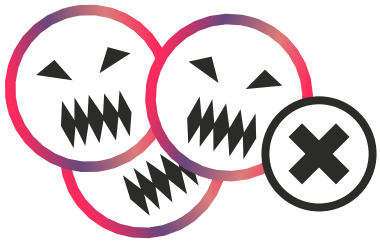
Charte des droits fondamentaux de l'Union européenne
Adoption de la Charte des droits fondamentaux par l'Union européenne, qui regroupe l'ensemble des droits civils, politiques, économiques et sociaux des personnes, notamment le respect de la dignité, de la vie privée, de l'égalité et de l'accès à la justice.

2004

Loi pour la confiance dans l'économie numérique (LCEN)
Création d'un cadre juridique régissant les services et les acteurs du numérique, en encadrant notamment les responsabilités des hébergeurs et des éditeurs de contenus, les obligations de retrait des contenus illicites et les modalités de coopération avec les autorités.

2006

Arrêt Erbakan c. Turquie, Cour européenne des droits de l'Homme
Validation par la Cour européenne des droits de l'Homme des restrictions à la liberté d'expression pour lutter contre les discours de haine.



Convention d'Istanbul (entrée en vigueur 2014)
Reconnaît les violences faites aux femmes comme une violation des droits humains. Inclut les violences psychologiques et le harcèlement.

2016

Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
Instauration de nouvelles dispositions pour lutter contre la diffusion non consentie de contenus à caractère sexuel (article 226-2-1 du Code pénal).

2018

Loi n°2018-703 du 3 août 2018
Renforcement la lutte contre les violences sexuelles et sexistes en élargissant la définition du harcèlement et en créant l'infraction d'outrage sexiste (R625-8-3 du Code pénal). Elle incrimine également l'upskirting ou captation d'images impudiques (226-3-1 du Code pénal).

2023

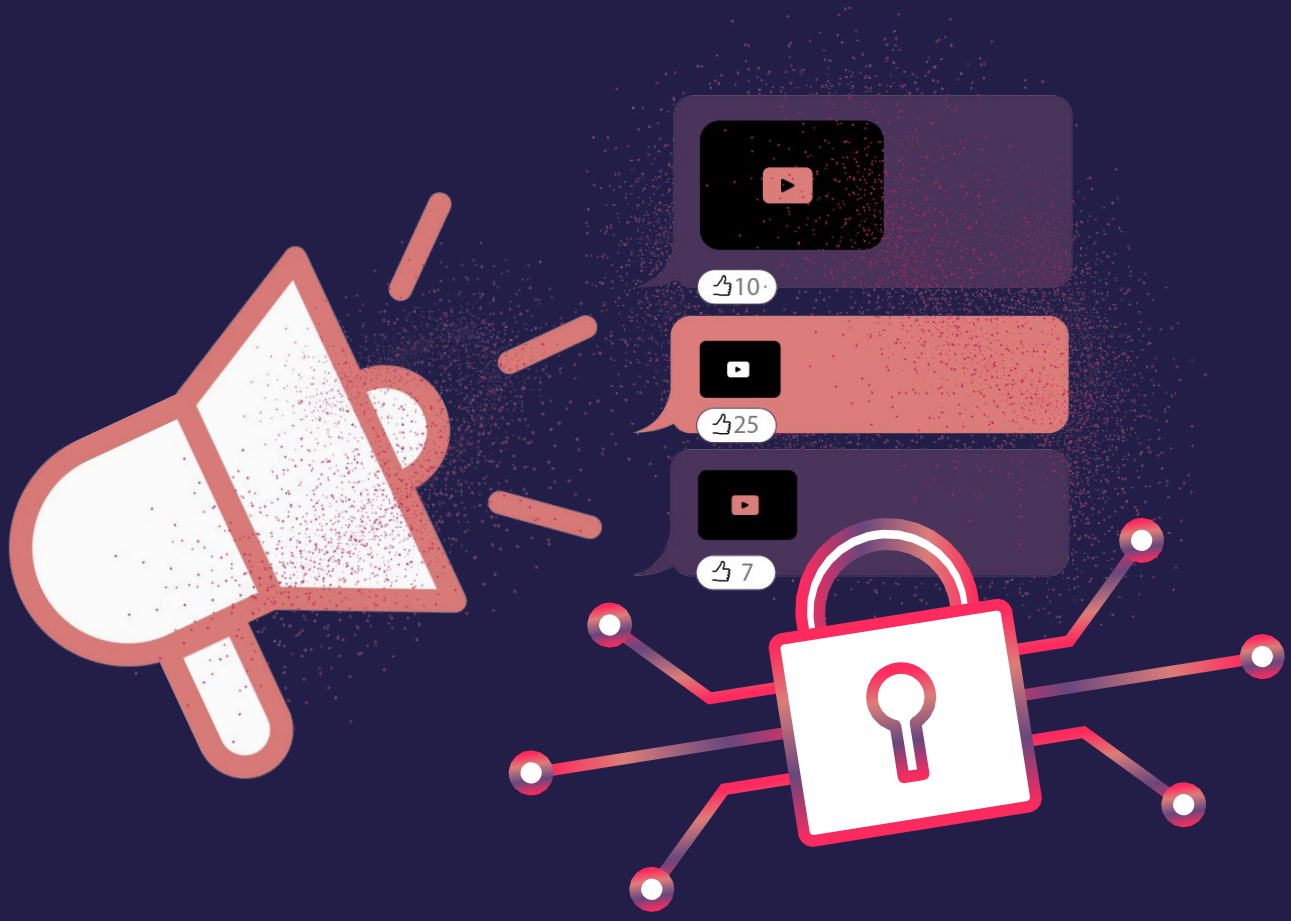
Loi n°2023-22 du 24 janvier 2023 visant à mieux lutter contre les violences intrafamiliales et sexistes
Elle élève l'outrage sexiste au rang de délit (222-33-1-1 du Code pénal) avec amende et tribunal compétent, et crée l'infraction de doxing (223-1-1 du Code pénal)

2024

Directive sur la lutte contre la violence à l'égard des femmes
Intégration explicite des violences numériques (partage non consenti d'images intimes, cyberharcèlement, incitation à la violence ou la haine envers les femmes).

2024

Loi pour Sécuriser et réguler l'espace numérique (SREN)
Renforcement de la protection des internautes contre la haine en ligne, le cyberharcèlement et les deepfakes, en responsabilisant plateformes et utilisateurs et en alignant le droit français sur le DSA. Elle crée l'incrimination spécifique de la sextorsion (312-10 du Code pénal).



IV. RECOMMANDATIONS

Documenter les cyberviolences sexistes et sexuelles ne suffit pas : il faut transformer la manière dont notre société les comprend, les prévient et y répond. Tel est l'objet de ces recommandations. Elles engagent les pouvoirs publics – administrations centrales comme collectivités territoriales –, les plateformes numériques et les institutions européennes ; mais elles appellent aussi le monde éducatif, les professionnel·les de santé, du social et de la justice, les chercheur·euses, les structures associatives et, plus largement, chacun·e d'entre nous. Faire reculer ces violences suppose en effet une réponse à la fois publique, collective et ancrée dans le quotidien. Organisées en sept leviers complémentaires – éduquer, signaler, accompagner, mesurer, responsabiliser, innover et faire évoluer le droit –, elles poursuivent un même horizon : reconnaître ces violences pour mieux les prévenir, les nommer et les réparer.

1. Prévenir les cyberviolences par l'éducation et l'information

Les cyberviolences sexistes et sexuelles prolongent dans l'espace numérique des rapports de domination qui traversent toute la société : les prévenir suppose donc d'agir aussi, en amont, sur leurs déterminants sociaux. Or la connaissance du grand public demeure superficielle – si 99 % des répondant·es à la Grande Enquête savent ce qu'est le cyberharcèlement, seul·es 38 % identifient le grooming et 24 % le doxxing. La prévention doit donc commencer tôt, nommer précisément les violences et s'appuyer sur les associations, que seules 4 % des victimes ont pourtant sollicitées.

Recommandation	Acteur·ices concerné·es
1.1 Prévenir les cyberviolences dès le plus jeune âge par l'éducation à la vie affective, relationnelle et à la sexualité (EVARS). Mettre en œuvre l'EVARS de manière effective et y intégrer, dès le plus jeune âge, les pratiques et usages numériques.	État, Éducation nationale
1.2 Déployer de grandes campagnes nationales de sensibilisation et d'information. Financées à la hauteur des ambitions (campagnes à 360°, présence dans l'espace public et sur les réseaux), elles couvrent la réduction des risques, la protection des données, les risques judiciaires encourus par les auteurs et l'accès aux droits des victimes (recours auprès des plateformes, plainte, soins). Toucher en priorité les publics les plus éloignés, là où les inégalités sociales et territoriales creusent la fracture numérique.	État, collectivités territoriales
1.3 Rendre visibles et financer durablement les dispositifs associatifs existants. Le maillage associatif spécialisé demeure largement méconnu des victimes : sa visibilisation par les pouvoirs publics, autant que la pérennisation de son financement, conditionnent l'accès des personnes concernées à un accompagnement adapté, notamment dans une perspective féministe pour les femmes et les filles. Associer ces structures à la conception des campagnes et soutenir leurs travaux d'observation, de recherche et d'action.	Administrations centrales, collectivités territoriales

48 %

des victimes et du grand public ne se sentent pas suffisamment informé·es sur les cyberviolences sexistes et sexuelles.

2. Un signalement simple, interopérable et suivi d'effets

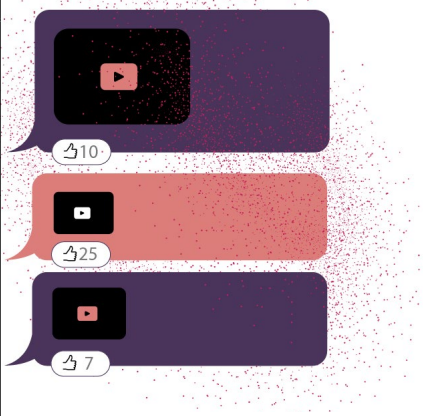
Signaler doit être simple, accessible et suivi d'effets. Or les fenêtres institutionnelles demeurent limitées et parfois mal organisées : certaines formes de cyberviolences n'y trouvent aucun interlocuteur identifié, et un contenu retiré d'une plateforme réapparaît ailleurs, faute de mécanisme empêchant sa remise en ligne. Cette complexité décourage les démarches – seules 12 % des victimes déposent plainte. Le signalement doit devenir un droit effectif, lisible et coordonné entre les services.

Recommandation	Acteur·ices concerné·es
2.1 Rendre le signalement réellement accessible et transparent. Appliquer des standards d'ergonomie et de transparence du traitement, garantir une décision motivée, des voies de recours compréhensibles et une revue humaine systématique dans les cas de cyberviolences sexuelles.	Plateformes, régulateur
2.2 Faire de la conservation des preuves un droit effectif pour la victime. L'obligation légale de conservation des contenus illicites pèse sur les plateformes, mais elle ne garantit pas que la victime puisse accéder aux preuves la concernant. Au-delà de l'horodatage et de la traçabilité dès le signalement, reconnaître à la victime un droit d'accès à ces éléments conservés, ainsi qu'un canal sécurisé de transmission à la justice et aux associations habilitées, afin qu'elle ne porte plus seule la charge de documenter les faits. De surcroît, le coût relatif au constat d'huissier continue d'être supporté par les victimes alors même que les plateformes devraient jouer un rôle dans l'authentification des preuves numériques.	Plateformes, État
2.3 Élargir et harmoniser les critères de signalement. Y intégrer les cyberviolences sexistes et sexuelles, en recherchant l'équilibre entre exhaustivité des catégories et simplicité d'usage, et en harmonisant ces catégories entre plateformes.	Plateformes, régulateur
2.4 Associer les structures spécialisées comme interlocutrices régulières de la régulation du numérique. Leur connaissance fine du terrain et leur expertise – détection, accompagnement, qualification des violences – gagnent à être pleinement mobilisées en instaurant un dialogue continu avec les plateformes et les régulateurs sur les politiques de modération et de prévention.	Plateformes, régulateurs, société civile

Recommandation	Acteur·ices concerné·es
2.5 Promouvoir l'interopérabilité entre plateformes comme un levier de lutte contre les cyberviolences. Une interopérabilité accrue des services numériques améliorerait les parcours de signalement, faciliterait la détection proactive des contenus, permettrait aux internautes de circuler d'une plateforme à l'autre sans y perdre leurs protections, et renforcerait ainsi leur pouvoir d'agir face aux violences.	État, Éducation nationale
2.6 Renforcer la coopération entre structures spécialisées et autorité judiciaire. Organiser une collaboration concrète, notamment dans le recueil et la conservation des preuves et, le cas échéant, par une participation des associations au contentieux aux côtés des victimes. Adapter la recevabilité des associations aux violences numériques en modifiant le code de procédure pénale afin de permettre aux associations spécialisées dans la lutte contre les violences sexistes, sexuelles, discriminatoires ou numériques de se constituer partie civile pour les infractions commises au moyen des technologies numériques. Cette adaptation est nécessaire afin d'éviter que les nouvelles infractions créées pour répondre aux violences en ligne – diffusion non consentie de contenus intimes, *deepfakes* pornographiques – demeurent exclues des régimes de recevabilité applicables aux associations, faute d'avoir été expressément ajoutées aux listes d'infractions prévues par le code de procédure pénale.	État, collectivités territoriales

66 %

des diffusions de contenus intimes ont lieu via une messagerie privée – un espace où la visibilité vis à vis de l'efficacité des dispositifs de signalement est largement entravée.



3. Garantir aux victimes un accueil compétent et un accompagnement digne

Prendre en charge une victime, c'est d'abord lui offrir un accueil compétent et bienveillant. Les données de la Grande Enquête disent l'inverse : près de 40 % des victimes qui ont fait la démarche se confier se sont senties mises en cause ou blâmées, et une victime mineure sur trois ignorait même que le dépôt de plainte était possible. Accompagner suppose des professionnel·les formé·es, un parcours judiciaire lisible et des ressources clairement identifiées, mobilisant de concert les expertises relatives au genre, aux violences sexuelles et au numérique.

34 %

des victimes se sont senties écoutées et aidées lors de leur dépôt de plainte – à peine plus d'une sur quatre parmi les victimes de diffusion non consentie.

Recommandation	Acteur·ices concerné·es
3.1 Former l'ensemble des professionnel·les. Santé, justice, police, social, éducation : instaurer une formation structurée, initiale et continue. Intégrer les violences en ligne à la formation initiale obligatoire des policier·es, gendarmes et magistrat·es aux violences sexistes et sexuelles ; prévoir une sensibilisation annuelle aux usages numériques ; s'assurer que les référent·es « violences faites aux femmes » en commissariat et gendarmerie sont formé·es aux CVSS y compris sur les aspects techniques ; rendre obligatoire la formation des professionnel·les de l'Éducation nationale.	État (santé, justice, intérieur, éducation)
3.2 Améliorer l'accueil lors du dépôt de plainte. Prendre systématiquement en compte la dimension numérique lors des auditions pour violences conjugales (cybersurveillance, cyberharcèlement, menaces de diffusion d'images intimes), comme le propose le Centre Hubertine Auclert. Réaffirmer l'obligation de recevoir les plaintes visant des cyberviolences (article 15-3 du code de procédure pénale).	Police, gendarmerie, justice
3.3 Renforcer le suivi judiciaire. Sur le modèle allemand, permettre aux tribunaux d'ordonner à un·e expartenaire la suppression de tout contenu intime sur demande de la victime. Renforcer les moyens du parquet national de lutte contre la haine en ligne. Développer des prises en charge alternatives des auteurs (cellules spécialisées, ateliers, programmes de responsabilisation).	Justice, parquet
3.4 Créer une plateforme de référence recensant l'ensemble des ressources. Dispositifs juridiques, associations d'accompagnement, conseils de sécurisation en ligne : offrir conseils juridiques et techniques, accompagnement psychologique et social, en réunissant des compétences encore rarement associées – celles du genre, des violences sexuelles et du numérique.	État, associations

4. Ce qui n'est pas mesuré reste impuni

On ne prend en charge que ce que l'on mesure – et ce rapport est né du manque d'études exhaustives sur ces violences. Deux ans après l'entrée en vigueur du DSA, les rapports de transparence des plateformes restent peu harmonisés et l'accès effectif des chercheur·euses aux données demeure difficile, laissant la société civile documenter ces phénomènes face à des acteurs privés puissants et souvent peu enclins à la transparence.

Recommandation	Acteur·ices concerné·es
4.1 Produire et financer de grandes enquêtes nationales et européennes. Sur les cyberviolences, notamment à caractère discriminatoire, avec des indicateurs publics obligatoires et ventilés (genre, âge, type de violence) et la collecte de données intersectionnelles, les groupes minorisés étant les plus exposés.	État, Union européenne, recherche
4.2 Exiger des plateformes des statistiques standardisées. Harmoniser les rapports de transparence et de risques systémiques du DSA autour d'indicateurs obligatoires (délais moyens, taux de retrait, taux d'erreur, taux de récidive, issue des recours), ventilés au minimum par type de violence et selon que les victimes sont mineures ou majeures. Le rôle de pilotage de la Commission européenne est ici déterminant.	Union européenne (DSA), plateformes
4.3 Rendre effectif l'accès des chercheur·euses aux données. Garantir un accès effectif et gratuit, y compris au monde associatif, pour documenter les risques systémiques, évaluer la modération et comprendre les dynamiques de viralité. Lever les difficultés persistantes de mise en œuvre de l'article 40 du DSA, qui conditionne cet accès.	Union européenne (DSA, art. 40), plateformes

79 %

des victimes déclarent être exposées à au moins une forme de discrimination – d'où la nécessité de données ventilées et intersectionnelles.

5. La sûreté en ligne est une obligation des plateformes, pas un effort des victimes

La sécurité des internautes n'est pas optionnelle : c'est une obligation légale, pas un effort à la charge des victimes. L'étude comparée des conditions d'utilisation de douze très grandes plateformes révèle pourtant une prise en compte inégale des cyberviolences de genre, alors que plus des trois quarts des victimes de cyberviolences sexuelles sont des femmes, et la motivation des décisions de modération y reste l'exception. La protection doit être intégrée à l'architecture même des services.

Recommandation	Acteur·ices concerné·es
5.1 Imposer des paramètres protecteurs par défaut. Santé, justice, police, social, éducation : instaurer une formation structurée, initiale et continue. Intégrer les violences en ligne à la formation initiale obligatoire des policier·es, gendarmes et magistrat·es aux violences sexistes et sexuelles ; prévoir une sensibilisation annuelle aux usages numériques ; s'assurer que les référent·es « violences faites aux femmes » en commissariat et gendarmerie sont formé·es aux CVSS y compris sur les aspects techniques ; rendre obligatoire la formation des professionnel·les de l'Éducation nationale.	Plateformes
5.2 Faire appliquer les bonnes pratiques de modération. S'appuyer sur les lignes directrices de la Commission européenne au titre du DSA et systématiser les pratiques déjà éprouvées par les plateformes les plus diligentes : suspension préventive des contenus dès leur signalement (mise en quarantaine jusqu'à décision), accusé de réception et décision motivée et traçable, sans imposer aux victimes de démarches disproportionnées. Renforcer les mécanismes de retrait rapide des images intimes non consensuelles déjà signalées, jusqu'à décision définitive, notamment par le recours proportionné aux empreintes numériques pour détecter les réapparitions d'un même contenu, sans affaiblir le chiffrement de bout en bout ni créer d'obligation générale de surveillance des communications privées.	Plateformes, Commission européenne
5.3 Concilier éthique et sécurité dans la détection des contenus. Recueillir systématiquement le consentement éclairé des victimes lorsque leurs images alimentent des bases de détection de contenus intimes non consentis, afin de ne pas reproduire une logique d'appropriation de leur corps. Le dispositif français Disrupt, développé par Point de Contact – empreintes générées à la demande de la victime, examen humain, base hébergée en France – illustre une approche respectueuse des droits des personnes, qu'il conviendrait de généraliser.	Plateformes, régulateurs

5.4 Faire contribuer les grandes plateformes à la réparation des dommages, au nom du principe de responsabilité. Si le signalement et le retrait des contenus demeurent essentiels, ils ne sauraient à eux seuls réparer les préjudices subis. Au nom du principe de responsabilité, une contribution pérenne des très grandes plateformes – par exemple par l'affectation d'une part des sanctions financières prévues par le *Digital Services Act* – permettrait d'alimenter un fonds dédié à la prise en charge des victimes, à la recherche indépendante, à la formation et à la prévention.	**État, Union européenne**

En récompensant les contenus polarisants, les algorithmes de recommandation transforment la misogynie en modèle économiquement rentable.

6. Penser le genre dès la conception des technologies de demain

Les technologies ne sont pas neutres : conçues majoritairement depuis des positions masculines, elles reconduisent les discriminations existantes, et l'IA générative industrialise déjà la violence – applications de « nudification » accessibles au grand public, *deepfakes sexuels*, détournement d'outils comme Grok début 2026. Les technologies à venir doivent intégrer, dès leur conception, la prévention des détournements et des discriminations.

Recommandation	Acteur·ices concerné·es
6.1 Intégrer la dimension de genre dès la conception des nouveaux outils. Rendre obligatoires, dès la phase de conception, des analyses d'impact sur les risques de cyberviolences, de fuite de données, de détournement des fonctionnalités et de reproduction des inégalités. Ces évaluations doivent associer des chercheur·ses spécialisé·es, des associations de terrain, ainsi que des femmes et des personnes minorées concernées par ces risques, afin que leur expertise participe directement à la conception, aux tests et aux paramètres de protection des outils et évaluent leur conformité en matière de protection des droits fondamentaux.	Concepteurs, Union européenne, État
6.2 Exiger des plateformes des statistiques standardisées. Harmoniser les rapports de transparence et de risques systémiques du DSA autour d'indicateurs obligatoires (délais moyens, taux de retrait, taux d'erreur, taux de récidive, issue des recours), ventilés au minimum par type de violence et selon que les victimes sont mineures ou majeures. Le rôle de pilotage de la Commission européenne est ici déterminant.	Union européenne (DSA), plateformes
6.3 Inscrire la supervision des plateformes dans un écosystème partenarial, du national à l'international. Favoriser des rapprochements transversaux entre pouvoirs publics, chercheur·euses, plateformes et société civile, afin de croiser les expertises et de superviser collectivement les pratiques de modération. Un tel dispositif – observatoire ou fonction équivalente – pourrait se déployer d'abord à l'échelle nationale, avant de s'articuler à des initiatives européennes et internationales.	État, recherche, société civile, UE

7 %

des contenus sexuels diffusés sans consentement sont issus de *deepfakes* – une part amenée à croître avec l'essor de l'IA générative.

7. Mobiliser le droit existant au plus près de la réalité des violences

Le droit offre déjà des leviers substantiels contre la diffusion non consentie de contenus intimes ; encore faut-il les mobiliser pleinement. Parce que cette infraction relève des atteintes à la vie privée, son appréciation gagne à s'ancrer dans la notion d'intimité autant que dans le seul caractère sexuel d'un contenu. Et parce que ces violences s'inscrivent massivement dans des relations de couple ou affectives, les circonstances aggravantes qui s'y rattachent doivent être

Recommandation	Acteur·ices concerné·es
7.1 Encourager une interprétation large du « caractère sexuel » des contenus. La diffusion non consentie relevant des atteintes à la vie privée, inviter le pouvoir judiciaire à mobiliser la notion d'intimité et à protéger également des contenus qui, sans être manifestement sexuels, portent atteinte à l'intimité de la personne lorsqu'ils sont divulgués.	Justice
7.2 Appliquer pleinement les circonstances aggravantes liées à la relation de couple. Sensibiliser les enquêteur·ices et les magistrat·es au fait que les auteurs de diffusion de contenus à caractère sexuel sont, le plus souvent, des partenaires amoureux·ses ou sexuel·les, et veiller à ce que les circonstances aggravantes correspondantes soient effectivement retenues – y compris lorsque la relation n'est ni mariée ni cohabitante, conformément à l'esprit de la loi qui vise aussi le PACS et le concubinage, ou que les violences sont commises entre mineur·es.	Enquêteur·ices, justice, législateur
7.3 Créer une infraction spécifique permettant de sanctionner l'envoi non consenti à une personne majeure de contenus sexuels explicites. Par message privé ou tout autre moyen de communication électronique tel que l'usage de technologie de Bluetooth, afin de sortir ces faits du seul régime contraventionnel des « messages contraires à la décence » et de reconnaître leur dimension d'atteinte sexuelle et d'intrusion dans l'intimité.	Législateur

76 %

victimes de diffusion non consentie de contenus intimes avaient entretenu une relation amoureuse ou de couple avec l'auteur des faits.

GLOSSAIRE

Algospeak
Langage codé (utilisation d'emojis, détournement orthographiques et phonétiques, euphémismes…) permettant de contourner la modération automatisée des plateformes.

Algorithme
Système automatisé permettant d'analyser les données issues de l'activité des internautes afin d'établir la pertinence de chaque contenu et ainsi de les filtrer, les organiser et les hiérarchiser.

Backlash
Le *backlash* désigne une réaction hostile aux avancées sociales, politiques ou culturelles obtenues par des groupes historiquement discriminés. Il s'agit d'un mouvement de rappel à l'ordre : lorsque des femmes, des personnes LGBTQIA+, des personnes racisées ou d'autres groupes minorisés gagnent en visibilité, en droits ou en capacité d'agir, des forces réactionnaires cherchent à restaurer l'ordre antérieur en délégitimant leurs revendications, en ridiculisant leurs prises de parole ou en les exposant à des formes renouvelées de violence. Dans les espaces numériques, ce contrecoup prend souvent la forme de cyberharcèlement, de campagnes de dénigrement, de menaces, de désinformation ou de violences sexistes et sexuelles coordonnées.

Bodycount
Le terme *bodycount*, littéralement « décompte des corps », désigne dans les discours contemporains le nombre de partenaires sexuel·les qu'une personne aurait eu·es au cours de sa vie. Il dissimule souvent une logique de contrôle moral et sexuel, en particulier lorsqu'il est appliqué aux femmes et aux personnes minorisées, transformant dès lors la sexualité en indice supposé de valeur, de respectabilité ou de disponibilité. Dans cette perspective, le terme bodycount devient un outil de jugement et de disqualification misogyne.

Body-shaming
Le *body-shaming* désigne les pratiques consistant à humilier, dévaloriser ou disqualifier une personne en raison de son apparence physique, de son poids, de sa taille, de sa morphologie, de son âge, de sa pilosité, de sa couleur de peau, de son handicap visible ou de toute autre caractéristique corporelle. Il repose sur des normes esthétiques et sociales qui hiérarchisent les corps.

Boycott
Initiative désormais principalement numérique visant à boycotter – ne plus donner de crédit, d'argent et de visibilité – à une personne physique ou morale (entreprise, association, etc) à partir de divers motifs liés par exemple à des accusations de violences sexuelles, de pollution, de discriminations, de soutien à des guerres et génocides, de maltraitances animales, etc.

Compte fisha
Compte sur un réseau social – ou groupe/canal sur une messagerie instantanée – dédié à la publication de contenus sexuels ou intimes de personnes n'ayant pas consenti à cette diffusion. Celle-ci peut s'accompagner d'informations personnelles (doxing) comme les réseaux sociaux, le numéro de téléphone, l'adresse, etc.

Contenu pédocriminel
Contenu représentant, mettant en scène ou sexualisant une personne mineure, réelle, supposée ou présentée comme telle, qu'il s'agisse d'une photographie, d'une vidéo, d'un dessin, d'un montage, d'une image altérée ou d'un contenu fabriqué par intelligence artificielle.

Cyberarabisogynie
Cyberviolence s'exerçant à l'encontre des femmes arabes en raison de leur genre et de leur origine.

Cyberautodéfense féministe
Ensemble de pratiques, savoirs et stratégies individuelles ou collectives visant à prévenir, limiter et contrer les violences numériques sexistes et sexuelles, ainsi qu'à résister aux rapports de domination qui se prolongent dans les espaces numériques.

Cybercontrôle coercitif
Le cybercontrôle coercitif désigne l'ensemble des comportements répétés par lesquels une personne utilise les outils numériques pour surveiller, intimider, isoler ou contraindre une victime, limiter son autonomie, l'éloigner de ses proches ou la priver de ressources matérielles, sociales et psychologiques. Il s'agit d'une stratégie globale d'emprise visant à maintenir la victime dans un état de dépendance, de peur ou de contrôle permanent.

Cyberdiscrimination
Toute discrimination exercée, reproduite ou amplifiée par des outils et espaces numériques, qu'elle relève de la conception même des technologies – par exemple des systèmes de reconnaissance faciale moins fiables pour les personnes racisées ou des algorithmes invisibilisant certains corps – ou de comportements discriminatoires en ligne, comme des insultes transphobes, racistes, sexistes, validistes ou grossophobes.

Cyberespace
Le cyberespace désigne l'ensemble des espaces, services et infrastructures numériques dans lesquels les personnes communiquent, interagissent, travaillent, se divertissent, s'informent ou organisent leur vie quotidienne. Il comprend notamment les réseaux sociaux, les messageries privées, les forums, les plateformes de partage de contenus, les jeux en ligne, les applications mobiles, les sites web, mais aussi l'ensemble des environnements rendus accessibles via les smartphones, ordinateurs, tablettes et objets connectés.

Cybergrossophobie
Ensemble des violences, propos, discrimination ou comportements commis, diffusés ou amplifiés dans les espaces numériques à l'encontre de personnes grosses ou perçues comme telles, en raison de leur poids, de leur morphologie ou de leur apparence corporelle.

Cyberharcèlement
Le cyberharcèlement désigne toute forme de harcèlement commise dans le cyberespace ou au moyen d'outils numériques, qu'il s'agisse de harcèlement moral, sexuel, scolaire, discriminatoire, professionnel ou conjugal.

Cyberharcèlement sexuel
Cyberharcèlement à connotation sexuelle ou sexiste pouvant par exemple se manifester par l'envoi de messages ou d'images obscènes et peut aller jusqu'au menaces de viol.

CyberLGBTQIA+phobies
Cyberviolence s'exerçant à l'encontre des personnes s'identifiant ou identifiées comme appartenant à la communauté LGBTQIA+ en raison de leur identité de genre et/ou de leur orientation sexuelle.

Cybermisogynoir
Cyberviolence s'exerçant à l'encontre des femmes noires en raison de leur genre et de leur couleur de peau.

Cyberouting
Cyberviolence consistant à révéler en ligne l'orientation sexuelle ou l'identité de genre réelle ou supposée d'une personne sans son consentement.

Cybersécurité
Ensemble des pratiques, outils et mesures visant à protéger les personnes, les données, les comptes, les appareils et les systèmes numériques contre les intrusions, les détournements, les vols d'informations, les surveillances non consenties ou les usages malveillants.

Cybersexisme
Le cybersexisme désigne l'expression du sexisme dans le cyberespace, à travers des propos, comportements, représentations ou discriminations sexistes produits, diffusés ou facilités par des outils numériques : réseaux sociaux, messageries, SMS/MMS, jeux en ligne, plateformes de contenus, objets connectés ou autres dispositifs relevant des technologies numériques.

Cybervalidisme
Le cybervalidisme désigne l'expression du validisme dans le cyberespace : propos, comportements, représentations ou discriminations visant les personnes en situation de handicap au moyen d'outils numériques. Il repose sur le fait d'ériger les personnes sans handicap – donc valides – en norme sociale.

Cyberviolence
Violence commise au sein de l'espace numérique ou au moyen d'outils et de technologies numériques.

Cyberviolence conjugale
Violence exercée par un·e conjoint·e, ex-conjoint·e ou partenaire au moyen d'outils numériques, dans une logique de surveillance, de contrôle, d'intimidation, d'emprise ou de harcèlement, y compris après la séparation.

Cyberviolence sexiste et sexuelle
Les cyberviolences sexistes et sexuelles désignent l'ensemble des violences de genre commises, facilitées ou amplifiées par des outils numériques, qu'elles aient lieu sur Internet, les réseaux sociaux, les messageries, les jeux vidéo, les plateformes de contenus, via les objets connectés ou toute autre technologie numérique.

Dickpic
Une *dickpic* désigne l'envoi d'une photographie de pénis, généralement par voie numérique. Lorsqu'elle est envoyée sans consentement préalable, elle constitue une intrusion sexuelle : elle impose à la personne destinataire une image intime qu'elle n'a pas sollicitée et participe d'une forme d'exhibitionnisme numérique.

Deepfake
Un *deepfake* désigne un contenu visuel ou sonore généré ou manipulé au moyen de systèmes d'intelligence artificielle, de manière à faire croire qu'une personne, un objet, un lieu, une entité ou un événement réel apparaît, dit ou fait quelque chose qui n'a pas eu lieu. Il peut prendre la forme d'une image, d'une vidéo ou d'un enregistrement audio particulièrement vraisemblable. Les *deepfakes* peuvent être utilisés pour produire ou diffuser de faux contenus à caractère sexuel impliquant des personnes qui n'y ont jamais consenti.

Diffamation
Imputation d'un fait précis portant atteinte à l'honneur ou à la considération d'une personne identifiable.

Diffusion non consentie de contenus sexuels
La diffusion non consentie de contenus sexuels désigne le fait de transmettre, publier, partager ou rendre accessible à des tiers un contenu intime ou à caractère sexuel – photographie, vidéo, enregistrement sonore, capture d'écran ou tout autre support – sans le consentement de la personne représentée ou identifiable. Le caractère consenti de la prise ou de l'envoi initial du contenu ne vaut jamais consentement à sa conservation, à sa transmission ou à sa diffusion.

Domotique
La domotique désigne l'ensemble des technologies permettant d'automatiser, programmer ou contrôler à distance les équipements d'un logement, comme l'éclairage, le chauffage, les volets, les caméras, les alarmes, les serrures ou les appareils connectés.

Doxing
Le *doxing* désigne la diffusion non consentie d'informations personnelles permettant d'identifier, de contacter ou de localiser une personne, l'exposant ainsi à des risques de harcèlement, de menaces ou d'atteinte à sa sécurité, à sa vie privée, à ses proches ou à ses biens.

Empouvoirement
L'empouvoirement désigne le processus par lequel une personne ou un groupe renforce sa capacité d'action, de décision et d'autonomie, en acquérant les ressources, la confiance et la légitimité nécessaires pour reprendre du pouvoir sur sa vie et sa place dans la société.

Féminismes
Mouvements de lutte pour les droits des femmes et minorités de genre et contre les violences sexistes et sexuelles, au pluriel car il existe une diversité d'approches et de méthodes.

Grooming
Le *grooming* désigne la prise de contact et la manipulation progressive d'un·e mineur·e par un adulte, le plus souvent en ligne, afin d'obtenir des contenus sexuels, d'exercer une emprise ou de préparer la commission de violences sexuelles, en ligne ou hors ligne.

Happy-slapping
Le *happy-slapping* désigne le fait de filmer une agression physique et/ou sexuelle ou une humiliation commise contre une personne, puis de diffuser ou partager ces images, notamment en ligne.

HaChage
Procédé technologique permettant de transformer une image (photo, vidéo, contenu virtuel) en signature numérique unique. Cette technique permet de stocker uniquement cette empreinte et non le contenu en lui-même.

Hébergeur
Entreprise qui fournit l'hébergement des données circulant sur Internet. En d'autres termes, ces structures permettent de stocker sur des serveurs l'ensemble des contenus et données numériques.

Identité de genre
L'identité de genre désigne l'expérience intime et personnelle qu'une personne a de son propre genre. Elle peut correspondre au fait de se reconnaître comme femme, homme, les deux, ni l'un ni l'autre, ou de se situer autrement dans le spectre du genre. Cette identité peut correspondre ou non au genre socialement associé au sexe assigné à la naissance.

Incitation à la haine sexiste
Fait de provoquer par des propos ou des actes à la haine, à la violence, à la discrimination envers les femmes.

Injure
Parole, écrit ou expression de la pensée adressée à une personne dans l'intention de la blesser ou de l'offenser. L'injure peut s'appuyer sur des préjugés sexistes, LGBTQIA+phobes, racistes, validistes, xénophobes, etc.

Intelligence artificielle
L'intelligence artificielle désigne un ensemble de systèmes informatiques capables d'accomplir des tâches qui nécessitent habituellement des capacités associées à l'intelligence humaine, comme analyser des informations, reconnaître des formes, produire du texte, des images ou du son, formuler des recommandations, prédire des comportements ou prendre des décisions automatisées. Ces systèmes fonctionnent à partir de modèles entraînés sur des données et peuvent produire des résultats influençant des environnements physiques ou numériques.

Intersectionnalité
L'intersectionnalité désigne l'articulation de plusieurs rapports de domination dans l'expérience d'une même personne ou d'un même groupe. Développé par Kimberlé Crenshaw en 1989, ce concept permet de comprendre que les discriminations liées notamment au genre, à la race, à la classe, au handicap ou à l'orientation sexuelle ne s'additionnent pas seulement, mais produisent des formes spécifiques d'inégalités et de violences.

Masculinismes
Les masculinismes désignent un ensemble de mouvances antiféministes fondées sur l'idée que les hommes seraient menacés par les femmes, le féminisme ou les politiques d'égalité. Elles s'appuient souvent sur le récit d'une « crise de la masculinité » et cherchent à maintenir ou restaurer la domination masculine, en légitimant les hiérarchies de genre, le contrôle des femmes ou certaines formes de violence. Le pluriel permet de rendre compte de la diversité de ces discours, de la « complémentarité des sexes » aux théories de la manosphère comme le « 80/20 », la *red pill* ou les communautés incel.

Manosphère
Ensemble des communautés en ligne qui promeuvent de façon croissante des conceptions rigides et hostiles de la masculinité, tout en véhiculant l'idée fausse selon laquelle le féminisme et l'égalité des sexes se seraient construits au détriment des droits des hommes.

Menace
Manifestation de violence par laquelle il est signifié à une personne l'intention de lui faire du mal (ex : menace de diffusion de nudes).

Nude
Le mot *nude* désigne une image ou vidéo intime, généralement dénudée ou à caractère sexuel, produite ou partagée dans un cadre privé. Leur création ou leur envoi peut s'inscrire dans une relation consentie, de confiance ou de séduction. En revanche, leur conservation contre la volonté de la personne concernée, leur transmission à des tiers, leur menace de diffusion ou leur diffusion sans consentement constituent des formes de cyberviolences sexuelles.

Nudificateur
Un nudificateur est un outil, souvent fondé sur l'intelligence artificielle, permettant de modifier ou fabriquer une image ou une vidéo afin de faire apparaître une personne nue ou partiellement dénudée sans qu'elle l'ait été dans le contenu d'origine.

Outrage sexiste
Propos ou comportement à connotation sexuelle ou sexiste imposé à la victime et qui porte atteinte à sa dignité, l'intimide, la blesse, la met mal à l'aise ou l'humilie.

Proxénétisme numérique
Phénomène émergent renvoyant à l'utilisation des plateformes en ligne, des messageries chiffrées, des sites de rencontres ou encore des espaces de jeu en ligne pour recruter, piéger ou exploiter des personnes – souvent mineures – à des fins sexuelles.

Public-shaming
Humiliation publique d'une personne en ligne.

Revictimisation
La revictimisation désigne le fait, pour une personne ayant déjà subi une violence, d'être de nouveau exposée à une violence, similaire ou différente, à un moment ultérieur de son parcours.

Sexisme
Le sexisme désigne l'ensemble des représentations, propos, comportements, pratiques ou discriminations fondés sur l'idée d'une hiérarchie entre les sexes ou les genres. Il vise principalement les femmes et les personnes minorisées de genre, en raison de leur appartenance réelle ou supposée à un groupe de genre, et contribue à maintenir les inégalités, les stéréotypes et les rapports de domination.

Sextorsion
La sextorsion désigne une forme de chantage sexuel dans laquelle une personne menace d'exposer, de diffuser ou de rendre publics des contenus intimes afin d'obtenir de l'argent, d'autres images sexuelles, des actes sexuels ou une forme de soumission. Elle repose sur l'exploitation de la peur, de la honte et du risque social, et constitue une forme de violence sexuelle et psychologique.

Slut-shaming
Le *slut-shaming* désigne l'ensemble des pratiques qui consistent à juger, humilier ou disqualifier une personne – le plus souvent une femme ou une personne minorisée – en raison de sa sexualité réelle, supposée ou fantasmée. Il repose sur une police des corps et des désirs : certaines tenues, pratiques sexuelles, manières de se montrer, de parler ou d'exister sont alors utilisées pour remettre en cause la respectabilité, la crédibilité ou la valeur d'une personne. Le *slut-shaming* est une dispositif de contrôle visant à rappeler à l'ordre celleux qui s'écartent des normes attendues par l'ordre patriarcal.

Stalking
Le *stalking* désigne une forme de harcèlement répétée et intrusive consistant à surveiller, suivre ou traquer une personne, en ligne ou hors ligne, sans son consentement. Il peut notamment passer par l'observation de ses activités numériques, la collecte d'informations personnelles, les messages répétés ou l'usage de faux comptes.

Système de genre
Hiérarchie de considération et de pouvoir en fonction du genre des personnes. Dans le système de genre, les hommes cisgenres dyadiques (non intersexes) sont en haut de la pyramide et dominent les femmes cisgenres, les hommes transgenres, les personnes intersexes, les femmes transgenres, les personnes non-binaires et autres minorités de genre.

Tana
Terme initialement démocratisé par une chanson de Niska mentionnant la mannequin portugaise et cap-verdienne Ana Montana en transformant la fin de son nom 'tana' pour lui donner le sens de « pute »/« salope ». Une réappropriation du terme s'est faite par un mouvement en ligne pour s'affranchir du regard des hommes et rejoindre l'île de « Tanaland ».

Trend
Une *trend* désigne un format, un thème, un son, un geste, une blague, un défi ou un type de contenu qui se diffuse rapidement sur une plateforme et est massivement repris, imité ou détourné par les internautes, jusqu'à devenir une tendance identifiable.

Upskirting
L'*upskirting* désigne la captation non consentie d'images sous les vêtements d'une personne, notamment sous une jupe ou une robe, afin de photographier ou filmer son entrejambe, ses sous-vêtements ou ses parties intimes. Cette pratique réprimée par la loi constitue une atteinte à l'intimité et à l'autonomie corporelle de la personne visée.

Victim-blaming
Le *victim-blaming*, ou culpabilisation des victimes, désigne le fait d'attribuer à une victime la responsabilité des violences qu'elle a subies, en interrogeant ses comportements plutôt que ceux de l'agresseur. Il contribue à minimiser les violences, à renforcer l'impunité des agresseurs et à dissuader les victimes de demander de l'aide ou de dénoncer les faits.

Bibliographie.

I. Ouvrages

Bereni, L., Chauvin, S., Jaunait, A., & Revillard, A. (2020). *Introduction aux études sur le genre* (3e éd., coll. « Ouvertures politiques »). De Boeck.

Collet, I. (2025). *Le numérique est l'affaire de toutes*. Le Bord de l'eau.

Condomines, A., & Friedmann, E. (2019). *Cyberharcèlement - Bien plus qu'un mal virtuel*. Pygmalion.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*. St. Martin's Press.

Ferrari, P. (2023). *Formés à la haine des femmes*. Éditions du Seuil.

hooks bell, *La volonté de changer*, Éditions Divergences, 2021.

Lafourcade, M. (2025). *Démasculiniser la justice*. Éditions Les petites mains.

Lamy, S. (2024). *La terreur masculiniste*. Détour.

Mutombo, K., & Salmona, L. (2023). *Politiser les cyberviolences : une lecture intersectionnelle des inégalités de genre sur Internet*. Le Cavalier Bleu.

Salmona, L. (2025). *15 idées reçues sur les cyberviolences et le cyberharcèlement*. Le Cavalier Bleu.

Association #StopFisha : Outaik, H., Maclaren, S. C., Outaik, H., Bories, J., Pereira Diogo, L. , Gauvin Drillaud, L., Janvier, M., Haouari, S., Reynaud, L., & Pardo, R. (2021). *Combattre le cybersexisme*. Éditions Leduc.

Zuboff, S. (2022). *L'âge du capitalisme de surveillance*. Zulma.

II. Articles scientifiques, chapitres et travaux universitaires

Albrengues, A., & Lu, L. (2025, octobre). *Weight of gender in artificial intelligence models' implementation in the European Union non-discrimination laws.* ELSP.

Blaya, C. (2013). *Introduction.* Dans *Les ados dans le cyberespace : prises de risque et cyberviolence* (p. 9-12). De Boeck Supérieur.

Blaya, C. (2018). Le cyberharcèlement chez les jeunes. *Enfance*, 2018(3), 421-439. https://doi.org/10.3917/enf2.183.0421

Cai, J., Chowdhury, S., Zhou, H., & Wohn, D. Y. (2023). Hate raids on Twitch: Understanding real-time human-bot coordinated attacks in live streaming communities. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2), Article 342, 1-28. https://doi.org/10.1145/3610191

Crenshaw, K. W. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stanford Law Review*, 43(6), 1241-1299.

Daniele, F., Bucher, L., Servida, G., & Gilman, R. (2025, 17 décembre). Monetising misogyny: Engagement farming and the tactics behind incendiary online content. *Global Network on Extremism and Technology*.

Des Roches, A. (2025, octobre). *Sexy robots: A perpetuation of patriarchy*.

Détraz, S. (2016). Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple (commentaire de l'article 226-2-1 du Code pénal issu de la loi n° 2016-1321 du 7 octobre 2016). *Revue de science criminelle et de droit pénal comparé*, 2016(4), 741-753.

Ganesh, M. I., & Moss, E. (2022). Resistance and refusal to algorithmic harms: Varieties of "knowledge projects". *Media International Australia*, 183(1), 90-106.

Gibson, C., Olszewski, D., Brigham, N. G., Crowder, A., Butler, K. R. B., Traynor, P., Redmiles, E. M., & Kohno, T. (2024). *Analyzing the AI nudification application ecosystem*. arXiv. https://arxiv.org/abs/2411.09751

Gonseth, J. (2008). Stalking : une nouvelle figure de la clinique du traumatisme. *Revue Médicale Suisse, 4*(144), 472-475.

Guevara-Gómez, A., De Zárate-Alcarazo, L. O., & Criado, J. I. (2021). Feminist perspectives to artificial intelligence: Comparing the policy frames of the European Union and Spain. *Information Polity, 26*(2), 173-192.

Kelman, H. C. (1973). Violence without moral restraint: Reflections on the dehumanization of victims and victimizers. *Journal of Social Issues*, 29(4), 25-61. https://hckelman.scholars.harvard.edu/sites/g/files/omnuum10576/files/hckelman/files/Violence_1973.pdf

Lütz, F. (2022). Gender equality and artificial intelligence in Europe: Addressing direct and indirect impacts of algorithms on gender-based discrimination. *ERA Forum*.

Maoz, I., & McCauley, C. (2008). Threat, dehumanization, and support for retaliatory aggressive policies in asymmetric conflict. *Journal of Conflict Resolution, 52*(1), 93-116. http://www.jstor.org/stable/27638596

Mincke, M. (2021). *Le phénomène du Revenge Porn : entre reconnaissance et stigmatisation, le point de vue des victimes* [Mémoire de master, Université catholique de Louvain].

Morley, C., & Kuntz, P. (2019). Empowerment des femmes par les technologies numériques : pouvoir avec, pouvoir pour et pouvoir intérieur. *Terminal*, 125-126.

Morrigan, V. (2022). Patriarchal imaginaries beyond the human: "Sex" robots, fetish and fantasy in the domination and control of women. Dans K. Richardson & C. Odlind (dir.), *Man-made women: Social and cultural studies of robots and AI*. Palgrave Macmillan.

Parizot, R., & Perrier, J.-B. (2017). Chronique législative. *Revue de science criminelle et de droit comparé, 2017*(2), 378.

Pradhan, A., Erete, S., Chopra, S., Upadhyay, P., Sule, O., et al. (2025). "No, not that voice again!": Engaging older adults in design of anthropomorphic voice assistants. *Proceedings of the ACM on Human-Computer Interaction, 9*(2). [Liste complète des auteur·ices à compléter si disponible]

Rodríguez-Castro, Y., Martínez-Román, R., Alonso-Ruido, P., Adá-Lameiras, A., & Carrera-Fernández, M. V. (2021). Intimate partner cyberstalking, sexism, pornography, and sexting in adolescents: New challenges for sex education. *International Journal of Environmental Research and Public Health, 18*(4), Article 2181.

Uhl, C. A., Rhyner, K. J., Terrance, C. A., & Lugo, N. R. (2018). An examination of nonconsensual pornography websites. *Feminism & Psychology, 28*(1), 50-68. https://doi.org/10.1177/0959353517720225

Xenidis, R., & Senden, L. (2020). EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination. Dans U. Bernitz et al. (dir.), *General principles of EU law and the EU digital order* (p. 151-182) Kluwer Law International.

III. Rapports, études et enquêtes

Assemblée nationale. (2025, 4 septembre). *Rapport de la commission d'enquête sur les effets psychologiques de TikTok sur les mineurs.*

Bartoletti, I., & Xenidis, R. (2023). *Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination*. Conseil de l'Europe, Gender Equality Commission & CDADI.

University of Bedfordshire. (2011). *Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey*.

Equality Now. (2022). *A call for an intersectional feminist-informed universal declaration on digital rights.*

Equal Rights Trust. (2025). *Principles on equality by design in algorithmic decision-making.*

Féministes contre le cyberharcèlement & IPSOS. (2021, novembre). *Cyberviolence et cyberharcèlement : état des lieux d'un phénomène répandu* [Enquête conduite auprès de 1 008 Français·es âgé·es de 18 ans et plus].

Haut Conseil à l'Égalité entre les femmes et les hommes. (2017). *En finir avec l'impunité des violences faites aux femmes en ligne : une urgence pour les victimes.*

Haut Conseil à l'Égalité entre les femmes et les hommes. (2025, 22 janvier). *État des lieux du sexisme en France à l'heure de la polarisation* (Rapport n° 2024-01-22-STER-61).

Haut Conseil à l'Égalité entre les femmes et les hommes. (2025). *Violences faites aux femmes : mettre fin au déni et à l'impunité.*

Centre Hubertine Auclert. (2018). *Cyberviolences conjugales*. Centre Hubertine Auclert.

Centre Hubertine Auclert. (2025). *(Cyber)violences de genre chez les 11-18 ans : victimisations sexistes, sexuelles et LGBTphobes dans des collèges et lycées franciliens*. Centre Hubertine Auclert.

IPSOS & Association Mémoire traumatique et victimologie. (2019, février). *Les Français et les représentations sur le viol.*

Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche. (2023). *Repères et références statistiques 2023*. MESR-DEPP.

Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche. (2025, février). *Un programme ambitieux : éduquer à la vie affective et relationnelle, et à la sexualité.*

de Montaignac, M., Jolly, C., & Furic, P. (2025, mai). *Lutter contre les stéréotypes filles-garçons : quel bilan de la décennie, quelles priorités d'ici 2030 ?*.

Ministère chargé de l'Égalité femmes-hommes, Observatoire national des violences faites aux femmes. (2024, mars). Les violences au sein du couple et les violences sexuelles en France en 2022. *Lettre de l'Observatoire*, 19.

Panorama Global. (2023). *I didn't consent: A global landscape report on image-based sexual abuse*.

Poty, A. (2023). Les femmes restent très minoritaires dans les métiers de la transformation numérique et du développement durable. Dans *Emploi, chômage, revenus du travail. Insee Références, édition 2023*. Insee.

Qustodio. (2024, 19 août). *Apps through the ages: A Qustodio study on kids' tech use in the USA*.

Reset Australia & Institute for Strategic Dialogue. (2022, avril). *Algorithms as a weapon against women: How YouTube lures boys and young men into the "manosphere"*.

SKEMA Business School. (2026, 24 février). *CAC 40 : plus de femmes, mais toujours pas au sommet*. SKEMA Business School.

UNESCO & International Center for Journalists. (s. d.). *Enquête mondiale sur les violences en ligne à l'encontre des femmes journalistes* [Enquête auprès de plus de 1 200 journalistes].

UN Women. (2022). *Accelerating efforts to tackle online and technology-facilitated violence against women and girls*.

Yeung, K. (2019). *Responsibility and AI: A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework*. Conseil de l'Europe.

IV. Articles de presse et publications en ligne

Le Monde. (2023, 11 octobre). Affaire Griveaux : l'artiste russe Piotr Pavlenski condamné à une peine de six mois de prison ferme aménageable. *Le Monde*.

Le Parisien. (2017, 23 juin). Aude : le maire de Limoux s'excuse après la fuite d'une sex-tape. *Le Parisien*.

Melty. (2025, 7 octobre). Baghera victime de cyberharcèlement pendant le GP Explorer. *Melty*.

Melty. (2025, 17 septembre). Baghera Jones harcelée depuis son passage dans la vidéo du train de Squeezie. *Melty*.

Le Monde & Agence France-Presse. (2025, 6 octobre). La DJ Barbara Butch cible d'une nouvelle campagne de cyberharcèlement, selon la Ville de Paris. *Le Monde*.

Konbini. (2025, 20 décembre). « Beurette de luxe », « Beurette de Sciences Po » : Sarah Bouchamama témoigne. *Konbini*.

Libération. (2024, 23 novembre). Boycotter X, un dilemme plus complexe que prévu. *Libération*.

Condomines, A. (2017, 5 janvier). Cyberharcèlement et « raids » antiféministes sur le forum 18-25 de JeuxVideo.com : « cela a assez duré ». *TF1 Info*.

Courret, M. (2025, 21 mars). Elsa Bois, Léna Mahfouf, Chloé Gervais… : les compagnes de YouTubeurs, cibles constantes des masculinistes d'Internet. *Marie Claire*.

Croquet, P. (2024, 23 octobre). Exprimer le viol avec l'émoji violet, paradoxe et symbole de la libération de la parole sur les réseaux sociaux. *Le Monde*.

Dang, L. (2025, 17 janvier). « L'idée, c'est de créer une issue de secours pour la démocratie ». *Socialter*.

France Info. (2023, 25 novembre). Définition du masculinisme par Mélissa Blais. *France Info*.

Desmarais, A. (2025, 4 novembre). La France traite le cyberharcèlement différemment du reste de l'UE : voici d'autres affaires phares. *Euronews*.

Le Monde. (2014, 1er septembre). Des photos piratées de Jennifer Lawrence et plusieurs autres stars nues mises en ligne. *Le Monde*.

Courrier international. (2021, 13 août). Drame. L'ombre « incel » plane sur la tuerie de Plymouth, la pire depuis onze ans au Royaume-Uni. *Courrier international*.

Duffaut, M. (2024, 11 janvier). Depuis Elon Musk, Twitter/X a licencié plus d'un tiers de ses employés dans la modération et la sécurité. *Radio France*.

Forgar, S. (2024, 30 novembre). « Tarée », « morue », « journalope » : quand Salomé Saqué dénonce son cyberharcèlement. *Madame Figaro*.

Fourneau, L. (2023, 10 août). Qu'est-ce que le body count, une tendance sur TikTok au sexisme décomplexé. *20 Minutes*.

Gadedjisso-Tossou, E. E. (2023, 13 mars). Témoignage - Bénin : « Le cyberharcèlement m'a poussé au suicide », Majoie Houndji. *AfrikElles*.

Radio France. (2024, 17 décembre). L'affaire de cyberharcèlement du Gamergate. *France Inter*.

France Info. (2023, 13 janvier). La chanteuse Hoshi victime de cyberharcèlement homophobe : plusieurs suspects mineurs identifiés en plus de la personne renvoyée en procès. *France Info*.

Jezequel, M. (2025, 9 juin). Au Brésil, la misogynie en ligne est une affaire rentable. *Courrier international*.

Khomani, N. (2024, 14 août). JK Rowling and Elon Musk named in Imane Khelif cyberbullying lawsuit. *The Guardian*.

Le Monde. (2014, 24 mai). Le fils d'un réalisateur annonce « le jour du châtiment » et tue 6 personnes en Californie. *Le Monde*.

Leloup, D. (2025, 8 janvier). Meta assouplit fortement sa modération des contenus haineux sur Facebook ou Instagram. *Le Monde*.

Mariani, M. (2024, 20 juillet). Manon Lanza, seule face au sexisme de la Gen Z. *France Inter*.

Le Monde. (2025, 7 avril). « Meta » met fin à son programme de fact-checking aux États-Unis ce lundi. *Le Monde.*

RTL Info. (2025, 4 mars). « Je refuse de m'excuser d'avoir grandi » : Millie Bobby Brown dénonce le harcèlement médiatique dont elle est victime. *RTL Info*.

Murhula, C. (2022, 5 octobre). Tarana Burke, la lanceuse méconnue de #MeToo. *Le Monde*.

Le Monde & Agence France-Presse. (2024, 15 mars). Polémique Aya Nakamura aux JO : le parquet de Paris ouvre une enquête après un signalement de publications racistes visant la chanteuse. *Le Monde*.

Nasi, M. (2022, 24 mai). Les comptes « fisha » sur les réseaux sociaux, nouvelle plaie du cybersexisme. *Le Monde*.

Antidote Magazine. (2021, 20 avril). Pourquoi les masculinistes inondent certains comptes Instagram avec des émojis médaille ? *Antidote Magazine*.

Le Monde. (2025, 2 juillet). Projet d'attentat masculiniste déjoué : une première en France, où la menace « incel » est émergente. *Le Monde*.

Roney, E. (2025, 31 janvier). « Quand je vois la police, je tremble » : le double traumatisme de femmes victimes de violences qui portent plainte. *INDEX*.

Ronfaut, L. (2021, 14 mai). Deepfake : avant la présidentielle, le grand faux dans l'inconnu. *Libération*.

Reporters sans frontières. (2024, 27 novembre). Inde : Rana Ayyub, figure emblématique de l'ampleur du cyberharcèlement contre les femmes journalistes. *Reporters sans frontières*.

Sharman, L. (2021, 14 octobre). Tom Daley opens up about vile homophobic abuse. *The Standard*.

Sire, G. (2016, 28 octobre). Facebook, YouTube, Twitter : hébergeurs ou éditeurs ? La Revue des médias. *INA*.

Radio France. (2025, 13 septembre). Tanaland : nouvelle expression du féminisme 2.0. *France Inter.*

Le Monde. (2025, 12 février). Trois hommes condamnés par la justice pour le cyberharcèlement de la streameuse Ultia. *Le Monde*.

Zeid, J. (2014, 1er septembre). Le Cloud à l'épreuve du #CelebGate. *France Info*.

V. Contenus audiovisuels et publications sur les réseaux sociaux

Agence France-Presse. (2025, février). *Deepfake, les méthodes de réalisation* [Vidéo]. YouTube.

@camk798. (s. d.). Critique de la trend « bodycount » [Vidéo]. TikTok.

D. Typhaine. (2025, 7 octobre). *Violence en ligne, quelle action internationale ?* [Vidéo]. Assemblée nationale, Délégation aux droits des femmes.

D'Escufon, T. (s. d.). *Vidéo publiée sur TikTok* [Vidéo]. TikTok.

NousToutes, Parents & Féministes, Le Planning familial, & #StopFisha. (2025, à partir du 17 juin). *L'EVARS, c'est pour nous toustes* [Publications Instagram en série]. Instagram.

France 3 Occitanie. (2025, juillet). *Tout le monde peut faire un deepfake ?* [Vidéo]. YouTube.

Hofmeier, S. (Réalisatrice). (2025). *Qu'est-ce qu'un deepfake ?* [Vidéo]. ARTE.

@hugo_tournier. (s. d.). Vidéo sur le « body count » [Vidéo]. TikTok.

@kheyos_plus. (s. d.). Vidéo sur le « body count » [Vidéo]. TikTok.

Arrianz Taqqin. (2022, 27 juin). *Meme template - Team Fortress woman meme full version* [Vidéo]. YouTube.

Zirah, S. (2025, 3 janvier). *Ranelle Brown a été menacée par des hommes* [Interview vidéo]. YouTube.

VI. Ressources institutionnelles, parlementaires et sites de référence

Commission européenne. (2025). *Types of EU law*.

Commission européenne. (2025, 5 décembre). *La Commission inflige à X une amende de 120 millions d'euros au titre du règlement sur les services numériques* [Communiqué de presse]. Commission européenne.

CNIL. (2016, 16 novembre). *Ce que change la loi pour une République numérique pour la protection des données personnelles*.

Centre national de ressources textuelles et lexicales. (s. d.). Menace. Dans *Dictionnaire de l'Académie française* (9e éd.).

Conseil de l'Europe. (2025). *Une Convention pour protéger vos droits et libertés*.

Garcia Diaz, E., & Méndez, L. (2020, août). L'ère du « cyberbullying » vs la protection des données personnelles. *Village de la Justice*.

Ministère de la Justice du Canada. (2016). *Identité de genre et expression de genre*. Gouvernement du Canada.

Lyannaz, C. (2025, 28 novembre). DSA et article 6-3 LCEN : continuité des principes, proportionnalité des mesures. *Lamy Liaisons*.

Meta. (s. d.). *Lutter contre la sextorsion et la divulgation d'images intimes*. Centre de sécurité de Meta.

Muller, Y. (2024, 7 mars). Consécration de la notion de contrôle coercitif… Lorsque la Cour d'appel de Poitiers anime la conversation judiciaire. *Le Club des juristes*.

ONU Femmes France. (s. d.). *Définition de la « manosphère » (d'après le rapport du Secrétaire général des Nations Unies sur les violences faites aux femmes et aux filles)*.

Pinterest. (s. d.). *Avis de procédure : combattre les images intimes non consentantes*. Centre d'aide Pinterest.

Assemblée nationale. (2025, 26 août). *Question écrite n° 1225 : application de l'article 6-3 de la loi dite LCEN*.

La Fabrique des soignants. (2025, 30 juin). Ça veut dire quoi le validisme ? *La Fabrique des soignants*.

Sénat, Délégation aux droits des femmes. (2026, 30 avril). *Cyberharcèlement, haine en ligne : protégeons les victimes !* [Auditions].

StopNCII.org. (s. d.). *Frequently asked questions*. Consulté le 28 janvier 2026.

National Center for Missing & Exploited Children. (s. d.). *À qui s'adresse Take It Down ?* Take It Down. Consulté le 28 janvier 2026.

Take Back the Tech. (s. d.). *Site de la campagne*.

TikTok. (s. d.). *Soutien aux victimes d'abus sexuels*. Centre de sécurité de TikTok.

VII. Textes juridiques

A. Droit international et européen

Charte des droits fondamentaux de l'Union européenne (2000/C 364/01), 7 décembre 2000.

Convention européenne de sauvegarde des droits de l'homme, Conseil de l'Europe, 4 novembre 1950.

Convention sur la cybercriminalité (STE n° 185), Budapest, 23 novembre 2001 (entrée en vigueur le 1er juillet 2004).

Directive 2000/31/CE du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, 8 juin 2000.

Directive 2000/78/CE portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail, 2000.

Directive 2006/54/CE relative à la mise en œuvre du principe de l'égalité des chances et de l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail, 2006.

Directive (UE) 2024/1385 du Parlement européen et du Conseil sur la lutte contre la violence à l'égard des femmes et la violence domestique, 14 mai 2024.

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 (Règlement général sur la protection des données, RGPD), 27 avril 2016.

Règlement (UE) 2022/2065 du Parlement européen et du Conseil relatif à un marché unique des services numériques (Digital Services Act, DSA), 19 octobre 2022.

Règlement (UE) 2024/1689 sur l'intelligence artificielle (Artificial Intelligence Act, AI Act), 13 juin 2024.

B. Droit national (France)

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

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

Loi n° 2004-1486 du 30 décembre 2004 portant création de la Haute Autorité de lutte contre les discriminations et pour l'égalité (HALDE).

Loi n° 2010-769 du 9 juillet 2010 relative aux violences faites spécifiquement aux femmes, aux violences au sein des couples et aux incidences de ces dernières sur les enfants.

Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, JORF n° 0177 du 4 août 2018.

Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (LOPMI).

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN), JORF n° 0117 du 22 mai 2024.

Code pénal (France), notamment art. 222-17 à 222-18-3 (menaces), art. 222-33-2-1 et 222-33-2-2 (harcèlement et cyberharcèlement), art. 226-2-1 (diffusion d'images intimes), art. 226-3-1 (atteinte à la vie privée).

C. Droit comparé

Act on the Prevention of Damage by the Provision of Private Sexual Image Records, art. 3, 2014 (Corée du Sud).

Code pénal allemand (StGB), § 201a.

Code pénal brésilien, art. 218-C, 2018.

Code pénal canadien, art. 162.1, 2015.

Code pénal italien, art. 612-ter (Diffusione illecita di immagini o video sessualmente espliciti), 2019.

Code pénal portugais, art. 192 et art. 193.

Code pénal russe, art. 137.

Criminal Justice and Courts Act, s. 33 (Disclosing private sexual photographs and films with intent to cause distress), Royaume-Uni, 2015.

Cybercrime Act, s. 16(2)(b)(i)(ii), Afrique du Sud.

Harmful Digital Communications Act, s. 22A, Nouvelle-Zélande, 2022.

Sexual Crimes Punishment Act, art. 14(3), Corée du Sud.

VIII. Jurisprudence

CJUE, Association belge des consommateurs Test-Achats e.a. c. Conseil des ministres, C-236/09, 2011.

CJUE, Deldits, C-247/23, 13 mars 2025.

Cour EDH, Erbakan c. Turquie, n° 59405/00, 6 octobre 2006.

Cour EDH, Féret c. Belgique, n° 15615/07, 16 juillet 2009.

Conseil constitutionnel, décision n° 2004-496 DC, 10 juin 2004.

Conseil constitutionnel, décision n° 2021-933, 30 septembre 2021.

Cour de cassation, chambre criminelle, 16 mars 2016, n° 15-82.676.

Cour de cassation, chambre criminelle, 23 juin 2021, n° 21-80.682.

Ce rapport inter-associatif est également consultable en version numérique.

Il examine en profondeur les enjeux sociétaux, juridiques, techniques et politiques liés aux cyberviolences sexistes et sexuelles, et formule des recommandations concrètes en matière de prévention, de protection des victimes et de régulation des plateformes.

Retrouvez le rapport en version numérique ici ››

Féministes contre le cyberharcèlement est une organisation féministe intersectionnelle fondée en janvier 2016. Elle a pour vocation de lutter contre les violences exercées à l'encontre des femmes, des filles et des personnes LGBTIQ+ par le biais des outils et technologies numériques. Les missions de l'association sont l'information et la sensibilisation des publics, la formation des professionnel·les, la recherche et le plaidoyer.

> vscyberh.org

Point de Contact est une association de lutte contre les cyberviolences qui bénéficie du statut de signaleur de confiance. Elle permet en ce sens aux victimes et aux témoins de lui signaler des contenus ou des comportements malveillants et collabore étroitement avec les autorités et les plateformes numériques pour en obtenir le retrait. L'association mène également des actions de formation, de sensibilisation et de plaidoyer à l'attention des jeunes, des professionnels, des entreprises et des pouvoirs publics.

> pointdecontact.net

#StopFisha est une association féministe de lutte contre les cyberviolences sexuelles et à caractère discriminatoire. Les actions principales consistent en l'aide à la suppression de contenus haineux en ligne, à l'accompagnement de victimes et témoins ainsi qu'au plaidoyer et à la sensibilisation tout public aux multiples enjeux.

> stopfisha.org

Retrouvez la synthèse en version numérique ici >>

MINISTÈRE CHARGÉ DE L'ÉGALITÉ ENTRE LES FEMMES ET LES HOMMES ET DE LA LUTTE CONTRE LES DISCRIMINATIONS
Liberté
Égalité
Fraternité

La Grande Enquête sur les cyberviolences sexistes et sexuelles est un projet d'origine inter-associative, qui a bénéficié d'un soutien financier de la part du ministère chargé de l'Égalité entre les femmes et les hommes et de la Lutte contre les discriminations.