



Décryptage n°12 : Deepfakes à caractère sexuel : décrypter pour mieux accompagner les victimes

Depuis quelques années, **les deepfakes à caractère sexuel** s'imposent comme une forme de violence sexiste numérique croissante, profondément marquée par les rapports de domination de genre. Ces contenus — images ou vidéos truquées — sont produits par les agresseurs via des technologies d'intelligence artificielle qui permettent d'insérer **sans consentement** l'image d'une personne dans des scènes sexuelles ou pornographiques. Les logiciels et applications numériques permettant de produire les *deepfakes* sont nombreuses et facilement accessibles. La diffusion de ces images et vidéos peut être massive : envoyées au réseau personnel, professionnel de la victime, voire plus largement à des inconnus. **Les conséquences psychologiques et sociales sont graves pour les victimes**, et les mécanismes juridiques encore peu connus des professionnelles et professionnels accompagnant des victimes.

La loi SREN de 2024 a introduit une incrimination spécifique pour lutter contre ces contenus, mais son application et la réponse aux besoins des victimes restent encore à renforcer. Cet article offre un décryptage complet des spécificités des *deepfakes* à caractère sexuel, du cadre légal et des démarches concrètes à mettre en œuvre pour accompagner et protéger les victimes.

Pour faciliter la lecture, les notes de bas de page sont répertoriées dans l'index, à la fin du décryptage.

SOMMAIRE

Comprendre les <i>deepfakes</i> à caractère sexuel.....	3
Origine et définition du terme	3
Peu de données spécifiques malgré l'ampleur	3
Les conséquences pour les victimes	4
Le cadre légal depuis la loi SREN (2024).....	5
Avant la loi SREN.....	5
Création d'un délit autonome depuis la loi SREN en 2024	5
Limites dans l'application.....	6
Les dispositifs et les démarches d'accompagnement des victimes	7
Accueil et soutien psychologique	8
Collecte des preuves.....	8
Signalements spécialisés des <i>deepfakes</i> à caractère sexuel.....	8
Conclusion.....	11
Les ressources du Centre	11
INDEX	13

Comprendre les *deepfakes* à caractère sexuel

• Origine et définition du terme

Le mot « **deepfake** » apparaît en **2017 sur le réseau social Reddit**, lorsqu'un utilisateur anonyme, sous le pseudonyme "**deepfakes**", publie des vidéos pornographiques truquées mettant en scène des célébrités. Ce terme combine deux notions :

- **Deep learning** (*apprentissage profond*), une technique d'intelligence artificielle, permettant de produire des contenus très proches d'une représentation réelle, fondée sur des réseaux neuronaux capables d'apprendre à partir de grandes quantités de données, dont visuelles ou sonores ;
- **Fake**, qui signifie *faux* en anglais.

Un **deepfake à caractère sexuel** consiste ainsi à insérer l'image ou la voix d'une personne dans une vidéo, photo ou séquence à caractère intime, sexuel ou pornographique, sans son consentement¹. Souvent, **une ou quelques images publiques de la victime accessibles en ligne** - profil de réseaux sociaux, photos professionnelles - suffisent comme base pour produire des contenus truqués très réalistes suite à leur traitement par l'intelligence artificielle.

Ces applications sont mises en avant dans des publicités sur les réseaux sociaux, ou des messageries, qui proposent parfois des abonnements payants pour produire en grande quantité des *deepfakes* à caractère sexuel.

Ces *deepfakes* sont ainsi **massivement non consensuels**. La personne concernée est mise en scène sans son accord et elle les découvre souvent bien plus tard lorsqu'ils ont déjà été largement partagés. Ces contenus sont utilisés pour **harceler, humilier, discréditer ou faire du chantage** à la victime. Cette méthode de cyberviolence peut être utilisée par exemple par un conjoint ou partenaire violent, comme une forme de (cyber)violences au sein du couple, ou vis-à-vis des femmes politiques, des personnes prenant la parole sur les réseaux sociaux, etc. Ces pratiques s'inscrivent ainsi dans un rapport de domination de genre et dans un continuum de **(cyber)violences sexistes et sexuelles**, qui affectent principalement les femmes et les personnes LGBTQIA+. Ces cyberviolences renforcent également d'autres systèmes de domination : racisme, validisme, classisme, grossophobie, etc...

• Peu de données spécifiques malgré l'ampleur

Il existe peu d'études sur l'ampleur de ce phénomène mais les chiffres disponibles démontrent le caractère sexué et sexiste de cette cyberviolence : **98% des deepfakes produits en ligne sont à caractère pornographique et 99% des personnes ciblées sont des femmes**, selon la recherche « State of Deepfakes » de Security Hero en 2023².

En 2026, trois associations, Féministes contre le cyberharcèlement, StopFisha et Point de contact ont publié une Grande Enquête sur les cyberviolences sexistes et sexuelles³. D'après cette enquête :

- **L'image est utilisée comme un moyen de violence sexuelle** puisque **plus d'un quart des victimes ont subi une diffusion non consentie d'image intime ou sexuelle**, dont certaines sont des *deepfakes* à caractère sexuel. Ce chiffre monte à 30% chez les filles et les femmes, 21 % chez les garçons et les hommes, et touchent 36% des mineures et mineurs.

- **La diffusion massive de ces contenus non consentis**, incluant des *deepfakes* à caractère sexuels, a été faite via des **messages privés pour 66% des victimes**. 30% ont vu leurs contenus publiés sur un réseau social, pour 27% sur des groupes ou sites dédiés et 8% sur un site pornographique. Certaines **boucles de conversations sur Télégram ou channel Discord** sont créés spécifiquement pour partager des contenus intimes non consentis. Ils sont **quasiment exclusivement composés d'hommes** et peuvent atteindre des milliers de membres.
- Comme pour les violences sexistes et sexuelles, **les victimes connaissent majoritairement leur agresseur, même si rencontré en ligne**. Dans 85% des cas où la victime connaît l'agresseur, il s'agit d'un **homme**. Lorsqu'elle le connaît aussi hors ligne, il fait partie de son **entourage proche**. A travers cette enquête, 52% des victimes mentionnent des cyberviolences dans le cadre d'une **relation amoureuse ou de couple**.

Les données du Centre Hubertine Auclert apportent un éclairage complémentaire. Concernant les **cyberviolences au sein du couple**, l'étude de 2018 du Centre montre que **34 % des victimes ont subi des cyberviolences sexuelles**, incluant la **menace (33 %) ou la diffusion effective (16 %) de contenus intimes sans leur consentement**.

Concernant les **jeunes de 11 à 18 ans**, l'étude de 2025 du Centre Hubertine Auclert révèle que **7 % des élèves sont victimes d'atteintes à l'image intime**, avec une **surreprésentation marquée des filles et des personnes assignées LGBT+**. Plus précisément, 25 % des filles assignées LBT+ et 22 % des garçons assignés GBT+ subissent des atteintes à l'image intime, contre 9 % des filles non assignées LBT+ et 5 % des garçons non assignés GBT+. Ces chiffres soulignent que l'assignation à une identité LGBT+ et la mise en couple multiplie par deux le risque de subir des atteintes à l'image intime.

• Les conséquences pour les victimes

Les *deepfakes* à caractère sexuel ont des conséquences graves et multiples pour les victimes :

- des sentiments de **déshumanisation, de honte et de traumatisme psychologique** ;
- des conséquences sur la vie sociale, professionnelle et affective ;
- une **peur de l'exposition continue**, même après le retrait de certains contenus.

Dans la Grande Enquête, 78 % des victimes de cyberviolences déclarent des répercussions sur leur vie, dont : 58% des conséquences psychologiques, 40% des conséquences sociales, 38% des conséquences sexuelles, 30% des conséquences physiques, et 22% des conséquences sociales ou pro. Toutes les sphères de la victimes, privées ou publics, sont fortement impactées. Ces conséquences peuvent aller jusqu'à des pensées suicidaires ou des tentatives de suicides comme c'est le cas pour 45% pour les victimes de cyberviolences sexuelles⁴. Même si les cyberviolences se déroulent dans l'espace cyber, **les conséquences multiples sont bien réelles pour les victimes**.

Le cadre légal depuis la loi SREN (2024)

En France, la **loi SREN de 2024** a introduit une **incrimination spécifique** pour lutter contre les *deepfakes* à caractère sexuel.

• Avant la loi SREN

Avant l'adoption de la loi SREN, les victimes de *deepfakes* à caractère sexuel pouvaient s'appuyer sur différentes incriminations :

- l'atteinte à la représentation de la personne (**art. 226-8 du Code pénal**) ;
- l'atteinte à la vie privée (**art. 9 du Code civil**) ;
- l'usurpation d'identité (**art. 226-4-1 du Code pénal**) ;
- le harcèlement moral (**art. 222-33-2-2 du Code pénal**) ou sexuel (**art. 222-33 du Code pénal**).

Cependant les dispositions ne mentionnaient pas expressément les montages à **caractère sexuel, réalisés sans consentement**. L'atteinte à la représentation de la personne à de l'article 226-8 du Code pénal s'appliquait uniquement que s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention, remettant ainsi à la victime la charge de la preuve qu'il s'agissait d'un montage et non d'une image réelle. Pour les autres articles, il fallait démontrer un préjudice concret, que cette diffusion avait porté atteinte à la dignité de la personne, avait eu un impact négatif important ou répété sur sa vie.

• Création d'un délit autonome depuis la loi SREN en 2024

Pour répondre à cette lacune, la loi **SREN (Sécuriser et Réguler l'Espace Numérique) de 2024**⁵ a introduit un **nouvel article 226-8-1 du Code pénal**⁶. Cette incrimination spécifique avait largement été sollicitée par des avocates, juristes et associations accompagnant les victimes. Elles soulignaient l'importance de sanctionner la création et la diffusion de *deepfakes* à caractère sexuel, sans avoir besoin pour la victime d'apporter la preuve d'un préjudice concret.

Cet article reconnaît spécifiquement :

- Comme infraction, le « fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un **montage à caractère sexuel** réalisé avec les paroles ou l'image d'une personne, sans son consentement. »
- Comme infraction, le « fait de porter à la connaissance du public ou d'un tiers, par quelque voie que ce soit, un **contenu visuel ou sonore à caractère sexuel généré par un traitement algorithmique** et reproduisant l'image ou les paroles d'une personne, sans son consentement »
- Que la peine encourue est de **2 ans d'emprisonnement et 60 000 € d'amende**.
- Que si la « publication du montage ou du contenu généré par un traitement algorithmique a été réalisée en utilisant un service de communication au public en ligne », c'est à dire que la diffusion a lieu sur un service en ligne, par exemple un réseau social tel que les posts publics de Instagram, la peine est portée à **3 ans et 75 000 € d'amende**.

Le texte reconnaît que la diffusion d'une image ou vidéo à caractère sexuel sans consentement constitue une infraction, qu'il s'agisse d'un montage ou d'un contenu généré par intelligence artificielle. Cette avancée juridique permet de répondre à la question de l'absence de consentement et à la logique de viralité de ces contenus.

• Limites dans l'application

Si le texte existe, son application reste complexe. Comme l'a rappelé par exemple l'avocate Rachel-Flore Pardo « La loi, en théorie, en France est suffisante, le problème, c'est son application »⁷.

Son **application** rencontre en effet plusieurs **obstacles** :

- **L'anonymat des auteurs** : l'usage de pseudonymes, de VPN ou d'infrastructures étrangères rend l'identification difficile ;
- **Le manque de formation des forces de l'ordre** : cela conduit parfois des refus de plainte (malgré l'interdiction légale du refus d'enregistrement d'une plainte (art. 15-3 du Code de procédure pénale) ; à des manquements dans les investigations, et à des classements sans suite ;
- **La vitesse de diffusion virale** : bien plus rapide que les procédures judiciaires ;
- **La responsabilité des plateformes** : si elles sont légalement tenues de coopérer, leur réactivité reste limitée.
- Ce qui amène à une grande **difficulté des victimes à supprimer les deepfakes** dont elles sont victimes.

Une étude juridique européenne⁸ conduite dans le cadre du projet EUCLID souligne que les *deepfakes* et contenus manipulés à caractère sexuel, constituent des formes de cyberviolences sexistes et sexuelles qui nécessitent des **réponses normatives spécifiques, tant au niveau national qu'europpéen**. Elle propose ainsi des pistes d'harmonisation des législations dans l'Union Européenne.

Par exemple, plusieurs textes européens imposent des obligations pour des plateformes mais l'application pratique de ces dispositions doit être renforcée :

- Le **Digital Services Act (DSA, 2022)** impose aux grandes plateformes des **obligations renforcées de modération et de transparence** des contenus illicites.
- Le **Règlement IA (juin 2024)** prévoit l'obligation d'étiquetage des contenus générés par intelligence artificielle, facilitant la détection des *deepfakes*.
- La **Directive (UE) 2024/1385** du Parlement européen et du Conseil reconnaît diverses formes de **cyberviolences de genre**, dont le partage non consenti de contenus intimes ou manipulés (*article 5*)⁹.

La question de l'encadrement juridique des plateformes et outils permettant de produire des *deepfakes* reste un enjeu international fort. **Début 2026**, la médiatisation autour de **Grok**, l'intelligence artificielle intégrée à la plateforme X appartenant à Elon Musk, en a fourni un exemple concret. Des enquêtes ont montré que cette IA avait généré **des millions d'images à caractère sexuel non consenties en quelques jours**, notamment des représentations de femmes, de mineures et mineurs¹⁰. Cela a suscité une réaction internationale de régulateurs ainsi

que de gouvernements, et plusieurs pays ont déjà engagé des actions juridiques et réglementaires¹¹. Face à cette polémique, X a annoncé des restrictions pour empêcher certaines fonctions de création d'images. Cependant, les critiques ainsi demeurent sur l'efficacité de ces mesures car le réseau permet toujours accès à ces fonctionnalités pour les abonnés payants, ainsi que via des applications auxiliaires.

L'affaire Grok illustre que **la création et la diffusion de deepfakes à caractère sexuel restent difficiles à contraindre**, renforçant la nécessité de cadres juridiques robustes, d'un engagement des plateformes et de dispositifs de protection des victimes.

Les dispositifs et les démarches d'accompagnement des victimes

Pour aider et protéger les victimes, un accompagnement à plusieurs niveaux est nécessaire, combinant **soutien psychologique, démarches juridiques et stratégies de protection numériques**.

Les parties qui suivent (ainsi que la partie ressources à la fin de cet article) apportent des conseils opérationnels pour les professionnelles et les professionnels qui accompagnent les victimes.

Associations spécialisées dans l'accompagnement des victimes des (cyber)violences de genre

Les victimes peuvent être orientées vers les associations spécialisées suivantes :

- **StopFisha** : association féministe luttant contre les cyberviolences de genre, elle propose un accompagnement juridique, psychologique et pour signaler des contenus illicites ou des tendances illicites sur les réseaux sociaux comme les comptes Fisha (affiché à l'envers) qui partagent des contenus intimes non consentis, sur des plateformes publiques : stopfisha.org
- **Fédération Nationale Solidarité Femmes (FNSF)** : réseau d'associations féministes qui accompagnent les victimes des (cyber)violences faites aux femmes ; elle gère le numéro gratuit d'écoute national - 3919 - solidaritefemmes.org
- **Centres d'information sur les droits des femmes et des familles (CIDFF)** : associations féministes qui proposent un accompagnement juridique et psychologique : fncidff.info
- **Planning familial** : associations féministes qui informent et accompagnent sur la sexualité, la contraception et les (cyber)violences : planning-familial.org
- **Collectif Féministe Contre le Viol (CFCV)** : association féministe accompagnant les victimes de (cyber)violences sexuelles à travers un numéro d'appel gratuit : 0 800 05 95 95
- **En Avant Toute(s)** : association féministe qui soutient les jeunes femmes et les personnes LGBTQIA+ victimes de (cyber)violences sexistes et sexuelles avec un tchat gratuit et anonyme commentonsaime.fr et premieresfois.fr/
- **e-Enfance** : association de protection de l'enfance qui lutte contre le cyberharcèlement et facilite le retrait des contenus sur les plateformes : e-enfance.org et numéro d'écoute : 3018

Les **dispositifs d'accompagnement des femmes victimes de (cyber)violence en Île-de-France** : orientationviolences.hubertine.fr

- **Accueil et soutien psychologique**

Le premier accueil est souvent déterminant pour la suite du parcours. Les victimes de *deepfakes* à caractère sexuel ressentent fréquemment **honte, peur ou culpabilité**. Il est essentiel de rappeler que :

- La **responsabilité** incombe **exclusivement à l’auteur du contenu** et non à la victime ;
- Les contenus non consentis sont **illégaux** et relèvent du droit pénal ;
- Le fait d’en parler constitue une **étape courageuse** qu’il faut valoriser.

Ce soutien doit être bienveillant, empathique, non jugeant, et avec une **écoute active**.

- **Collecte des preuves**

La conservation d’éléments tangibles est essentielle pour toute procédure judiciaire. Si le premier réflexe peut être de supprimer ces contenus, il est d’abord nécessaire de conserver des preuves :

- **Réaliser des captures d’écran complètes** incluant les métadonnées visibles (utilisateur, URL, date, heure, etc.) ;
- **Télécharger le contenu incriminé**, lorsque cela est possible, et le **sauvegarder de manière sécurisée** (espace de stockage numérique protégé par un mot de passe, en dehors d’accès pour l’auteur, etc.) ;
- **Conserver les autres éléments de preuve associés** à la cyberviolence comme des messages de chantage, insultes, menaces, captures d’écran de commentaires, etc.

Ces éléments documentés faciliteront le dépôt de plainte et la qualification juridique des faits.

- **Signalements spécialisés des deepfakes à caractère sexuel**

Lorsque les *deepfakes* à caractère sexuel sont **partagés publiquement**, plusieurs dispositifs permettent de **signaler ces contenus pour qu’ils soient retirés** rapidement.

Dispositifs de signalement à mobiliser en cas de deepfakes à caractère sexuel

Plusieurs dispositifs complémentaires peuvent être utilisés pour faire retirer des *deepfakes* à caractère sexuel :

- **PHAROS** : la **plateforme gouvernementale officielle** de signalement des contenus illicites sur internet (violences, atteintes aux personnes, etc.) gérée par la police/gendarmerie française, qui permet de transmettre directement aux autorités les contenus manifestement illégaux, y compris ceux diffusés sur les réseaux sociaux : <https://internet-signalement.gouv.fr/>
- **3018** : numéro national et service d’écoute agissant comme **signaleur de confiance, géré par E-Enfance** disposant d’un canal prioritaire pour faire supprimer des contenus illégaux en quelques heures sur les plateformes ; <https://e-enfance.org/besoin-daide/>

- **Point de Contact** : association qui permet de **signaler anonymement ou non** des contenus potentiellement illicites pour obtenir leur retrait et orienter vers les autorités ; <https://www.pointdecontact.net/signaler/>

e-Enfance / 3018 et Point de Contact ont un statut de tiers de confiance ou signaleur de confiance¹² (ou *trusted flagger*) ; il s'agit d'organisation désignée par l'État ou par le cadre européen du **Digital Services Act (DSA) pour identifier et signaler des contenus illégaux auprès des plateformes numériques avec un **statut prioritaire**, permettant une réponse et une suppression plus rapides par les plateformes (réseaux sociaux etc.), donc **un retrait des deepfakes non consentis accéléré**.**

- **Disrupt** : plateforme française et de l'Union européenne gérée par **Point de Contact**, spécialisée dans le retrait et l'interruption de la diffusion des contenus à caractère sexuel non consentis en utilisant une technique de hashage, <https://www.pointdecontact.net/disrupt/>
- **StopNCII** : initiative internationale soutenue par Meta et des ONG qui utilise une technique de hashage de contenus à caractère sexuels non consenti pour les retirer. <https://stopncii.org/>

Le hashage

Disrupt et **StopNCII** utilise une technique de **hashage** qui permet de déposer sur la plateforme une « **empreinte numérique** » appelé **hash** de ses contenus non consentis à caractère sexuels. Cet **hash** est en fait une **empreinte cryptographique unique d'un fichier** - image ou vidéo - qui permet de **d'identifier spécifiquement** ce contenu, **sans avoir besoin de stocker l'image ou la vidéo elle-même**. Ainsi, aucun contenu non consenti n'est enregistré sur les serveurs de ces deux services de signalement, ce qui protège davantage la vie privée des victimes. C'est cet **hash** qui est ensuite transmis aux sites hébergeant ces contenus non consentis pour qu'ils les retirent. La republication de cet hash est automatiquement bloquée sur les plateformes partenaires pour éviter une nouvelle diffusion

Ces plateformes ne peuvent **retirer des contenus que s'ils sont publics**. En revanche, lorsqu'ils sont partagés dans des conversations privées (messages fermés, groupes privés), ces dispositifs ne peuvent pas agir directement : dans ce cas, il faut signaler le message et le compte auteur sur le réseau social, puis envisager le dépôt de plainte pour obtenir des mesures judiciaires.

1. Déposer plainte

La Grande Enquête citée ci-dessus montre **que seulement 12% des victimes de cyberviolences ont porté plainte** et ce chiffre descend à 10% chez les mineures et mineurs. Ce chiffre peut être expliqué en partie par une méconnaissance du cadre légal ou un manque de confiance dans leur prise en charge.

Pourtant le dépôt de plainte est important pour être reconnue en tant que victime, faire valoir ses droits et engager des poursuites contre l'agresseur.

Une **plainte spécifique contre les deepfakes à caractère sexuel** peut désormais être déposée sur le fondement direct de l'article 226-8-1. Les victimes peuvent être accompagnées par une **avocate ou avocat spécialisé en droit numérique** et/ou **(cyber)violences de genre** ainsi que par une **association féministe d'aide aux victimes**.

La plainte doit être accompagnée des preuves collectées, et l'avocate ou l'avocat ou l'association peut aider à la qualification juridique (article 226-8-1 du Code pénal) et au suivi de la procédure.

2. Protection numérique

Au-delà des démarches juridiques, il est essentiel d'aider la victime à **prévenir d'éventuelles nouvelles expositions** et assurer une **protection numérique durable**. Parmi les recommandations utiles :

- **Déposer le deepfake à caractère sexuel sur Disrupt ou StopNCII pour que son hash – et non le contenu – soit dans leur base de données** : chaque nouvelle apparition du contenu illicite sur un des sites partenaires sera automatiquement supprimé ;
- **Effectuer régulièrement des recherches inversées d'images** (via Google, Yandex, Bing) pour détecter d'éventuelles autres ou nouvelles publications non signalées ;
- **Paramétrer la confidentialité des profils en ligne** - limiter l'accès au contenu à un cercle restreint de personnes - afin de réduire la récupération automatique des images par des tiers ;
- **Créer des alertes automatiques** (par exemple via *Google Alerts*) sur le nom ou des combinaisons de mots clés associés pour repérer toute apparition suspecte ; notamment en cas de **doxing**, qui consiste à publier des informations privées - nom, prénom, adresse - pour identifier et harceler une personne.

Ces mesures peuvent aider dans la démarche de la protection mais ne garantissent pas l'élimination totale des risques car il n'est jamais possible de s'assurer totalement que tous les deepfakes à caractère sexuels sont supprimés. Il est toujours possible qu'une personne l'ait enregistré localement et le repartage ultérieurement. Cependant, ces mesures aident à réduire l'exposition et à détecter plus rapidement les nouvelles apparitions de deepfake à caractère sexuel.

3. De potentielles solutions techniques de détection des deepfakes ?

De nombreux outils techniques de détection des deepfakes ont été développés, mais **leur fiabilité reste limitée**.

Parmi les solutions, il existe, par exemple : **Reality Defender, Deepware Scanner**. Ces outils sont capables d'analyser des images ou vidéos pour détecter des signes de falsification et d'autres sont encore en développement ou recherche.

Malgré ces progrès, **la détection de deepfakes à caractère sexuel reste imparfaite** : les contenus courts, compressés ou fortement retouchés échappent souvent aux protections

automatisées. Aucune solution technique n'est actuellement infaillible et que seule **une combinaison d'outils technologiques et d'analyse humaine** permet une détection plus fiable.

Ainsi, les dispositifs associatifs d'accompagnement et de signalement présentés plus haut sont particulièrement importants face à la complexité des démarches et des conséquences pour les victimes. Il est essentiel que ces dispositifs soient renforcés et dotés des moyens nécessaires pour proposer une aide et un accompagnement rapide à toutes les victimes qui les sollicitent.

Conclusion

Les *deepfakes* à caractère sexuel s'imposent aujourd'hui comme une **violence genrée importante**, visant principalement les **femmes et les personnes LGBTQIA+**. Ils instrumentalisent l'image d'une personne sans son consentement pour l'humilier ou la contrôler, avec des conséquences importantes.

Il est important de rappeler que l'enjeu de lutte contre les *deepfakes* à caractère sexuel n'est pas uniquement technique. S'attaquer aux **inégalités de genre structurelles** et **l'éducation** et la **prévention** auprès des jeunes constituent aussi un levier fondamental dans la lutte contre les *deepfakes* à caractère sexuel. Il est crucial de développer dès le plus jeune âge une **éducation qui intègre spécifiquement les enjeux de genre, de consentement et de respect de la vie privée**.

Les ressources du Centre Hubertine Auclert pour aller plus loin

Etude complète et Synthèse : *(Cyber)violences de genre chez les 11-18 ans - Victimations sexistes, sexuelles et LGBTphobes dans des collèges et lycées franciliens*, 2025.

Disponible ici : <https://www.centre-hubertine-auclert.fr/egalitheque/publication/synthese-cyberviolences-de-genre-chez-les-11-18-ans-victimations-sexistes> ;

Webinaire de présentation, disponible ici : <https://www.centre-hubertine-auclert.fr/agenda/evenements/webinaire-cyberviolences-de-genre-chez-les-11-18-ans-presentations-de-la-nouvelle>

Campagne de sensibilisation sur les (cyber)violences de genre à destination des 14-18 ans « Gênant ? Surtout violent ! », 2025.

Disponible ici : genant-surtout-violent.com

Cyberviolences conjugales - Recherche-action menée auprès de femmes victimes de violences conjugales et des professionnel·les les accompagnant, 2018.

Disponible ici : <https://www.centre-hubertine-auclert.fr/egalitheque/publication/rapport-cyberviolences-conjugales>

Fiche pratique juridique « Que dit la loi face au cybersexisme ? », 2022.

Disponible ici : <https://www.centre-hubertine-auclert.fr/egalitheque/publication/fiche-juridique-que-dit-la-loi-face-au-cybersexisme>

Fiche pratique juridique « Que dit la loi face aux cyberviolences conjugales ? », 2022. Disponible ici :

Fiche pratique « Que faire en cas de diffusion de contenus intimes en ligne ? », 2022.

Disponible ici : <https://www.centre-hubertine-auclert.fr/egalitheque/publication/fiche-pratique-que-faire-en-cas-de-diffusion-de-contenus-intimes-en-ligne>

Guide de protection numérique, *Je protège ma vie privée en ligne*.

Disponible ici : guide-protection-numerique.com

Guide, *Les cyberviolences au sein du couple - Repérer, accompagner, orienter les victimes*, en collaboration avec Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains novembre 2022.

Disponible ici : <https://www.centre-hubertine-auclert.fr/egalitheque/publication/guide-sur-les-cyberviolences-au-sein-du-couple>

Kit d'action contre les cyberviolences conjugales pour les professionnel·les, *Cyberviolences conjugales : repérer, accompagner, orienter les victimes*, avec des fiches techniques, 2020.

Disponible ici : <https://www.centre-hubertine-auclert.fr/egalitheque/publication/kit-daction-contre-les-cyberviolences-conjugales>

Site avec des conseils utiles pour lutter contre les cyberviolences de genre chez les jeunes.

Disponible ici : stop-cybersexisme.com

Webinaire « La collecte de preuves en cas de cyberviolences », dans un cycle de webinaires sur les cyberviolences sexistes, sexuelles et conjugales, 2023.

Disponible ici : <https://www.centre-hubertine-auclert.fr/agenda/evenements/webinaire-la-collecte-de-preuves-en-cas-de-cyberviolences>

INDEX

¹ « Deepfakes : quand l'IA trahit notre intimité », épisode 1, Sorbonne TV, 2025. Disponible ici : <https://sorbonne.tv/episode-1-deepfakes-quand-lia-trahit-notre-intimite>

² Security Hero, *State of Deepfake*. 2023. Disponible ici : <https://www.securityhero.io/state-of-deepfakes/>

³ « La Grande enquête nationale sur les cyberviolences sexistes et sexuelles : premiers résultats », novembre 2025. Disponible ici : <https://www.vscyberh.org/post/800843542972039168/grande-enqu%C3%AAt-nationale-cyberviolences-sexistes-sexuell>

⁴ « La Grande enquête nationale sur les cyberviolences sexistes et sexuelles : premiers résultats, Replay Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, 2025. Disponible ici : <https://www.youtube.com/watch?v=kN4OkNtNP0k>

⁵ Assemblée nationale, Amendements n° 9 et 10, Projet de loi SREN, 2024. Disponible ici : <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/>

⁶ Code pénal français, article 226-8-1 (introduit par la loi SREN, 2024). Disponible ici : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049567458

⁷ Interview *Franceinfo*, 10 février 2025. Disponible ici : https://www.franceinfo.fr/internet/intelligence-artificielle/intelligence-artificielle-et-deepfakes-la-loi-en-theorie-en-france-est-suffisante-le-probleme-c-est-son-application-deploire-une-avocate_7066454.html

⁸ « État des lieux : cadres juridiques sur les cyberviolences sexistes et sexuelles en France et dans l'UE », *Enseignement Universitaire Clinique du Droit (EUCLID) de l'Université Paris Nanterre en collaboration avec Osez le Féminisme (OLF) et la Coordination Française pour le Lobby Européen des Femmes (CLEF)*, 2025. Disponible ici : <https://stopsexualexploitationonline.eu/wp-content/uploads/2025/11/EUCLID-fini-FR.pdf>

⁹ Union européenne, Directive 2024/1385 sur la lutte contre la violence à l'égard des femmes et la violence domestique, article 5. Disponible ici : <http://data.europa.eu/eli/dir/2024/1385/oj>

¹⁰ AI Forensics, *Grok Unleashed - Grok Generating Flood of Sexualized Images of Women, Including Minors, and Extremist Propaganda*, Flash Report, janvier 2026.

Disponible ici : <https://aiforensics.org/uploads/GrokUnleashed.pdf>; Center for Countering Digital Hate, *Grok Floods X with Sexualized Images*, Research Report, 2026.

Disponible ici : <https://counterhate.com/research/grok-floods-x-with-sexualized-images/>

¹¹ « Le détournement de Grok est choquant : plus d'une image générée sur deux serait sexuelle », *Numerama*, 23 janvier 2026. Disponible ici : <https://www.numerama.com/tech/2165587-le-detournement-de-grok-est-choquant-plus-dune-image-generee-sur-deux-serait-sexuelle.html>