Rapport sur la Cyber Violence contre les Femmes

RÉSUMÉ ANALYTIQUE ET
RECOMMANDATIONS
SEPTEMBRE 2024

Financé par l'Union européenne. Les points de vue et les opinions exprimés sont toutefois ceux du (des) auteur(s) uniquement et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive pour l'éducation et la culture (EACEA). Ni l'Union européenne, ni l'EACEA ne peuvent en être tenus responsables.

CRÉDITS:

Virginia Dalla Pozza
Autrice Principale

Iliana Balabanova
La Présidente du LEF

Mary Collins
La Secrétaire Générale du LEF

Veronica Zaboia
La Coordinatrice du Projet

Maria João Faustino
Contribution Scientifique

Yvonne Redin
Conception Graphique

Laura Kaun, Irene Rosales, Alexia Fafara, Veronica Zaboia, Maria João Faustino
Contributrices

Funded by the European Union

EUROPEAN WOMEN'S LOBBY
EUROPEEN DES FEMMES

ACRONYMS

CEDH
Convention européenne des droits humains

CoE
Conseil de l'Europe

CSN
Coordinateur des services numériques

CV
Cyber violence

CVCF
Cyber violence contre les femmes

CVCFF
Cyber violence contre les femmes et les filles

DDV
Directive sur les droits des victimes

DSA
Règlement sur les services numériques

EIGE
Institut européen pour l'égalité entre les hommes et les femmes

EPRS
Service de recherche du Parlement européen

FRA
Agence des droits fondamentaux de l'Union européenne

GREVIO
Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique

IA
Intelligence artificielle

LEF
Lobby européen des femmes

ODD
Objectifs de développement durable

ONU
Nations unies

TGMRL
Les très grands moteurs de recherche en ligne

TGPL
Très grandes plateformes en ligne

TIC
Technologies de l'information et de la communication

VCF
Violence à l'encontre des femmes

VD
Violences domestiques

VFFT
La violence à l'encontre des femmes facilitée par les technologies

VFT
La violence facilitée par les technologies

VPI
Violence entre partenaires intimes

VS
Violence sexiste

Les violences contre les femmes sont une manifestation de la domination masculine et de son pouvoir supérieur sur les femmes pour les réduire au silence, contrôler leurs vies, leurs corps et leur sexualité et les «maintenir à leur place».

La violence masculine contre les femmes revêt de multiples formes et fait partie du continuum de la violence ancrée dans une société patriarcale. Il n'y a pas un seul pays au monde où les femmes et les filles vivraient libres de toute violence masculine et pas un seul domaine dans la vie des femmes où elles ne soient pas exposées à la menace ou à la réalité d'actes de violence masculine.

Le monde/la culture numérique n'est pas une exception à cette règle. Les données fournies par l'EIGE[1] estiment qu'une femme sur dix a déjà vécu une forme de cyberviolence depuis l'âge de 15 ans.

Demander justice pour combattre la violence en ligne exige d'importantes mesures internationales juridiques et politiques, car l'espace virtuel ne connait pas de frontières géographiques. Une approche holistique qui inclut des outils juridiques pour prévenir la cyberviolence et protège efficacement les victimes, la responsabilisation des entreprises de technologies (tech) aussi bien que des réponses coordonnées pour défier le sexisme et les normes culturelles relatives à la domination masculine à l'encontre des femmes sont nécessaires. Il faut également s'attaquer à l'industrie pornographique. Ce n'est jamais de la responsabilité des femmes de prévenir la violence masculine.

Ce document est un résumé du «Rapport sur la Cyberviolence contre les femmes du Lobby européen des femmes (LEF) : vue d'ensemble politique et Recommandations» qui est rédigé et disponible en anglais.

Ce rapport s'intègre dans la mission, la vision et les principes du Lobby européen des femmes (LEF) : les droits des femmes sont des droits humains, la solidarité, l'autonomie, la participation et l'inclusion

OBJECTIF DU RAPPORT ET APPROCHE MÉTHODOLOGIQUE.

Dans la continuité du rapport et du dossier de ressources #HerNetHerRights de 2017,[2] ce rapport a pour but de fournir des recommandations aux décideurs politiques et autres parties concernées pour contrer la cyberviolence contre les femmes (CVCF).

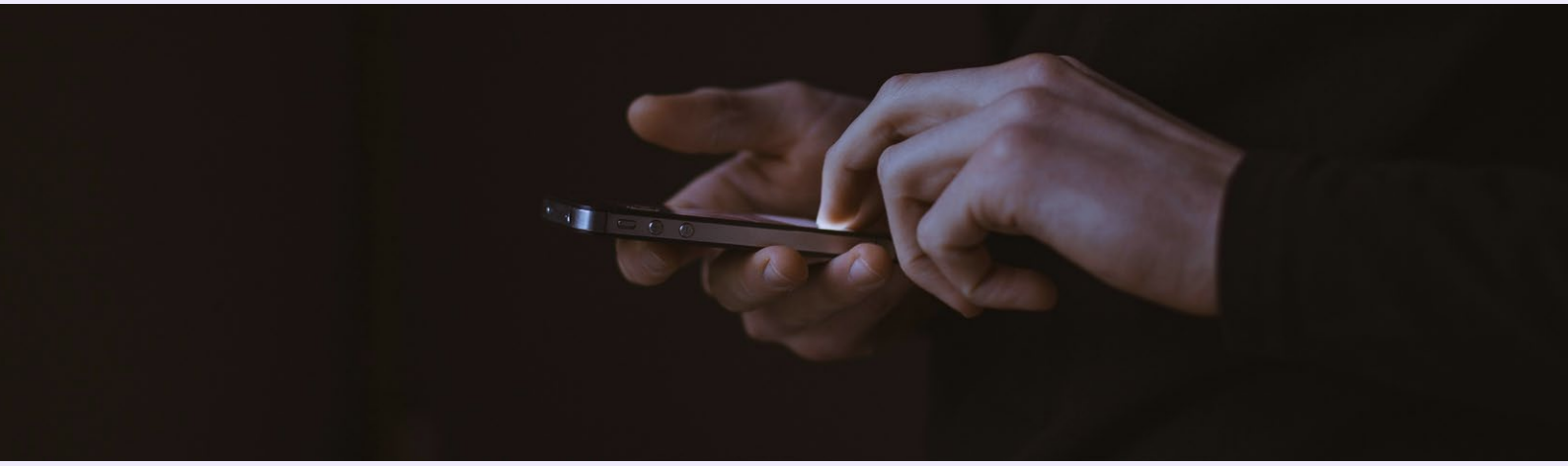
Le rapport a **cinq objectifs principaux**:

- Fournir un aperçu de la cyberviolence à l'égard des femmes et de ses caractéristiques clés.
- Examiner le cadre juridique et politique de la violence à l'égard des femmes au niveau international, européen et national;
- Identifier les principaux défis dans ce domaine;
- Sélectionner des exemples de bonnes pratiques pour lutter contre la violence à l'encontre des femmes;

Formuler des recommandations à l'intention des institutions européennes et des États membres afin de lutter efficacement contre la violence à l'égard des femmes.

La recherche sous-jacente à ce rapport s'est déroulée sur la période mars-mai 2024 ; les méthodes de recherche suivantes ont été utilisées :

- **Recherche documentaire:** Une recherche documentaire approfondie a utilisé un large éventail de documents, incluant des études, des rapports, des articles, des sites web, des bases de données et des projets sur la cyberviolence contre les femmes, publiés par des acteurs internationaux, européens et nationaux.
- **Examen juridique et politique** : Un examen détaillé des documents juridiques/politiques dans l'UE, au niveau international et national a été effectué pour avoir une cartographie des instruments juridiques et politiques qui peuvent être applicables aux violences contre les femmes.
- **Consultation des parties prenantes : de façon à explorer plus à fond des thèmes spécifiques du rapport**: 5 acteurs clés de différentes catégories ont été consultés (universités, institutions, ONGs).



CYBER VIOLENCE CONTRE LES FEMMES
(CVCF)

La Cyberviolence (CV) signifie l'utilisation de technologies en ligne et de communication pour causer, faciliter ou menacer de violences contre des individus.[3] Les définitions des cyberviolences varient considérablement non seulement d'un pays à l'autre mais aussi parmi les acteurs clés dans ce domaine. Ceci a pour résultat d'avoir différentes terminologies et méthodologies pour les mesurer. La cyberviolence contre les femmes (CVCF) est une **forme de violence basée sur le genre**.[4] Il est évident qu'il y a une **dimension genrée** claire : les femmes ont beaucoup plus de chances de subir des formes uniques de violence genrée dans les contextes numériques, reflétant un modèle similaire à celui des violences contre les femmes dans le monde hors ligne.[5] **La Cyberviolence s'enracine dans le même contexte d'inégalité des femmes que dans celui hors ligne**.[6] Les espaces numériques renforcent et intensifient **les inégalités de genre systémiques** structurelles de même que les modèles de masculinités dangereuses qui conduisent à toutes formes de violences à l'encontre des femmes.[7]

Conformément au Comité consultatif sur l'égalité des chances pour les femmes et les hommes[8] et selon le LEF, la cyberviolence fait partie du continuum des violences faites aux femmes ; elles n'existent pas dans un vide, mais plutôt à la fois en découlent et alimentent de multiples formes de violence hors ligne.[9] En effet, la violence en ligne et la violence hors ligne sont souvent interconnectées et/ou imbriquées.[10]

Bien que la CVCF soit aussi dangereuse que la violence hors ligne, elle a des traits spécifiques qui la distingue des autres formes de violence contre les femmes, la rendant particulièrement dangereuse. La portée de ses large diffusion, transmission et vitesse, rend difficile le contrôle du type d'information qui est diffusé par les moyens numériques. L'anonymat accentué dans les espaces numériques et virtuels permettent aux utilisateurs d'agir en toute impunité. Il est difficile d'effacer et, cela ajoute un traumatisme aux victimes.

Les auteurs des cyberviolences contre les femmes peuvent être leurs partenaires ou ex-partenaires, des membres de la famille, des amis ou des inconnus. L'impact de la cyberviolence contre les femmes et les filles peut être aussi grave que la violence hors ligne. Les victimes se retirent souvent de la sphère digitale, se taisent et s'isolent. Elles perdent des opportunités pour construire leur éducation, leur carrière professionnelle et le soutien des réseaux.[11]

PRINCIPALES FORMES DE VIOLENCE À L'ENCONTRE DES FEMMES

Le rapport présente les formes principales de violence contre les femmes[12] qui ne doivent pas être considérées comme des catégories distinctes alors que chaque forme de violence est imbriquée avec d'autres formes, à la fois hors ligne et en ligne, dans la droite ligne du concept de continuum de la violence. Le rapport reconnait que les formes de cyberviolence sont en évolution constante, si l'on considère l'évolution rapide de l'environnement numérique.

FORMES LES PLUS RÉPANDUES:

Les données sur les formes de cyberviolences les plus fréquentes varient d'une étude à l'autre, selon la méthodologie et la sphère géographique considérées aussi bien que les définitions utilisées pour la cyberviolence. Néanmoins, il semble que **le cyberharcèlement, la cybertraque, le partage non consenti de contenu intime et le discours de haine** sont les formes les plus répandues.[13]

AUGMENTATION DES FORMES DE MENACES:

Parmi les formes diverses, **l'utilisation de l'intelligence artificielle (IA), de la réalité virtuelle et des jeux en ligne** est devenue de plus en plus menaçante pour les femmes. L'utilisation de l'IA a contribué à une forte **augmentation de fausses images sexuelles générées par l'IA (connues sous le terme « deepfakes »)**.[14] Comme le montre l'étude du Service de recherche du Parlement européen (EPRS) de 2021, les outils de l'IA pour créer de fausses vidéos sexuelles se développent rapidement et deviennent moins onéreux, plus sophistiqués et accessibles aux utilisateurs lambda.[15] Le rapport sur les risques mondiaux du World Economic Forum's de 2024[16] a classé la désinformation, surtout alimentée par les "deepfakes", comme le risque global à court terme le plus grave auquel le monde sera confronté au cours des deux prochaines années.

La dimension genrée du phénomène est bien mise en évidence. Les fausses images sexuelles virtuelles ciblent presque uniquement les femmes.[17] En effet, la majorité des vidéos « deepfakes » qui circulent actuellement en ligne contiennent des images sexuelles de femmes. **On a estimé qu'entre 90% et 95% de tous les « deepfakes » se rapporte à du contenu montrant la nudité ou des activités sexuelles explicites;**[18] **la grande majorité de ces « deepfakes » (90%) concernent les femmes**.[19]

De la même façon, la technologie d'animation 3D accroit fortement les capacités à générer des vidéos avec une qualité similaire à la technologie «deepfake» de l'IA.[20] Quelques programmes « deepfakes » combinent même la génération d'images par l'IA et l'animation 3D ; les plus courantes sont les **technologies de l'avatar** qui transforment des modèles en 3D de la tête d'une personne ou de son corps entier. L'utilisation des avatars 3D s'est diffusée dans le metaverse où **le nombre inquiétant de comptes de femmes subissant du harcèlement et des agressions sexuelles par des avatars 3D a augmenté.** Ainsi, alors qu'un nombre croissant de femmes se joint **aux communautés**

La « manosphere » est un réseau de communautés d'hommes en ligne qui plaident pour divers droits et intérêts des hommes, tout en promouvant en même temps des idéologies misogynes, et des convictions antiféministes et sexistes.

de jeux en ligne, elles rapportent les taux élevés de harcèlement sexuel qu'elles subissent. Les communautés de jeux en ligne sont perçues comme **un des environnements les plus inégalitaires pour les femmes**.[22]

MACRO-FORMES:

Alors que les formes de cyberviolences contre les femmes (CVCF) sont nombreuses et définies différemment suivant les pays et parties prenantes, quelques **macro catégories** des cyberviolences contre les femmes peuvent être identifiées. Ce sont celles couvertes par la toute première Directive européenne sur les violences contre les femmes adoptée en avril 2024 : le partage de contenus intimes ou de contenu manipulé sans consentement ; le cyberharcèlement, la cybertraque et l'incitation à la violence ou à la haine.

FORMES SUPPLÉMENTAIRES:

Le rapport fournit une description des formes supplémentaires de cyber violence : changement de référencement sur google (google bombing), intrusions répétées (sealioning) etc... La liste n'est pas exhaustive alors que de nouvelles formes continuent d'émerger avec l'accroissement de la numérisation, et l'évolution rapide de la technologie. Parmi ces formes supplémentaires figurent et sont décrites ci-dessous la « manosphère » et la pornographie .

La « **manosphere** » est un réseau de communautés d'hommes en ligne qui plaident pour divers droits et intérêts des hommes, tout en promouvant en même temps des idéologies misogynes, et des convictions antiféministes et sexistes. Ils considèrent les femmes et les féministes responsables de toutes sortes de problèmes de société. Beaucoup de ces communautés encouragent le ressentiment ou même la haine, envers les femmes et les filles.[23] La **pornographie** promeut des stéréotypes dangereux dans son image des femmes. La production et la vente de pornographie conduisent à des violences sexuelles contre les femmes, les encouragent et jouent un rôle clé dans la construction des représentations des relations des hommes et des femmes. De plus, la pornographie rend la violence « sexy ». Les chiffres montrent que les Etats qui ont les taux de diffusion de magazines pornographiques les plus élevés ont des taux plus élevés de viols.[24]

* Sealioning fusionne une questionnement persistant – souvent sur une information basique, une information facilement retrouvée ailleurs, ou des points qui n'ont aucun rapport ou tangentiels – avec un engagement sur lequel il est lourdement insisté pour un débat raisonnable. Il se déguise comme un essai sincère d'apprendre et de communiquer.

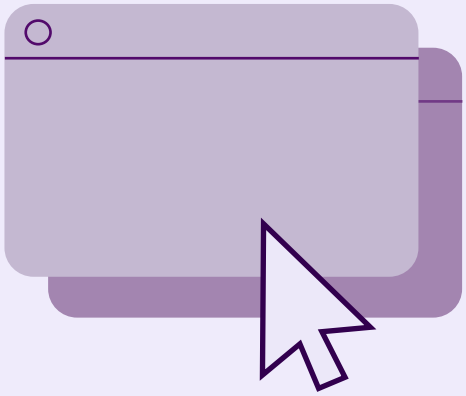
PRÉVALENCE

Le **manque de définitions consensuelles** des cyberviolences et **des méthodologies communes pour la mesurer rendent particulièrement difficile l'évaluation de l'étendue du problème**.[25] Malgré ces lacunes et ces différences dans les méthodologies, **quelques essais pour mesurer la cyberviolence contre les femmes ont été faites à la fois au niveau international et au niveau de l'UE**.

Au **niveau international**, un rapport global[26] qui synthétise les résultats d'enquêtes sur les cyberviolences contre les femmes et les filles, effectuées de 2018 à nos jours, estime qu'entre 16 à 58% des femmes ont subi personnellement des violences (CVCF) en ligne. De la même façon, the Economist Intelligence Unit a trouvé que 38% des femmes ont subi des violences en ligne, et 85% de femmes qui passent du temps connectées en ligne ont été témoins de violences numériques contre d'autres femmes.[27]

Le manque sévère de données et de recherche sur les CVCF est un problème majeur au niveau de l'UE. Quelques essais pour obtenir la prévalence des quelques formes de CVCF ont été faites par la Fundamental Rights Agency (FRA) antérieurement en 2014 et 2019.[28] L'enquête de 2019[29] du FRA a montré que 13% des femmes ont subi du cyberharcèlement au cours des cinq années précédentes. D'autres données intéressantes viennent de l'enquête faite par HateAid.[30] L'enquête a interrogé 2000 personnes de 18 à 80 ans dans tous les pays de l'UE sur leurs expériences de violence numérique. Les résultats indiquent que 50% des jeunes adultes (18 à 35 ans) de l'UE ont été affectés par de la haine sur internet ; 30% des femmes dans l'UE craignent que de fausses images intimes d'elles puissent être partagées sans leur consentement, 80% des répondant.es donnent aux plateformes en ligne une mauvaise note.[31]

Au **niveau national**, en Allemagne, France et Espagne, plus d'une femme sur deux (53%) entre 18 et 34 ans ont été victimes de malveillance basée sur leur image. Parmi les personnes victimes, 82% rapportent un sentiment d'insécurité, avec certaines qui s'interrogent sur un retrait total des espaces en ligne.[32] En France, plus de 4 personnes sur 10 disent avoir été victimes de cyberharcèlement.[33]



LA DIMENSION GENRÉE DES CYBER VIOLENCES

La cyberviolence porte une dimension genrée. Suivant un rapport du FRA en 2023,[34] se focalisant sur la haine en ligne dans les messages des réseaux sociaux, **les femmes sont confrontées à plus de harcèlement en ligne qu'aucun autre des groupes cibles** (personnes d'ascendance africaine, Juifs et Roms.) De même une étude américaine a montré que 33% des femmes de moins de 35 ans rapportent avoir été sexuellement harcelées en ligne, à comparer aux 11% d'hommes.[35] Dans le même ordre d'idées, le GREVIO[36] met en évidence que à la fois les hommes et les femmes peuvent subir des incidents de violence interpersonnelles ; toutefois **les femmes sont beaucoup plus à même d'être sujettes à de formes répétées et sévères** d'agressions, à la fois hors ligne et en ligne.

Alors que toutes les femmes qui ont accès à des espaces numériques sont exposées à des risques de cyberviolence, **certains groupes de femmes sont particulièrement vulnérables**. Les formes numériques des violences contre les femmes peuvent être particulièrement sévères pour les femmes et les filles risquant ou étant exposées à des formes intersectionnelles de discrimination et elles peuvent être exacerbées par des facteurs tels que **le handicap, l'orientation sexuelle, l'affiliation politique, la religion, l'origine sociale, le statut de migrante, ou le statut de célébrité, l'âge, parmi d'autres.[37] Les femmes dans vie publique y compris les militantes des droits des femmes, les défenseur.es des droits humains des femmes, les femmes politiques et les femmes journalistes sont aussi souvent des cibles de cyberviolences.[38]**

LES AGRESSEURS

La CVCF peut être perpétrée par des hommes et par des femmes. Pourtant, **dans la majorité des cas, les femmes sont ciblées par des hommes qui peuvent être inconnus ou connus de la victime**.[39] Par exemple, la grande majorité des auteurs d'abus sexuels fondés sur l'image sont des hommes.[40] Les agresseurs peuvent être uniques ou une multitude. Etant donné que la technologie permet une diffusion facile et rapide de contenus préjudiciables, il faut identifier à la fois les agresseurs primaires et secondaires. Par exemple une personne peut partager une image intime non consentie (agresseur primaire) qui peut ensuite être visionnée et partagée par une multitude d'utilisateurs (agresseurs secondaires).[41]

LES IMPACTS DE LA CYBERVIOLENCE SUR LES FEMMES

La cyberviolence contre les femmes est souvent perçue comme une forme moins sévère et moins préjudiciable des violences fondées sur le genre; pourtant elle peut avoir des conséquences aussi graves sur la santé et la vie des femmes que la violence physique et sexuelle. **La nature publique, invasive, répétitive et perpétuelle des cyberviolences contre les femmes de même que les interconnections entre la violence en ligne et la violence hors ligne, ont pour résultat que les survivant.es se sentent constamment dans la peur et l'insécurité**.[42]

Le GREVIO montre **les graves impacts psychologiques, économiques et sociaux des cyberviolences contre les femmes**. En plus des effets au niveau individuel et social, il y a également d'importantes **conséquences financières de la cyberviolence contre les femmes**, tels que les coûts encourus pour la santé résultant du harcèlement, les difficultés pour les perspectives de carrière, la perte d'emploi et les arrêts de travail. L'étude de l'EPRS indique que les coûts totaux du cyberharcèlement et de la cybertraque pour les individus et la société atteignent une fourchette entre 49 et 89,30 milliards d'euros.[43]

Les effets sur les femmes dans la politique et le journalisme sont particulièrement nuisibles. Les femmes politiques tendent à réduire leur activité politique, sont dissuadées de se présenter à des élections et même démissionnent de leur mandat prématurément.[44] De sérieux impacts affectent aussi **les femmes journalistes**. Une étude montre que 30% des femmes journalistes interviewées s'auto-censurent sur les réseaux sociaux en raison des cyberviolences contre les femmes en ligne.[45] Il en résulte que la CVCF limite la participation publique des femmes et leur leadership, **les voix des femmes sont réduites au silence, discréditées et censurées**.

LE CADRE JURIDIQUE ET POLITIQUE SUR LA CYBERVIOLENCE CONTRE LES FEMMES

NIVEAU INTERNATIONAL

Au niveau international, les Nations unies (ONU) et le Conseil de l'Europe (CoE) ont abordé les cyberviolences contre les femmes. L'instrument juridique principal est la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (**Convention d'Istanbul**).[46] L'UE a adhéré à la convention d'Istanbul en juin 2023, six ans après sa signature, déclenchant l'entrée en vigueur de la Convention pour l'UE le 1er Octobre 2023.[47] Malgré cette ratification de l'UE, cinq pays membres de l'UE[48] ne l'ont pas encore ratifiée.

Alors que la Convention ne se réfère pas aux cyberviolences contre les femmes, son champ d'application, comme défini dans l'Article 2, s'étend aux violences commises dans les espaces en ligne et au moyen des TICs. Pourtant les articles sur le harcèlement sexuel (Art. 40) et les traques furtives (Art. 34) s'appliquent à la cyberviolence contre les femmes. La Convention doit être interprétée à la lumière de **la recommandation n.1 du Grevio**[49] qui catégorise les manifestations des violences contre les femmes dans la sphère numérique comme des expressions de la violence basée sur le genre (VBG) couvertes par la Convention d'Istanbul.

NIVEAU DE L' UE

Au niveau de l' UE, le principal instrument législatif est la **Directive 2024/1385 sur la lutte contre la violence à l'égard des femmes et la violence domestique**,[50] adoptée par le Parlement européen et le Conseil de l'UE en avril 2024.Cette dernière contient quatre articles dédiées aux cyberviolences contre les femmes : Article 5 sur le partage de contenus intimes ou retouchés ; Article 6 sur la traque furtive ; Article 7 sur le cyberharcèlement et Article 8 sur la cyber incitation à la violence et à la haine. La Directive définit aussi les droits des victimes de toutes sortes de violences contre les femmes et violences domestiques et assure leur protection.[51]

La Directive peut être considérée **comme un pas en avant important pour mieux protéger les femmes et les filles des cyberviolences**. Elle **marque une amélioration significative** en cherchant à introduire des règles minimums en ce qui concerne ces formes de cyberviolence.[52] Parmi ses points forts, la Directive englobe dans un instrument unique à la fois les formes de violence contre les femmes hors ligne et en ligne. En outre, les deux formes, celle où la victime connait habituellement l'agresseur, (par exemple, traque furtive, harcèlement) et celle où la victime ne connait pas l'agresseur (par exemple haine, « deepfakes ») sont couvertes.

En dépit de ses points forts, la **Directive a des limites et a été l'objet de critiques**. Par exemple, les articles 5-8 sur les cyberviolences contre les femmes, reposent sur des **conduites intentionnelles**. Cette référence pose quelques problèmes juridiques car l'intentionnalité de l'acte doit être prouvée. Cela place **une charge de la preuve importante sur les victimes de cyberviolences**, en considérant également la complexité des nouvelles technologies utilisées pour commettre des cyberviolences et le fait que les victimes peuvent man-

quer de compétences en matière de technologies de l'information et de la communication (TIC). En outre, les articles 5, 6 et 7 font référence à un "**préjudice grave**". Cette condition crée une incertitude juridique pour les victimes dans les différents pays et à l'intérieur de ceux-ci, laissant à la discrétion de l'appareil judiciaire la décision sur quelles conduites sont punissables. Cette formulation est basée sur un manque de reconnaissance de la dangerosité des cyberviolences.[53]

De plus, les Article 5 et 7 font référence au fait de rendre accessibles **au public** certains contenus par le moyen des TIC. Le considérant 18, relatif à l'article 5 laisse l'interprétation du terme « public » à la discrétion du juge selon les circonstances et les technologies utilisées qui pourrait **risquer d'exclure par exemple les groupes Whatsapps**. Le Considérant 26, en relation avec l'article 8, établit au contraire que « public » doit être compris comme **un nombre illimité d'utilisateurs et d'utilisatrices**. Le terme plus large « les utilisateurs finaux et utilisatrices finales », comme l'a suggéré le Parlement européen, aurait été préférable ainsi que l'a clairement signifié le LEF.[54]

L'Article 5(b) sur le partage non consenti de contenus retouchés a aussi une portée limitée: Il s'applique seulement aux contenus où la personne apparait être **« engagée dans des activités sexuelles ». En conséquence, il exclut les nus, ignorant l'étendue d'une grande partie des faux sexuels numériques**. De plus ce qui peut donc constituer des « activités sexuelles » peut varier considérablement entre les pays membres et donner lieu à une confusion dans la définition.

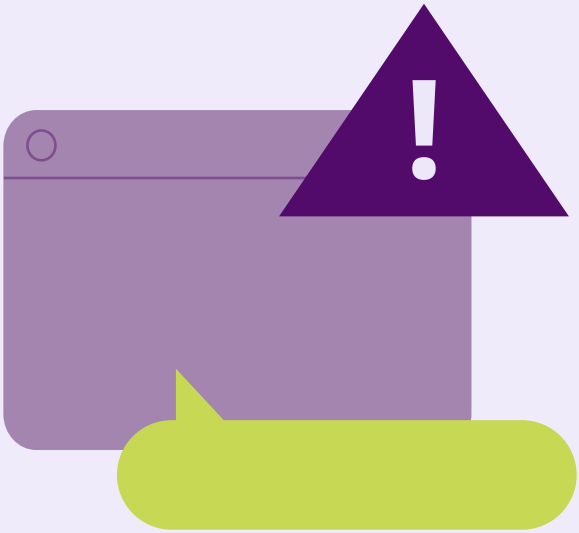
Les références aux exceptions liées à **« la liberté d'expression »** et la **« liberté artistique et scientifique »** dans l'article 5 et le Considérant 20 sont aussi inquiétants alors qu'ils pourraient être utilisés pour justifier un partage de contenus non-consenti. L'inclusion de ces exceptions peut supprimer l'efficacité de cet article en laissant le choix aux autorités judiciaires de criminaliser ou non le partage non consenti d'images intimes. Selon le LEF, la notion de liberté d'expression ne devrait pas devenir un moyen de justification de la haine et de la discrimination sexuelle.[55] Le retrait rapide de contenus nocifs est prévu dans l'Article 23 de la Directive sur les violences à l'encontre des femmes et les violences domestiques; de telles mesures complètent l'action menée dans le cadre d'un autre instrument clé dans le domaine numérique, **le Règlement sur les services numériques**[56] (DSA). Ce dernier, adopté en Octobre 2022, a pour objectif de créer un environnement en ligne plus sûr pour ls consommateurs et consommatrices et les entreprises de l'UE. Elle définit des responsabilités claires pour les plateformes en ligne et les réseaux sociaux; elle traite des contenus et produits illégaux, des discours de haine et de la désinformation. Elle augmente également la transparence avec de meilleurs rapports et un meilleur contrôle.

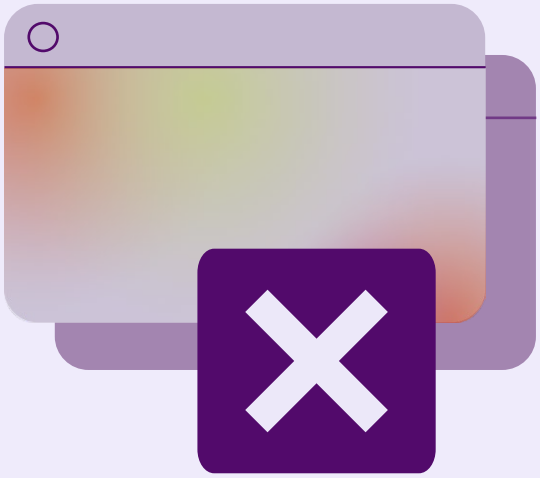
Selon des universitaires,[57] le Règlement européen sur les services numériques (DSA) peut être considéré comme une reconnaissance de la prévalence et des dommages résultant d'images basées sur les agressions sexuelles. La violence basée sur le genre est reconnue comme un important macro-domaine **de risques** parmi d'autres risques. Dans cet important macro-domaine des violences basées sur le genre, **la Commission est en train de créer des catégories spécifiques**[58] **dans le cadre de la Commission du "Paquet de rapports sur la transparence"**. Un autre développement positif du DSA est le fait que **la Commission a désigné, en référence au DSA, trois plateformes pornographiques (PorhHub, XVideos et Stripchat) comme de très grandes plateformes en ligne** en décembre 2023.[59] Cette désignation s'accompagne de responsabilités renforcées relatives à la transparence et à la protection des enfants.

D'AUTRE INSTRUMENTS LÉGISLATIFS DE L'UE POUVANT ÊTRE APPLIQUÉS DE FAÇON PERTINENTE AUX CYBERVIOLENCES CONTRE LES FEMMES EXISTENT :

- Le **Règlement européen sur l'intelligence artificielle** (IA),[60] adopté par le Parlement européen le 13 mars 2024. Alors que ce règlement représente une opportunité pour atténuer quelques-uns des risques posés par un mauvais usage de l'IA tels que les « deepfakes », elle ne contient pas de référence explicite aux cyberviolences contre les femmes. De plus, le Règlement ne se réfère à l'égalité femmes-hommes que de façon générale.[61]

- **La Directive sur les droits des victimes**[62] (Directive 2012/29/EU) encore en révision en 2024, qui déclare que toutes les victimes de crime (incluant les cyberviolences) et les membres de leur famille doivent être reconnues et traitées avec respect et sans discrimination en se basant sur une approche individuelle et personnalisée pour répondre aux besoins des victimes.





- **La Directive sur la prévention et la lutte contre le trafic d'êtres humains et la protection des victimes**[63] (Directive 2011/36/EU) qui a été remise à jour en avril 2024. La version révisée introduit le trafic d'êtres humains commis ou facilité par l'intermédiaire des TIC, y compris internet et les réseaux sociaux, comme une circonstance aggravante quand elle est reliée à l'exploitation sexuelle.

- **Le Règlement général sur la protection des données**[65](Regulation (EU) 2016/679) contient « un droit à l'effacement » plus connu comme le droit à être oublié. Pourtant le règlement ne définit aucune forme de cyberviolence, mais il fournit une protection aux victimes de la cyberviolence ; par exemple ; les victimes de partage non consenti d'images intimes et indique des sanctions à imposer à l'individu responsable du partage non consenti et contre l'éditeur de tels contenus. [66]

La Directive peut être considérée comme un pas en avant important pour mieux protéger les femmes et les filles des cyberviolences.

NIVEAU NATIONAL

Quelques Etats membres ont pris des mesures importantes pour prévenir et combattre certains aspects des cyberviolences contre les femmes au cours des cinq dernières années.[67] Par exemple en **France**, la cyberintimidation contre les femmes et les filles est considérée une nouvelle infraction pénale. En **Slovénie et en Pologne**, la législation criminalise les manifestations de cyberharcèlement, à la fois en ligne et hors ligne. Alors que **l'Italie** introduisait une nouvelle infraction pénale : la diffusion illégale d'images ou vidéos sexuellement explicites, **l'Autriche** adoptait un ensemble de mesures sur le discours de haine en ligne qui fournit de nouveaux outils pour traiter ce problème. En **Estonie**, une unité de police « les gendarmes du web » spécialisée dans le traitement du discours de haine et du cyberharcèlement a été créée. En **Irlande**, le projet de loi de 2021 sur le harcèlement, la communication nocive et les infractions connexes criminalise toutes les formes de partage non consenti d'images intimes, avec des peines de 10 ans de prison.

Hors de l'UE, **la Grande Bretagne a récemment adopté de nouvelles initiatives pour criminaliser le cyberflashing** (envoi d'images sexuelles non demandées) **et plus généralement les contenus illégaux en ligne** grâce à The Online Safety Act (loi de sécurité en ligne), qui a obtenu l'assentiment royal en 2023.[69]

LES DÉFIS CLEFS

Les défis suivants ont été identifiés:

- Le **manque de prise de conscience et la sous-estimation** de la gravité des cyberviolences à l'encontre des femmes sont des problèmes majeurs qui contribuent à la **sous-déclaration** des incidents.

- Au niveau international et au niveau de l'UE, il n'y a **pas encore une définition harmonisée des cyberviolences contre les femmes**. Il en résulte que **les définitions juridiques et statistiques des cyberviolences varient grandement** d'un pays à l'autre ou d'une organisation à une autre. En outre, la plupart des définitions sont **neutres du point de vue du genre et ne reconnaissent pas les liens entre la violence en ligne et la violence hors ligne.**

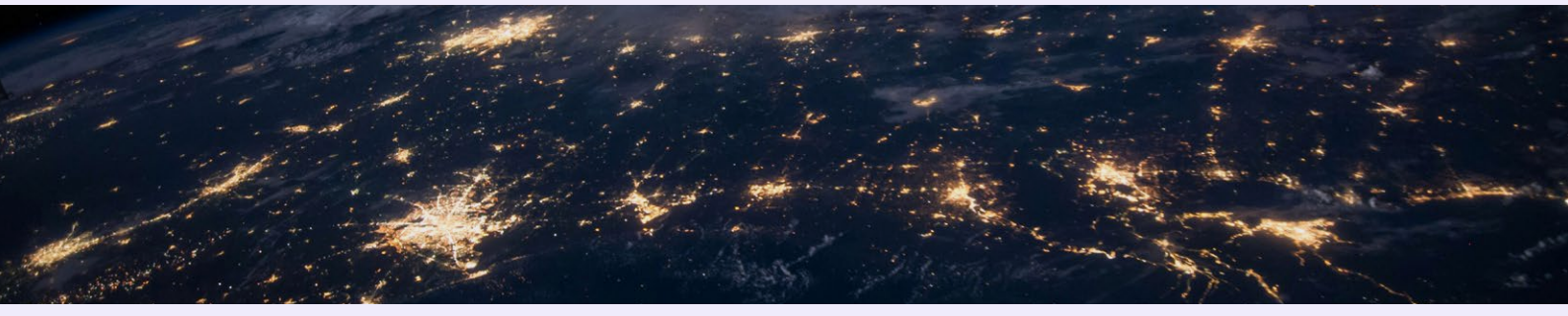
- Considérant la rapide évolution de la technologie, **les cadres législatifs sur les cyberviolences à l'encontre des femmes tendent à être dépassés très rapidement.**

- Le **manque de données sur les cyberviolences à l'encontre des femmes** est aggravé par le fait que **les données existantes sont souvent non ventilées** en fonction du sexe, de l'âge, de la relation entre la victime et l'agresseur, du handicap et d'autres critères pertinents.

- **La sous-représentation des femmes dans le secteur des TICs (technologies de l''information et de la communication) contribue à une absence de la dimension genrée dans les produits TIC,** y compris dans les jeux en ligne et les plateformes de réalité virtuelle, où les cyberviolences à l'encontre des femmes sont en augmentation.

- Il y a **peu de prise de conscience des cyberviolences à l'encontre des femmes et de ses différentes manifestations parmi les acteurs pertinents** y compris les juges, les magistrat.es, la police, les professionnel.les du soin et les éducateurs et éducatrices, qui **manquent d'une formation suffisante et d'une expertise spécifique.**

- **Les réseaux sociaux et les plate formes en ligne n'agissent pas toujours efficacement** pour retirer les contenus illégaux et préjudiciables. **Le système de signalement des plaintes des plateformes en ligne** ne sont pas toujours faciles à utiliser. Le résultat est que les victimes ne savent pas à qui elles peuvent demander de l'aide.



BONNES PRATIQUES POUR COMBATTRE LES CYBERVIOLENCES CONTRE LES FEMMES

De bonnes pratiques de différentes formes ont été identifiées à l'intérieur et au dehors de l'UE, ces dernières ayant été catégorisées par rapport à leur étendue et leur orientation. Un exemple de chaque pratique est décrit ci-dessous.

- **Renforcement des capacités:** En Slovénie, des séminaires et des sessions de formation ont été organisées pour les personnels chargés d'appliquer la loi et pour les juges avec l'objectif d'améliorer leur capacité à enquêter et sanctionner la dimension numérique de la violence contre les femmes et les filles. Un livret avec les lignes directrices sur la façon de traiter les cas de cyberviolence contre les femmes a aussi été adopté et diffusé à tous les commissariats et directions de police slovènes, aux bureaux des procureurs et aux tribunaux. [70]

- **Implication des institutions nationales sur les droits humains**: Les institutions nationales sur les droits humains jouent un rôle important dans la lutte contre les cyberviolences à l'encontre des femmes, particulièrement quand leur mandat leur permet d'enquêter sur les cas de discours de haine en ligne. En Belgique, l'Institut pour l'égalité entre les femmes et les hommes a déposé une plainte pénale contre une plate-forme de réseau social pour avoir refusé d'enlever des images intimes non consenties.[71]

- **Prévention**: Une étude[72] financée par le Conseil de recherches en sciences sociales et humaines (CRSH) et l'Héritage Canadien, révèle à quel point donner aux jeunes un pouvoir numérique peut être une force contre la vague croissante de la désinformation entretenue par les « deepfakes » et les technologies de l'intelligence artificielle. L'étude s'est concentrée sur la façon dont les jeunes perçoivent l'impact des « deepfakes » et a exploré leur capacité et leur volonté pour contrebalancer efficacement la désinformation.

- **Implication des survivants et survivantes**: La Reclaim Coalition to End Online Image-based Sexual Violence (la Coalition de réclamation pour mettre un terme à la violence sexuelle basée sur l'image en ligne) rassemble un réseau mondial de leaders pour accélérer la réponse mondiale à la violence sexuelle basée sur des images en ligne à travers des initiatives partagées au moyen de plaidoyers, par la politique, la technologie et des services pour les survivants et survivantes. La Coalition se réfère à des personnes ayant une connaissance de terrain de la violence sexuelle basée sur l'image comme « experts et expertes de l'expérience vécue ». La Coalition donne la parole aux survivants et survivantes et à leurs expériences.

- **Lignes d'écoute**: Access Now Digital Security Helpline (la ligne téléphonique d'aide Accès immédiat à la sécurité numérique)[73] aide les

femmes risquant des cyberviolences à améliorer leurs pratiques de sécurité numérique et fournit une assistance d'urgence pour les femmes subissant une attaque. Cette Digital Security Helpline (ligne de Sécurité numérique) ouverte 24h sur 24 et 7 jours sur 7 offre en temps réel une assistance technique directe et donne des conseils à des associations et des activistes de la société civile, des organisations de média, des journalistes, des blogueurs/blogueuses et des défenseur.es des droits humains.

- **Contrer le cyber sexisme et les discours de haine en ligne :** #StopFisha[74] est une association féministe française qui a pour but de lutter contre le cybersexisme. Elle a été créée comme soutien aux victimes et comme une alerte pour dénoncer le cybersexisme pendant l'épidémie du Covid19. Comme le mouvement continuait d'augmenter, #StopFisha est devenue une association qui s'attaque désormais à toutes les formes de cyberviolences sexistes et sexuelles.

- **Services d'aide spécialisés**: Dans plusieurs pays, des unités spéciales d'application de la loi, ayant une connaissance approfondie des cyberviolences contre les femmes, sont en cours de mise en place pour assurer des enquêtes de police efficaces et réactives et l'aide aux victimes. Des unités spécialisées pour l'application de la loi sont de plus en plus courantes en Amérique latine. Par exemple, la Police fédérale du Mexique a une division médico-légale responsable des enquêtes sur les cybercrimes, incluant les cyberviolences en ligne contre les femmes et les filles. De même, la Police nationale de Colombie inclut un Centre de police pour la cybernétique similaire et la Police fédérale du Brésil inclut un Bureau pour la suppression de la cybercriminalité.[75]

- **Suppression de contenus préjudiciables**: La UK Revenge Porn Helpline (RPH) (Ligne d'écoute sur la vengeance pornographique) en Grande Bretagne aide à empêcher que des personnes deviennent victimes d'abus d'images intimes dont la diffusion est non consentie. Depuis sa création, le RPH a aidé des milliers de victimes, avec un taux de retrait de l'Internet de 90% ; effaçant avec succès 200.000 images intimes pour des personnes qui n'avaient pas donné leur consentement à leur diffusion.[76]

RECOMMANDATIONS

Les recommandations qui suivent ont été formulées sur la base de recherches documentaires approfondies, l'examen de documents juridiques et politiques et la consultation de parties prenantes. Alors que des recommandations générales s'appliquent à toutes les parties prenantes dans le domaine des cyberviolences faites aux femmes, des recommandations spécifiques ont été élaborées pour les institutions de l'UE et les Etats membres.

RECOMMANDATIONS GÉNÉRALES

Renforcer les survivantes: Il est essentiel d'écouter la perspective des femmes survivantes de même que de les inclure dans le développement et l'application des programmes, politiques et la fourniture de services sur les cyberviolences faites aux femmes. Les survivantes font souvent face à la culpabilisation alors que la prévention des cyberviolences n'est pas de la responsabilité des femmes. Il est nécessaire d'agir avec une approche holistique qui comprend des outils juridiques pour protéger les victimes et prévenir les cyberviolences et qui demande aux grosses sociétés technologiques d'agir avec responsabilité. Une approche qui, de même, permet d'avoir une réponse coordonnée pour défier le sexisme et les normes culturelles afin d'éviter la culpabilisation des victimes.

Améliorer la participation des femmes dans le secteur technologique: Il est crucial d'assurer la participation des femmes à la création de produits tenant compte de l'égalité des femmes et des hommes. Ceci inclut la production de technologies dans lesquelles les femmes ne sont pas sexualisées et où des mécanismes d'alertes sûrs et accessibles de même que l'accès au support sont facilement disponibles.

Intensifier la coopération des divers parties prenantes: Renforcer la coopération entre un large spectre de parties prenantes (les acteurs de l'UE, les Etats membres, le secteur technologique, la société civile, les survivantes des cyberviolences contre les femmes, les institutions nationales des droits humains, les associations des droits des femmes etc....) pour traiter efficacement des cyberviolences contre les femmes, au moyen de partenariats clés et d'actions coordonnées éviterait les chevauchements et lacunes dans les actions. Les échanges permanents de la connaissance et la coopération des acteurs clés sont essentiels, y compris apprendre de pays qui ont des systèmes plus avancés pour lutter contre les cyberviolences faites aux femmes.

S'assurer que le secteur de la technologie, en particulier les plateformes en ligne et les ré-

seaux sociaux remplissent leurs obligations: Les réseaux sociaux. et les plateformes en ligne doivent être responsabilisés dans la lutte contre les cyberviolences à l'encontre des femmes. Le secteur de la technologie doit de façon proactive et efficace contrôler et retirer les discours de haine sur le genre, les contenus sexistes et misogynes et autres formes de cyberviolence contre les femmes. Il devrait aussi renforcer la coopération avec les forces de l'ordre actrices de l'application de la loi pour traiter de façon adéquate le cas de cyberviolences contre les femmes. De plus, elles devraient fournir aux utilisateurs et utilisatrices des ressources efficaces pour qu'elles et ils puissent identifier et intervenir contre les agressions en ligne. En bref, une transparence et une responsabilité, des retraits plus rapides des contenus illégaux, la sécurité pour la production et la prévention sont nécessaires de la part des sociétés technologiques, des plateformes en ligne et des réseaux sociaux, y compris les plateformes pornographiques.

Considérer la pornographie dans le continuum des violences faites aux femmes: le LEF dénonce le commerce de la pornographie et souligne les énormes profits financiers réalisés par l'industrie de la pornographie, en complicité avec le système prostitutionnel. Le LEF plaide pour que l'UE et les Etats membres agissent pour que la pornographie soit reconnue comme une forme de violence contre les femmes.

RECOMMANDATIONS POUR LES INSTITUTIONS DE L'UE

Harmoniser les définitions et les catégories des cyberviolences contre les femmes au niveau de l'UE et dans toutes les institutions de l'UE de façon à corriger les différences existantes dans les systèmes juridiques nationaux, différences qui font obstacle à une protection et à une sanction efficaces et impactent négativement le recueil de données. A ce jour, la seule tentative d'harmoniser les définitions juridiques et statistiques de la cyberviolence contre les femmes a été effectuée par l'EIGE [77](Institut européen pour l'égalité de genre). Les définitions de l'EIGE devraient être adoptées par toutes les institutions de l'UE.

Développer des lignes directrices et des indicateurs pour la collecte de données sur les cyberviolences à l'encontre des femmes: l'UE devrait développer des lignes directrices et des indicateurs clairs pour aider les Etats membres dans leurs efforts de recueil de données sur les cyberviolences contre les femmes, comme cela est fait actuellement par l'EIGE.

Améliorer la Directive de lutte contre la violence à l'égard des femmes et la violence domestique: à l'avenir et étendre sa portée. Dans l'ensemble, la directive peut être considérée comme un instrument valable pour protéger les femmes des principales formes de cyberviolences contre les femmes. Pourtant, quelques améliorations devraient être apportées dans le contexte de futures mises à jour de la Directive. En considérant les liens entre la cyberviolence et le viol, le viol comme rapport sexuel effectué sans un consentement libre devrait être inclus dans le texte. Les références à l'intentionnalité des conduites et au « grave préjudice » devraient être éliminées alors qu'elles imposent une lourde charge sur la victime. La production et la diffusion de contenus pornographiques décrivant des violences sexuelles devraient être incluses dans la révision de la Directive puisque c'est une forme d'exploitation sexuelle.

Un changement culturel systémique est nécessaire pour lutter contre les cyberviolences contre les femmes dans un perspective de genre, intersectionnelle et comme un continuum de la violence.

L'étendue de la criminalité devrait être élargie pour couvrir toutes les formes d'agressions sexuelles basées sur des images, y compris la pornographie.

Mettre à jour la législation existante de l'UE pour lutter contre la nature genrée des cyberviolences: La Directive sur les droits des victimes devrait être mise à jour avec pour objectif d'incorporer des articles spécifiquement dédiés aux cyberviolences et leur dimension genrée. La Décision cadre de 2008 sur la lutte contre certaines formes et expressions de racisme et de xénophobie devrait aussi être révisée pour incorporer la référence aux discours de haine sexiste au moyen des TIC.

Renforcer efficacement le Règlement européen sur les services numériques (DSA): La Commission européenne a des pouvoirs d'exécution et d'enquête relatifs aux obligations émises dans la DSA. Il est crucial que la Commission exerce efficacement ces pouvoirs (incluant l'imposition de sanctions financières), en coopération avec les Coordinateurs nationaux des services numériques (CSN), de façon à garantir que les plateformes en ligne et les services intermédiaires remplissent leurs obligations en conformité avec le DSA.

Incorporer une référence aux cyberviolences contre les femmes dans le Règlement européen sur l'intelligence artificielle: à la lumière de la prolifération des fausses images sexuelles numériques (« deepfakes ») et autres formes de violences contre les femmes au moyen de l'IA, il est recommandé d'urgence que les futures mises à jour du Règlement sur l'IA s'attaquent aux cyberviolences au moyen d'une approche exhaustive faisant référence au genre.

Publier régulièrement des conseils sur les nouvelles formes de cyberviolences contre les femmes: étant donné l'accroissement des formes de cyberviolences contre les femmes, facilitées par l'intelligence artificielle, et l'incapacité des cadres juridiques et politiques à suivre le rythme des nouveaux développements des TIC, l'UE devrait publier régulièrement des conseils sur la manière de traiter de façon efficace les dernières formes de cyberviolences contre les femmes.

RECOMMANDATIONS POUR LES ETATS MEMBRES

Aligner les définitions nationales des cyberviolences contre les femmes sur les définitions tenant compte du genre harmonisées de l'UE: Les Etats membres devraient incorporer les définitions et catégories des cyberviolences contre les femmes harmonisées dans leur propre cadres juridique et politique de même que dans leur sys-

tème statistique et de collecte de données pour garantir un recueil de données comparable entre les pays.

Collecter des données de qualité sur les cyberviolences contre les femmes de façon régulière: suivant l'Article 11 de la Convention d'Istanbul et l'article 44 de la Directive sur les violences contre les femmes, les Etats membres devraient collecter des données sur les cyberviolences faites aux femmes de bonne qualité comparables et genrées, suivant les lignes directrices de l'EIGE.

Ratifier et appliquer la Convention d'Istanbul: la Convention est un instrument clé pour protéger toutes les femmes de toutes les formes de violences y compris la cyberviolence contre les femmes. Il est donc important qu'elle soit mise en œuvre par tous les Etats membres. En outre, en suivant la recommandation n.1 du GREVIO, les Etats membres devraient assurer la reconnaissance de la dimension numérique des violences faites aux femmes dans les stratégies programmes et plans d'action nationaux sur les violences faites aux femmes comme faisant partie de la réponse holistique à toutes les formes de violence.

Renforcer la prévention dans un large sens: il est crucial de s'attaquer aux stéréotypes et normes de genre à un niveau sociétal plus étendu y compris par le biais de l'autonomisation des femmes. Les Etats membres devraient augmenter la prise de conscience sur les manifestations et les conséquences des cyberviolences contre les femmes parmi les professionnels.

La prévention et la sensibilisation aux cyberviolences contre les femmes devraient aussi être intégrées dans les programmes scolaires dès le plus jeune âge, à la fois pour les garçons et pour les filles.[78]

En outre, comme le recommande le LEF dans son rapport,[79] il est essentiel de mettre en place une éducation obligatoire aux relations et à la sexualité dans une perspective féministe. Eduquer les hommes et les garçons sur les formes, la gravité et les conséquences des cyberviolences contre les femmes est aussi crucial. En général, un changement culturel systémique est nécessaire pour lutter contre les cyberviolences contre les femmes dans un perspective de genre, intersectionnelle et comme un continuum de la violence.

Criminaliser les cyberviolences contre les femmes selon la Directive sur les violences faites aux femmes: Il est recommandé aux Etats membres de criminaliser les principales formes de cyberviolence contre les femmes dans la droite ligne des Articles 5 à 8 de la Directive sur les violences faites aux femmes et de tenir leur législation à jour au rythme des développements de la technologie. Les Etats membres, lors de la phase de transposition, devraient aller au-delà des normes minimums de protection établies par la Directive.

Contrôler et renforcer efficacement la conformité avec la DSA: Il est essentiel que les coordinateurs nationaux du service numérique contrôlent et renforcent la conformité avec la DSA. Ceci inclut l'imposition d'amendes, et, dans des cas particulièrement graves, la restriction d'accès au service pour des utilisateurs.

Assurer la responsabilité: les lois et les politiques des Etats membres devraient assurer la responsabilité des agresseurs et la responsabilité du secteur technologique, y compris dans les cas d'actes

de cyberviolence transfrontaliers. L'application efficace du cadre législatif sur les cyberviolences contre les femmes est cruciale.

Améliorer l'accès des victimes aux recours: il est important de garantir des mécanismes de signalement sûrs et facilement accessibles à la fois en ligne et hors ligne, permettant aux femmes de rapporter les faits de cyberviolence. Une information sur les procédures juridiques et autres recours devrait être rendue facilement accessible aux victimes de la cyberviolence contre les femmes.

Fournir des services d'aide spécialisés: il est essentiel de renforcer les capacités des fournisseurs de services des différents secteurs à répondre à la nature unique des cyberviolences contre les femmes et aux besoins des survivantes. Des aides dotées d'une expertise dans les TIC, centrées et spécialisées sur les survivantes devraient être assurées au moyen de financements et de ressources adéquats. Il est nécessaire de fournir une éducation obligatoire et continue et de la formation à tous les professionnels concernés afin de les équiper sur la connaissance des expressions numériques des violences contre les femmes pour leur permettre de répondre aux femmes sans leur causer une seconde victimisation et un nouveau traumatisme.

NOTES DE FIN

[1]EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[2]European Women's Lobby (EWL) (2017), #HerNetHerRights, Mapping the state of online violence against women and girls in Europe https://www.womenlobby.org/Read-and-share-HerNetHerRights-Resource-Pack-Report

[3]European Parliament Research Service (EPRS) (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

[4]EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[5]UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[6]Ibid

[7]World Wide Web Foundation (2021), Online Gender-Based Violence and Abuse:Consultation Briefing. https://uploads-ssl.webflow.com/61557f76c8a63ae527a819e6/61_5585a9bb-feb8836d512947_OGBV_ConsultationBriefing.pdf

[8]European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020), Opinion on combatting online violence against women, Brussels. https://commission.europa.eu/document/download/eae53eb9-ca88-4fc0-8a6e-51e771c96f68_en?filename=opinion_online_violence_against_women_2020_en.pdf

[9]Professor Liz Kelly a été la première à établir le concept d « un continuum de la violence » dans son livre 'Surviving Sexual Violence' (1st ed.).(1988). Polity.

[10]European Parliament Research Service (EPRS) (2021), Combating Gender based Violence: Cyber Violence. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

[11]UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwo-men.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

[12]Ibid

[13]The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence

against Women. https://onlineviolencewomen.eiu.com/. A survey was conducted across 45 countries (a sample of 100 replies for each country).

[14]Le terme " deepfake " est une contraction de " deep-learning " (qui fait référence à une méthode d'intelligence artificielle) et de " fake (faux) " ; cette expression est entrée dans le jargon public en 2017 lorsqu'un agresseur a utilisé ce nom sur le site web Reddit en référence à des images et des vidéos qu'il manipulait avec l'IA pour insérer le visage de célébrités féminines dans des vidéos pornographiques sans leur consentement. Étant donné que le terme a été inventé par un agresseur et afin de mieux refléter la perspective des victimes et des féministes, le LEF préfère utiliser l'expression "fausses images sexuelles virtuelles", comme l'a suggéré Mary Anne Franks, professeure à la faculté de droit de l'université George Washington et présidente et directrice de la politique législative et technique de la Cyber Civil Rights Initiative, une organisation à but non lucratif qui se consacre à la lutte contre les violences et les discriminations en ligne. Toutefois, par souci de clarté et afin de respecter la source d'information originale, nous avons conservé dans certains cas la référence aux "deepfakes, mise entre parenthèses dans le présent rapport.

[15]European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. L'étude se réfère à des 'Non-consensual pornographic deepfakes'. Le LEF préfère utiliser le terme "fausses images sexuelles virtuelles». https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[16]World Economic Forum (2024), The Global Risk Report 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[17]Ibid. The EPRS (2021) study refers to 'Non-consensual pornographic deepfakes'

[18]Patrini, Georgio (2019), Mapping the Deepfake Landscape. Sensity. Le rapport se réfère à du « contenu représentant de la pornographie » ; toutefois, le LEF préfère se référer à du « contenu représentant la nudité ou des activités sexuelles explicites »https://giorgiop.github.io/posts/2018/03/17/mapping-the-deepfake-landscape/

[19]Ibid

[20]European Parliament Research Service (EPRS) (2021), Tackling deepfakes in European policy. https://www.europarl.europa.eu/RegData etudes/STUD/2021/690039/EPRS_STU(2021) 690039_EN.pdf

[21]Monash Lens (2022), Sexual assault in the metaverse is part of a bigger problem. https://lens.monash.edu/@politics-society/2022/07/22/1384871/sexual-assault-in-the-metaverse-theres-nothing-virtual-about-it

[22]Information fournie par un représentant de DG Connect (interview effectué le 16.02.2024)

[23]Rothermel, A.-K. (2023), The role of evidence-based misogyny in antifeminist online communities of the 'manosphere'. Big Data & Society, 10(1). https://journals.sagepub.com/doi/10.1177/20539517221145671

[24]Baron & Straus (1984), in Mary Anne Layden. Pornography and Violence: a new look at research, 2009. https://www.socialcostsof pornography.com/Layden_Pornography_and_Violence.pdf

[25]UN Women (2023), Accelerating Efforts To Tackle Online And Technology Facilitated Violence Against Women And Girls. https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf

[26]Hicks, J. (2021), Global evidence on the prevalence and impact of online gender-based violence (OGBV).

[27]The Economist Intelligence Unit (2021), Measuring the Prevalence of Online Violence against Women. https://onlineviolencewomen.eiu.com/ Une enquête a été conduite parmi 45 pays (un échantillon de 100 réponses pour chaque pays) https://opendocs.ids.ac.uk/articles/report/Global_Evidence_on_the_Prevalence_and_Impact_of_Online_Gender-based_Violence_OGBV_/26428096?file=48181987

[28]FRA (European Union Agency for Fundamental Rights) (2014), Violence against Women: An EU-wide survey – Main results report, Publications Office of the European Union, Luxembourg.https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[29]FRA (2021), Crime, Safety and Victims' Rights – Fundamental Rights Survey. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

[30]HateAid (2021), Boundless hate on the internet – Dramatic situation across Europe. https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021_EN.pdf

[31]Ibid

[32]Bumble (2023), Bumble Backs Law to Ban Cyberflashing in 27 Countries. https://bumble.com/en/the-buzz/bumble-backs-law-to-ban-cyberflashing-27-countries-eu-europe

[33]Ipsos (2021), Les Français et le cyberharcèlement Ampleur du phénomène, conséquences, préoccupations et idées reçues. https://www.ipsos.com/sites/default/files/ct/news/documents/2021-12/Enquete%20Ipsos-Meetic.pdf

[34]FRA (2023), Online content moderation current challenges in detecting hate speech. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf

[35]Pew Research Centre, (2021), The state of online harassment. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

[36]GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[37]The global partnership (2023), Technology-Facilitated Gender-Based Violence: Preliminary Landscape Analysis. https://www.gov.uk/government/publications/technology-facilitated-gender-based-violence-preliminary-landscape-analysis

[38]UNESCO (2020), Online violence against women journalists: a global snapshot of incidence and impacts.https://unesdoc.unesco.org/ark:/48223/pf0000375136

[39]Ibid.

[40]Henry, N., McGlynn, C. ve diğerleri (2020), Image-based Sexual Abuse, A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery. https://www.routledge.com/Image-based-Sexual-Abuse-A-Study-on-the-Causes-and-Consequences-of-Non-consensual-Nude-or-Sexual-Imagery/Henry-McGlynn-Flynn-Johnson-Powell-Scott/p/book/9780367524401

[41]UN Expert Group (2023), Technology-facilitated Violence against Women: Towards a common definition Report of the meeting of the Expert Group 15-16 November 2022, New York, USA. https://www.unwomen.org/en/digital-library/publications/2023/03/expert-group-meeting-report-technology-facilitated-violence-against-women

[42]United Nations Population Fund (UNFPA) (2021), Making all spaces safe Technology-facilitated Gender-based Violence.https://www.unfpa.org/publications/technology-facilitated-gender-based-violence-making-all-spaces-safe

[43]Ibid.

[44]The European Liberal Forum (2021), Violence Against Women In European Politics https://liberalforum.eu/wp-content/uploads/2022/01/violence-against-women-in-european-politics_final.pdf

[45]Posetti, J., et AL. (2021). The chilling: Global trends in online violence against women journalists. UNESCO Research Discussion Paper. https://unesdoc.unesco.org/ark:/48223/pf0000377223/PDF/377223eng.pdf.multi

[46]Council of Europe, Convention on preventing and combating violence against women and domestic violence (Istanbul Convention). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

[47]European Parliament (2023), EU accession to the Istanbul Convention, https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739323/EPRS_ATA(2023)739323_EN.pdf

[48]Bulgaria, Czechia, Hungary, Lithuania and Slovakia.

[49]GREVIO (2021), General Recommendation No 1 on the digital dimension of violence against women, Council of Europe, Strasbourg. https://rm.coe.int/%20grevio-rec-no-on-digital-violence-against-women/1680a49147

[50]Directive 2024/1385 on combating violence against women and domestic violence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401385

[51]Council of the European Union (2024), Violence against women: Council and European Parliament reach deal on EU law. https://www.consilium.europa.eu/en/press/press-releases/2024/02/06/violence-against-women-council-and-european-parliament-reach-deal-on-eu-law/

[52]Rigotti, C. and Al. (2023), Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. Published in: New Journal of European Criminal Law. https://cris.vub.be/ws/portalfiles/portal/92354738/20322844221140713.pdf

[53]EWL (2023), Priorities for the Trilogues: Rape must be made an offence under the Directive on violence against women. https://www.womenlobby.org/EWL-Priorities-for-the-interinstitutional-negotiations?lang=en

[54]Ibid.

[55]Ibid.

[56]Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) https://eur-lex.europa.eu/legal-content/EN/

[57]Professor Clare McGlynn (2022), Image-Based Sexual Abuse, Pornography Platforms and the Digital Services Act. https://hateaid.org/wp-content/uploads/2022/04/ImageBasedAbuse-and-DSA-Expert-Opinion-McGlynn-and-Woods-17-Jan-2022.pdf

[58]Ces sous-catégories correspondent aux formes de cyberviolence qui peuvent être rapportées par les utilisateurs et utilisatrices tels que les traques furtives, le cyberharcèlement, le cyber flashing (consistant à envoyer des images sexuelles non sollicitées), les discours de haine, les images dont le partage n'est pas consenti etc...

[59]European Commission (2023), Commission designates second set of Very Large Online Platforms under the Digital Services Act. https://digital-strategy.ec.europa.eu/en/news/commission-designates-second-set-very-large-online-platforms-under-digital-services-actTXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG

[60]Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Règlement mettant en œuvre des règles harmonisées sur l'intelligence artificielle. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[61]Interview with a representative of DG Connect carried out on 16.02.2024. Interview avec un représentant de la DG Connect réalisé le 16.02.2024

[62]Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime. Directive établissant un minimum de normes sur les droits, l'aide et la protection des victimes de crime. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0029

[63]Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0036

[64]Ibid.

[65]Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement

of such data, (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[66]EIGE (European Institute for Gender Equality) (2022), Combating cyber violence against women and girls, Vilnius, Vilnius.

[67]Council of Europe (2022), No space for violence against women and girls in the digital world. https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

[68]Panorama Global (2023), I DIDN'T CONSENT: A Global Landscape Report on Image-Based Sexual Abuse, Prepared by: The Image-Based Sexual Abuse Initiative. https://assets-global.website-files.

[69]UK Parliament, House of Commons Library, Online Safety Bill: progress of the Bill. https://commonslibrary.parliament.uk/research-briefings/cbp-9579/

[70]Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

[71]Institut pour l'égalité des femmes et des hommes, Plainte au pénal contre Twitter pour la distribution non-consensuelle d'images intimes | Institut pour l'égalité des femmes et des hommes. https://igvm-iefh.belgium.be/fr/actualite/plainte_au_penal_contre_twitter_pour_la_distribution_non_consensuelle_dimages_

[72]Naffi, N. et Al. (2023), Empowering Youth to Combat Malicious Deepfakes and Disinformation: An Experiential and Reflective Learning Experience Informed by Personal Construct Theory, Journal of Constructivist Psychology. https://www.tandfonline.com/doi/full/10.1080/10720537.2023.2294314

[73]Panorama Global, The Reclaim Coalition. Last accessed in May 2024. https://www.panoramaglobal.org/reclaim

[74]Inach, #StopFisha. Last accessed in May 2024. https://www.inach.net/stopfisha/#:~:text=-Created%20in%20April%202020%20during%20the%20quarantine%2C%20the,given%20to%20the%20practice%20of%20disseminating%20intimate%20content.

[75]Council of Europe (2022), The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. https://www.coe.int/en/web/istanbul-convention/edvaw-platform

[76]StopNCII, About us. Last accessed in May 2024. https://stopncii.org/about-us/

[77]EIGE (2022), Combating cyber violence against women and girls. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en

[78]L' importance de la prévention a été soulignée par toutes les parties prenantes consultées. (voir l'Annex II du rapport complet)

[79]EWL (2020), Feminist Sexuality Education. https://www.womenlobby.org/IMG/pdf/lef_sexeduc_web.pdf