Violence basée sur le genre facilitée par la technologie

Rendre tous les espaces sûrs

Division technique
Décembre 2021

Remerciements

Alors que le monde continue d'évoluer et de s'étendre dans l'utilisation des technologies et des plateformes, il en va de même pour l'expansion des espaces dans lesquels la violence peut être perpétrée. La preuve en a été faite lors de la pandémie de COVID-19, où les efforts de confinement ont réduit l'accès à l'information et aux services, entraînant une utilisation accrue de la technologie et des espaces en ligne. Ce document est une sonnette d'alarme pour la communauté internationale, les mouvements numériques et féministes, les entreprises technologiques privées et les gouvernements nationaux, qui doivent agir à l'unisson pour mettre fin au fléau croissant de la violence sexiste facilitée par la technologie.

Au nom de l'UNFPA, le Fonds des Nations Unies pour la population tient à remercier les personnes suivantes pour le temps et l'expertise qu'elles ont consacrés aux discussions et à l'examen technique : le Dr Suzie Dunn, professeur adjoint en droit et technologie à la Schulich School of Law de l'Université Dalhousie, Sophie Read-Hamilton, consultante indépendante en matière de VBG, et Chandra Pauline Daniel, titulaire d'un doctorat en santé publique, politique et gestion de la santé, New York Medical College ; stagiaire en analyse des résultats du plan stratégique, PSIPB, Division des politiques et stratégies, UNFPA.

Ce rapport a été produit par la Division technique de l'UNFPA, Branche Genre et Droits de l'Homme, sous la direction technique d'Alexandra Robinson. Les co-auteurs du document sont Alexandra Robinson et Nora Piay-Fernandez, avec la révision de Sarah Baird, Mar Jubero, Dawn Minott et Jude Larnerd.

Violence basée sur le genre facilitée par la technologie

Rendre tous les espaces sûrs

Decembre 2021

Liste des acronymes

ABI	Abus basé sur l'image
GPS	Global Positioning System (Système mondial de positionnement)
HCDH	Haut-Commissariat des Nations unies aux droits de l'homme
IA	Intelligence artificielle
LGBTQIA+	Lesbienne, Gay, Bisexuel, Trans, Queer, Intersexuel, Asexué, Autre
VBG	Violence basée sur le genre
VBG	Violence basée sur le genre facilitée par la technologie
VPI	Violence entre partenaires intimes
UNFPA	Fonds des Nations Unies pour la Population

Table des matières

Partie 1

Qu'est-ce que la VBGFT

Définition, prévalence et impact

Contexte

L'émergence de la technologie et des espaces numériques, ainsi que la dépendance à leur égard, est une tendance lourde mondiale,[1] un phénomène universel qui façonne notre monde actuel. La numérisation entraîne des changements structurels dans la façon dont les gens communiquent, travaillent, apprennent, produisent et consomment. L'innovation technologique et la numérisation ouvrent une fenêtre d'opportunités pour le développement durable, à une époque où de nombreux aspects de la vie humaine sont radicalement transformés.[2] La technologie a le potentiel de favoriser la croissance économique, d'élargir l'accès à l'éducation, à l'information et à la connaissance, et de donner une voix et un pouvoir à ceux qui sont le plus à la traîne ainsi qu'à ceux dont la voix n'a pas été traditionnellement entendue, renforçant ainsi la participation à la vie publique et aux processus démocratiques.

Toutefois, si la numérisation du monde représente une opportunité importante, c'est aussi un espace dans lequel le mal peut être perpétré. Les recherches indiquent qu'au moins 38 pour cent des femmes dans le monde ont été personnellement victimes de violence en ligne et que ce taux est en augmentation.[3] La violence basée sur le genre facilitée par la technologie (VBGFT) vise toutes les femmes qui utilisent la technologie, y compris les femmes *cis et trans*, ainsi que les personnes qui se présentent comme des individus féminins, non binaires ou de genre divers.[4] Certains groupes de femmes courent un risque plus élevé en raison de ce qu'elles font, de qui elles sont ou si elles accèdent à certaines informations et services. Il s'agit par exemple des femmes journalistes, des politiciennes, des femmes activistes et des féministes, des universitaires et des jeunes.[5] Parmi les adolescentes qui ont accès aux technologies numériques, 64 pour cent sont de grandes utilisatrices et sont particulièrement vulnérables à la VBGFT.[6] La violence à l'égard des femmes et des filles est plus fréquente si elles souffrent d'un handicap, si elles sont racisées, LGBTQIA+, si elles sont défavorisées sur le plan socio-économique et/ou si elles ont un franc-parler politique.[7]

Selon les mots du Fonds d'action et d'éducation juridique pour les femmes :

> La présence partout de l'internet signifie que la VBGFT peut devenir omniprésente et incessante, s'infiltrant dans les espaces physiques les plus intimes de la victime, comme son domicile ou sa chambre. Les utilisateurs qui se livrent à la VBGFT peuvent également tirer parti de leurs propres réseaux sociaux en ligne et de ceux des personnes ciblées pour faire progresser les abus, en recrutant d'autres personnes pour qu'elles partagent sciemment ou involontairement du matériel abusif, et en contaminant les espaces et les communautés en ligne des personnes ciblées. La permanence en ligne du contenu abusif - qu'il est extrêmement difficile d'éliminer complètement une fois qu'il est partagé en ligne - garantit également une revictimisation continue, entraînant des dommages psychologiques et autres dommages durables[8]

En outre, la VBGFT peut prendre de nombreuses formes et est commise sur un continuum. En d'autres termes, elle est commise dans le cadre d'un ensemble de violences perpétrées à la fois en ligne et hors ligne.[9]

La lutte contre la VBGFT, qui est un sujet de préoccupation croissante, n'est plus négociable. Pour que les femmes puissent exercer efficacement leur droit à la liberté d'expression, il est essentiel de veiller à ce que chacun puisse participer librement en ligne et sans craindre la violence et les abus. Le Conseil des droits de l'homme des Nations unies a déclaré que «les mêmes droits dont jouissent les personnes hors ligne doivent également être protégés en ligne, en particulier la liberté d'expression, qui s'applique sans considération de frontières et par le biais de tout média de son choix, conformément aux articles 19 de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques».[10] Plus précisément, le principe selon lequel les droits humains et les droits des femmes protégés hors ligne doivent également être protégés en ligne, devrait intégrer pleinement le droit de vivre à l'abri des formes émergentes de violence à l'égard des femmes en ligne et facilitées par les technologies de l'information et de la communication, tout en respectant le droit à la liberté d'expression et le droit à la vie privée et à la protection des données.[11]

L'utilisation de la technologie et des espaces en ligne devrait servir d'outil pour accélérer la réalisation de l'égalité des sexes et l'autonomisation des femmes, au lieu d'être un outil d'assujettissement, de perpétration de violences et de réduction au silence des femmes dans toute leur diversité.

Définition de la VBGFT

Il n'existe pas de consensus mondial sur une définition de la violence perpétrée à l'aide de la technologie et commise dans des espaces en ligne et numériques.[12] Une définition bien établie, internationalement acceptée et normalisée de la VBGFT est essentielle pour fournir une compréhension commune permettant une mesure normalisée et des normes minimales pour la réponse et la prévention.

Afin de contribuer à combler cette lacune critique dans les connaissances, l'UNFPA (le Fonds des Nations unies pour la population) a examiné les termes et définitions publiés par des organisations internationales, des universitaires et des organisations de la société civile au cours des cinq dernières années et a proposé une nouvelle définition de travail. S'appuyant sur ces définitions et leur complémentarité, l'UNFPA propose d'adapter le terme d'abus facilité par la technologie au terme plus large de VBGFT, défini comme suit :

> Un acte de violence perpétré par un ou plusieurs individus, commis, aidé, aggravé et amplifié en partie ou en totalité par l'utilisation des technologies de l'information et de la communication ou des médias numériques,[13] contre une personne en raison de son sexe.

Cette définition de travail exhaustive a été choisie parce que : (1) elle met en évidence la nature genrée de la violence ; (2) elle englobe les circonstances et les formes dans lesquelles la technologie peut être utilisée pour perpétrer la violence. Cette définition large et inclusive englobe les schémas existants de violence, de harcèlement et d'abus, ainsi que de nouvelles formes d'abus, comme l'abus basé sur l'image (ABI). En outre, cette terminologie permet de différencier la « *violence en ligne* » ou « *violence numérique* », en tant que violence perpétrée à l'égard des femmes dans des espaces en ligne ou par le biais de médias numériques, de la « *violence facilitée par la technologie* », qui est perpétrée par tout type de moyens technologiques, de technologies de l'information et des communications et de médias numériques, y compris les téléphones, les dispositifs de repérage du système mondial de positionnement I (GPS), les drones et les appareils d'enregistrement non connectés à Internet.

Caractéristiques de la VBGFT

La VBGFT a des caractéristiques communes avec d'autres formes de violence basée sur le genre :

- elle est présente dans toutes les sociétés du monde ;
- elle est genrée et ancrée dans l'inégalité des sexes, ce qui a un impact disproportionné sur les femmes et les filles dans toute leur diversité ;
- elle peut avoir de graves répercussions sur la santé, le bien-être et la vie des survivants.

La VBGFT présente également des caractéristiques distinctes liées à sa nature numérique.[14]

Anonymat
L'auteur ou l'agresseur peut rester anonyme.

Action à distance
Elle peut être perpétrée à distance, de n'importe où dans le monde et sans contact personnel ou physique avec les victimes.

Accessibilité et prix abordable
Elle est accessible et financièrement abordable pour les auteurs, puisque les technologies de l'information et de la communication ont réduit le coût et la difficulté de produire et de distribuer des informations à grande échelle.

Propagation
Elle est constante et se propage facilement sur Internet, ce qui a pour effet de retraumatiser les victimes. La facilité, l'efficacité et le coût de l'automatisation et de la multiplication des cas d'abus à l'encontre d'un groupe ou d'un individu particulier en font une forme de violence efficace pour faire du mal.

Impunité
Elle est souvent perpétrée en toute impunité. Étant donné que la VBGFT peut être commise dans l'anonymat et à distance, il existe des difficultés d'application de la loi dans les pays et les juridictions qui limitent la capacité des systèmes judiciaires à tenir les agresseurs responsables de leurs actes.

Automatisation
Elle peut être automatique et facile à perpétrer, et permet aux auteurs de contrôler les mouvements des femmes, de surveiller leur activité en ligne et de distribuer des images ou des informations, entre autres actions abusives préjudiciables, avec un temps et des efforts limités.

Collectivité
Elle peut être organisée de manière collective et perpétrée par un grand nombre d'individus.

Normalisation de la violence
La VBGFT contribue à la normalisation de la violence à l'égard des femmes et des filles. La violence physique à l'égard des femmes est souvent normalisée et justifiée, notamment par les femmes elles-mêmes. En fait, dans 49 pays à revenu faible ou intermédiaire, 41 pour cent des femmes et 32 pour cent des hommes justifient la violence physique domestique dans au moins une circonstance.[15] Il est probable que cette normalisation de la violence soit exacerbée dans l'espace numérique, et que la VBGFT soit perçue comme moins grave, moins nuisible ou moins dangereuse pour les victimes.

Perpétuité
Elle peut être commise à perpétuité, car les images et le contenu numérique utilisés pour perpétrer des abus sont susceptibles d'exister indéfiniment ou pendant de longues périodes.

Les formes de VBGFT

La VBGFT est « exercée par le biais de textes, d'images et d'une surveillance et d'un suivi non désirés, activés ou renforcés par le numérique, à l'aide d'une variété d'appareils et de plateformes allant des outils numériques de base tels que les textos, les courriels et les réseaux sociaux, à des technologies plus avancées telles que l'intelligence artificielle (IA), le suivi GPS et les drones ».[16] Au fur et à mesure que de nouvelles technologies et de nouveaux espaces numériques deviennent disponibles, de nouvelles formes de VBGFT apparaissent, comme l'utilisation de l'IA pour l'ABI ou le harcèlement à l'aide du suivi GPS sur les téléphones portables.[17] Dans le même temps, d'anciennes technologies sont utilisées pour perpétrer des violences sous de nouvelles formes. Par exemple, dans le cadre de relations intimes abusives, les auteurs de violences utilisent les virements bancaires sur Internet pour envoyer des messages de harcèlement aux victimes.[18]

Parmi les formes les plus courantes de VBGFT, on peut citer, entre autres, les suivantes :[19]

le harcèlement en ligne, y compris le harcèlement sexiste et sexuel en ligne

Le harcèlement en ligne est l'utilisation de la technologie pour contacter, ennuyer, menacer ou effrayer une autre personne de manière répétée. Le harcèlement en ligne est un comportement continu dans le temps plutôt qu'un incident isolé.[20] Le harcèlement en ligne peut être perpétré par un seul individu ou par des bandes d'individus (*mobbing*), généralement des réseaux d'auteurs de sexe masculin qui ciblent les femmes et les minorités.[21] Lorsque le harcèlement en ligne est perpétré sur la base du sexe, de la sexualité ou de l'orientation sexuelle de la victime, il constitue une forme de VBGFT.[22]

Le harcèlement sexuel en ligne est une forme spécifique de harcèlement qui peut impliquer une attention sexuelle non désirée et une coercition sexuelle.[23] Il a également été défini comme « tout comportement sexuel non désiré via des moyens électroniques et peut inclure des sollicitations sexuelles non désirées, des demandes non désirées de parler de sexe, des demandes non désirées de faire quelque chose de sexuel en ligne ou en personne, la réception de messages et d'images sexuels non désirés, le partage de messages et d'images sexuels sans permission et la révélation d'informations d'identification et d'ordre personnel sur une personne en ligne » ;[24]

1

le cyberharcèlement, le pistage ou la poursuite et la surveillance cyberobsessionnelles

Le cyberharcèlement est « l'utilisation de la technologie pour traquer et surveiller les activités et les comportements d'une personne en temps réel ou dans le passé ».[25] Il est généralement considéré comme une extension du harcèlement hors ligne, avec des outils technologiques. De plus, il implique un ensemble de comportements non désirés, répétitifs, intrusifs, menaçants et harcelants, qui dans certains cas, sont considérés comme une pratique relationnelle ou amoureuse relativement normale. Certains chercheurs utilisent le terme « poursuite cyberobsessionnelle » pour désigner la « poursuite non désirée de l'intimité par une invasion répétée du sentiment d'intimité physique ou symbolique d'une personne, en utilisant des moyens numériques ou en ligne ». Ils considèrent aussi le cyberharcèlement comme une forme grave de poursuite et de surveillance cyberobsessionnelles, qui peut être motivée par le contrôle ou la destruction de la relation et provoquer un sentiment de peur chez la victime.[26]

Le cyberharcèlement consiste, par exemple, à surveiller ou à suivre la localisation et/ou les activités d'une personne à l'aide de traceurs GPS, de logiciels espions, de caméras et de microphones,[27] et d'applications de rencontres géolocalisées, à vérifier l'historique des courriels, des appels ou des messages, ainsi qu'à surveiller les profils d'une personne sur les réseaux sociaux ;[28]

l'abus base sur l'image

L'ABI consiste à « utiliser des images pour contraindre, menacer, harceler, chosifier ou abuser ». Une forme d'ABI est l'abus sexuel basé sur l'image,[29] qui implique au moins un des trois comportements suivants : prendre, partager ou menacer de partager des images sexuellement explicites sans consentement. Certains chercheurs ont plaidé pour l'inclusion d'autres formes d'abus sexistes et sexualisés, perpétrés à l'aide d'outils technologiques, tels que l'*upskirting*, ou la prise d'une image sous la jupe ou la robe d'une personne sans son consentement ; les *deepfakes* (hypertrucages) ou l'imagerie sexuelle créée sans son consentement qui dépeint la victime de manière sexuelle, généralement développée à l'aide d'outils d'intelligence artificielle, ainsi que le *cyberflashing* (cyberexhibitionnisme), qui est l'envoi d'images non sollicitées de ses propres organes génitaux à une autre personne.[30] D'autres exemples incluent le fait de photographier ou de filmer quelqu'un sans son consentement ou à son insu,[31] ou de contraindre quelqu'un à adopter un comportement sexuel non désiré en ligne ;[32]

les abus sexuels facilités par la technologie

Les abus sexuels facilités par la technologie désignent l'utilisation des technologies de la communication, telles que les téléphones portables, les courriels, les sites de réseaux sociaux, les salons de discussion ou les sites et applications de rencontres en ligne, pour commettre ou occasionner une agression ou un abus sexuel.[33] En général, les expériences sexuelles non désirées facilitées par la technologie impliquent trois comportements distincts : (1) la sextorsion ou le fait de contraindre quelqu'un à une activité sexuelle par le chantage, la corruption ou la menace de divulguer des images intimes ou des informations sensibles ; (2) l'utilisation de la technologie pour contacter une victime potentielle, par exemple par le biais d'applications de rencontre, pour ensuite commettre une infraction sexuelle ; et (3) le "viol par procuration", lorsque les délinquants sollicitent et organisent un tiers pour agresser sexuellement une personne, souvent en utilisant une fausse identité ou en se faisant passer pour la victime.[34] En outre, les abus sexuels facilités par la technologie peuvent impliquer la "coercition par sexting", lorsque les délinquants forcent une personne à s'engager dans l'envoi de textos sexuellement explicites non désirés ou le partage d'images et de vidéo, ainsi que dans la « sollicitation sexuelle non désirée », en recevant des demandes non désirées de parler de sexe ou de faire quelque chose de sexuel.[35]

Le *grooming en ligne* est un autre type spécifique d'abus sexuel facilité par la technologie, qui consiste à contacter des enfants et des jeunes par l'intermédiaire de réseaux sociaux ou d'autres plateformes numériques, dans le but de les agresser sexuellement. Il a été défini comme un « processus par lequel l'auteur de la violence prépare un enfant, des adultes importants et l'environnement pour l'abus. Il s'agit notamment d'avoir accès à l'enfant, d'obtenir son consentement et la préservation du secret de sa part pour éviter qu'il ne soit révélé » ;[36]

le *doxxing* ou *doxing*

Le doxing est la divulgation non consentie d'informations personnelles. Il implique la divulgation publique d'informations privées, personnelles et sensibles d'une personne, telles que son adresse personnelle et électronique, ses numéros de téléphone, les coordonnées de son employeur et des membres de sa famille, ou des photos de ses enfants et de l'école qu'ils fréquentent.[37] Le *doxing* est une forme de harcèlement en ligne qui se produit rarement de manière isolée, mais qui s'accompagne plutôt d'autres formes de harcèlement telles que l'ABI.[38] Les femmes, en particulier celles issues de groupes minoritaires, sont plus susceptibles d'être victimes de *doxxing*, qui touche de manière disproportionnée les femmes de couleur et les communautés LGTBQI+.[39] Selon Douglas, il existe trois types de *doxxing* : la désanonymisation, qui consiste à révéler l'identité d'une personne ; le ciblage, qui consiste à révéler des informations personnelles et privées permettant de localiser physiquement une personne, ce qui a des conséquences sexospécifiques et peut avoir de graves répercussions sur la sécurité de la plupart des femmes ; et la délégitimation, qui consiste à divulguer des informations privées dans le but de miner la crédibilité ou la réputation d'une personne, de lui faire honte et de l'humilier.[40] Le doxing entraîne souvent d'autres formes de harcèlement en ligne et physique, comme la réception d'un grand nombre de messages injurieux et de menaces par courriel, par téléphone ou par courrier postal ;[41]

le piratage

Le piratage est défini comme « l'utilisation de la technologie pour obtenir un accès illégal ou non autorisé à des systèmes ou des ressources dans le but d'acquérir des informations personnelles, d'altérer ou de modifier des informations, ou de calomnier et de dénigrer la victime et/ou les organisations de lutte contre la violence envers les femmes ».[42] L'ordinateur personnel ou le téléphone portable de la victime peuvent être piratés pour obtenir des images intimes afin de perpétrer un ABI, de la faire chanter ou de la contraindre à une activité sexuelle non désirée ou encore pour obtenir des informations privées qui peuvent être utilisées pour le doxxing ou d'autres actes de violence.[43] Les auteurs peuvent également pirater les comptes de messagerie et de réseaux sociaux d'une victime pour contrôler son activité en ligne, voire accéder à des comptes bancaires et contrôler les finances de la victime et/ou lui porter préjudice financièrement.[44] Les pirates peuvent également cibler les espaces en ligne des organisations de défense des droits des femmes, des militantes ou des personnalités publiques en raison de leurs opinions sur le féminisme, l'égalité des sexes ou les droits sexuels, limitant ainsi la participation des femmes aux forums en ligne et entravant leurs droits ;[45]

le recrutement et l'utilisation de la technologie pour localiser les victimes dans le but de perpétrer des violences

La technologie peut être utilisée pour attirer les victimes potentielles dans des situations de violence[46] ou pour faciliter des agressions physiques ou sexuelles en personne.[47] Les auteurs et les trafiquants peuvent utiliser la technologie pour contacter des victimes potentielles par le biais de messages et d'annonces frauduleux sur des sites et des applications de rencontre, des « agences matrimoniales » ou publier de fausses offres d'emploi et d'études.[48] Certaines technologies, comme les logiciels espions ou le suivi GPS, peuvent également être utilisées par les auteurs de violence entre partenaires intimes (VPI) pour suivre les mouvements et les activités des survivants, les surveiller, les contrôler et les localiser, dans le but de les intimider ou de les agresser physiquement.[49]

Cette forme de violence est également évidente dans la manière dont les femmes, les jeunes et les enfants sont attirés dans la traite.[50] On connaît également des cas de jeunes, d'enfants et d'adolescents, en particulier des filles, qui ont été recrutés en ligne par l'État islamique en Irak et en Syrie (ISIS) par le biais des réseaux sociaux, et attirés dans le mariage sous la promesse d'une vie utopique ;[51]

l'usurpation d'identité

L'usurpation d'identité consiste à voler l'identité de quelqu'un afin de le menacer ou de l'intimider, mais aussi de discréditer ou de porter atteinte à la réputation d'un utilisateur.[52] Les auteurs peuvent prendre le contrôle ou créer de faux comptes en ligne et de faux sites web de femmes pour diffuser de fausses informations et nuire à leur réputation,[53] pour ruiner leurs relations personnelles et/ou professionnelles,[54] pour appeler à la violence contre elles par le biais d'annonces de travail sexuel ou d'applications de rencontre[55] ou obtenir des informations sur la victime.[56] L'usurpation d'identité peut être perpétrée par des auteurs d'abus individuels, mais aussi par des acteurs étatiques. Par exemple, les acteurs étatiques ont la capacité de créer de faux comptes sur les réseaux sociaux ou d'usurper l'identité d'autres personnes dans le but de poursuivre les minorités et certains groupes, comme les personnes LGBTQIA+ ;[57]

le discours de haine

Le discours de haine est « tout type de communication par la parole, l'écrit ou le comportement, qui attaque ou utilise un langage péjoratif ou discriminatoire à l'égard d'une personne ou d'un groupe en raison de ce qu'ils sont, c'est-à-dire en fonction de leur religion, de leur appartenance ethnique, de leur nationalité, de leur race, de leur couleur, de leur ascendance, de leur sexe ou de tout autre facteur identitaire ».[58] Les discours de haine en ligne fondés sur le sexe et/ou l'orientation sexuelle renforcent le sexisme systémique tout en déshumanisant et en encourageant la violence contre les femmes et les filles. Ces dernières années, les discours de haine contre les femmes, les filles et les personnes LGTBQIA+ ont considérablement augmenté avec les plateformes de réseaux sociaux et les forums de discussion en ligne accueillant des groupes qui encouragent la haine et la violence contre les femmes ;[59]

la diffamation

10

La diffamation implique la diffusion publique de fausses informations qui portent atteinte à la réputation d'une personne et qui ont pour but d'humilier, de menacer, d'intimider ou de punir la victime.[60] Compte tenu des normes de genre strictes qui régissent la sexualité féminine, les déclarations diffamatoires sur la sexualité des femmes sont particulièrement préjudiciables à la réputation des victimes. En fait, la plupart des attaques diffamatoires en ligne contre les femmes et les filles portent souvent sur leur sexualité ;[61]

la limitation ou le contrôle de l'utilisation de la technologie

11

Dans les relations intimes abusives en particulier, les auteurs peuvent utiliser la technologie pour exercer un abus et un contrôle sur la victime, en suivant, surveillant ou limitant les mouvements, les communications et les activités de celle-ci. Ces comportements abusifs consistent notamment à forcer leur partenaire à donner ses mots de passe, à obtenir un accès non autorisé à ses comptes en ligne, à limiter son utilisation des appareils technologiques en contrôlant numériquement ou physiquement l'accès aux appareils ou aux comptes et à inspecter les appareils de la victime. Les partenaires intimes et les membres de la famille ont davantage accès aux appareils et aux informations personnelles d'une personne et peuvent exercer un pouvoir coercitif et un contrôle sur elle. Par exemple, les partenaires intimes peuvent connaître et surveiller les comptes bancaires et les réseaux sociaux de l'autre et partager des mots de passe et des appareils, volontairement ou non, avec l'autre. Dans les relations intimes abusives, les menaces qui pèsent sur l'utilisation de la technologie peuvent être le précurseur d'autres formes d'abus.[62]

Prévalence de la VBGFT

De plus en plus de recherches sont disponibles et mettent en évidence la prévalence des formes de VBGFT. Cependant, ces recherches utilisent des méthodologies et des outils d'enquête différents, ciblent des groupes de population différents et mesurent des formes spécifiques de VBGFT.

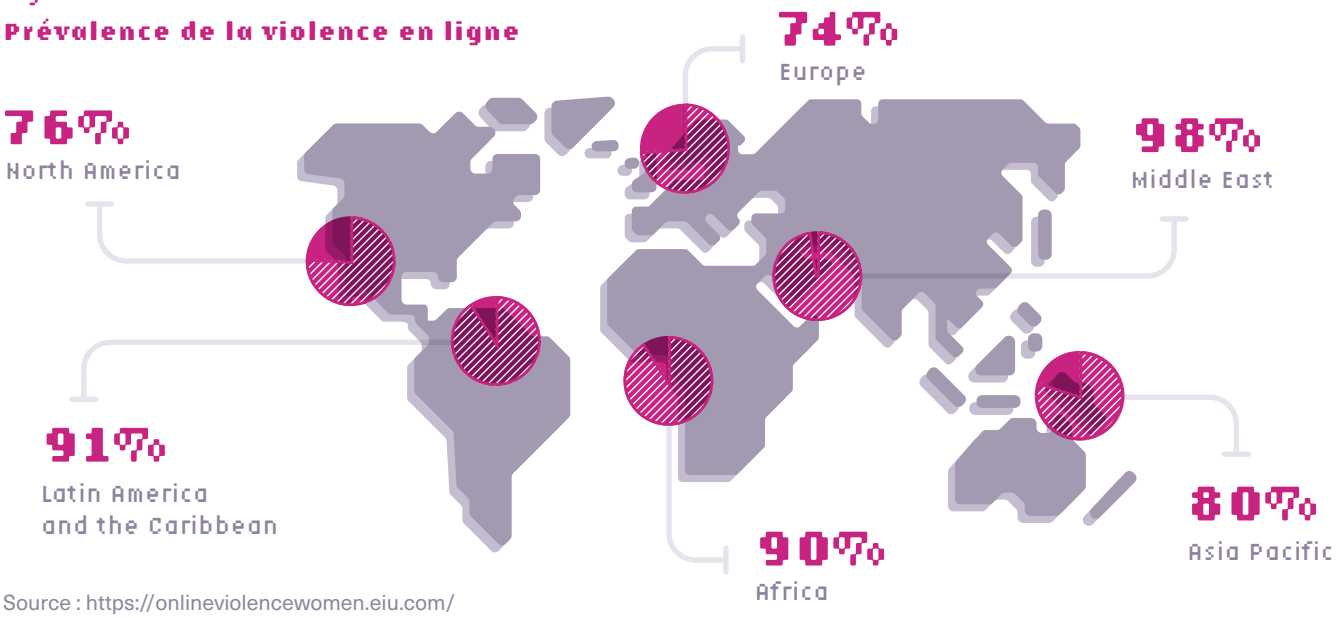
Mesurer l'ampleur et l'impact des actes de violence commis en ligne et/ou par des moyens numériques et technologiques est une tâche ardue, pour un certain nombre de raisons :

- l'absence d'une définition normalisée de la VBGFT et de ses différentes formes ;
- la prévalence peut être mesurée d'une manière qui ne tient pas compte du niveau d'accessibilité à la technologie et aux espaces numériques pour les femmes et les filles ;
- les formes de VBGFT qui ne cessent d'émerger au fur et à mesure que de nouvelles technologies apparaissent, que les anciennes technologies sont utilisées différemment et que de nouveaux espaces numériques et en ligne deviennent disponibles.

Tout cela mis ensemble signifie qu'il n'existe pas de mesure quantitative validée unique sur laquelle on puisse s'appuyer pour obtenir des données de prévalence aux niveaux local, national, régional et mondial[63] pour soutenir une politique fondée sur des preuves et des interventions de programmes (réponse et prévention) ainsi que des mesures de redevabilité.

Une étude récente menée par l'Economist Intelligence Unit en 2021 auprès des femmes des 51 pays ayant les taux de pénétration de l'Internet les plus élevés[64] a montré que, globalement, 38 pour cent des femmes ayant accès à l'Internet ont personnellement subi des violences en ligne, 63 pour cent connaissent quelqu'un qui en a été victime et 85 pour cent ont été témoins de violences en ligne perpétrées contre une autre femme.[65] Cette étude a également proposé des estimations régionales de la prévalence de la violence en ligne contre les femmes, comme le montre la figure 1.

Figure 1.
Prévalence de la violence en ligne



Source : https://onlineviolencewomen.eiu.com/

Il est probable que ces résultats sous-estiment la prévalence réelle de laVBGFT, étant donné que cette étude n'a pris en compte que la violence en ligne et n'a pas inclus d'autres formes de violence facilitée par la technologie et perpétrée par le biais de téléphones portables, du GPS et d'autres technologies. De plus, elle n'incluait que les femmes et non les adolescentes qui sont probablement plus exposées à la VBGFT. En effet, une étude menée par Plan International auprès de jeunes femmes et d'adolescentes (âgées de 15 à 25 ans) de 31 pays du monde entier a mis en évidence l'utilisation plus importante et plus fréquente des réseaux sociaux par les jeunes générations, augmentant ainsi l'exposition à la VBGFT . Le rapport a révélé que 58 pour cent des femmes et des filles âgées de 15 à 25 ans avaient été victimes de harcèlement en ligne.[66]

Bien que non exhaustif, un examen approfondi des enquêtes a été réalisé et figure dans la partie 3. Bien que le corpus de recherche soit restreint, les études ne mesurent généralement pas la VBGFT dans sa forme la plus inclusive mais examinent et mesurent des formes spécifiques de VBGFT. En outre, les données se limitent à des études localisées avec des échantillons de taille relativement réduite.

L'omniprésence de la VBGFT est une cause importante de préoccupation. Les données indiquent des estimations de prévalence de l'abus en ligne allant jusqu'à 58 pour cent,[67], ce qui est bien supérieur aux estimations mondiales actuelles de l'expérience de la violence entre partenaires intimes (VPI) et de la violence sexuelle sans partenaire au cours de la vie, qui est de 31 pour cent des femmes âgées de 15 à 49 ans.[68] Cela suggère que là où les taux de pénétration de l'Internet sont élevés et où les femmes et les filles ont accès à la technologie, les taux de VBGFT sont presque le double des taux de VPI. À mesure que la pénétration d'Internet et l'accès aux technologies augmentent, ces tendances devraient s'accentuer.

Outre la prévalence de la VBGFT, certaines données ont été recueillies sur les attitudes à l'égard de l'impact du harcèlement en ligne. Les résultats obtenus aux États-Unis ont montré une différence d'attitude entre les sexes : la moitié des femmes confirment que les contenus offensants en ligne sont trop souvent excusés comme n'étant pas significatifs, tandis que 64 pour cent des hommes et 73 pour cent des jeunes hommes, déclarent que les contenus offensants en ligne sont pris trop au sérieux.[69] Bien que limitée dans sa portée, cette recherche, tout comme les données de prévalence disponibles, est préoccupante et nécessite que des enquêtes similaires sur les attitudes soient entreprises à plus grande échelle.

Les données de prévalence disponibles, combinées à une compréhension limitée des impacts de la VBGFT et à l'absence de mécanismes de redevabilité et de réponses coordonnées, dressent un tableau sombre de l'état actuel de la perpétration et de la réponse à laVBGFT. Il est essentiel de se mettre d'accord sur des définitions standardisées et des méthodologies de collecte de données relatives à la VBGFT afin de disposer d'une base de données solide pour l'avenir.

58% 31%

Les données indiquent des estimations de prévalence de l'abus en ligne allant jusqu'à 58 %, ce qui est bien supérieur aux estimations mondiales actuelles de l'expérience de la VPI et de la violence sexuelle sans partenaire au cours de la vie, qui est de 31 % des femmes âgées de 15 à 49 ans.

Qui subit la VBGFT ?

Bien que les femmes et les filles soient les plus exposées à la VBGFT, certains groupes de femmes et de filles sont ciblés de manière disproportionnée. Il s'agit notamment des femmes handicapées, des adolescentes, des femmes de couleur, des femmes participant à la vie publique telles que les femmes journalistes ou les politiciennes et des personnes LGBTQIA+.[70]

Les adolescentes

La technologie occupe une place de plus en plus importante dans la vie des adolescents. Les adolescents, garçons et filles, utilisent la technologie et les plateformes en ligne pour apprendre et obtenir des informations et pour rester en contact avec leurs pairs.[71] Une étude menée par Plan International auprès de 14 000 filles dans 31 pays de toutes les régions a révélé que l'utilisation des réseaux sociaux est la plus fréquente à un jeune âge (15 ans),[72] bien que d'autres sources révèlent que les enfants vont en ligne à des âges beaucoup plus bas.[73]

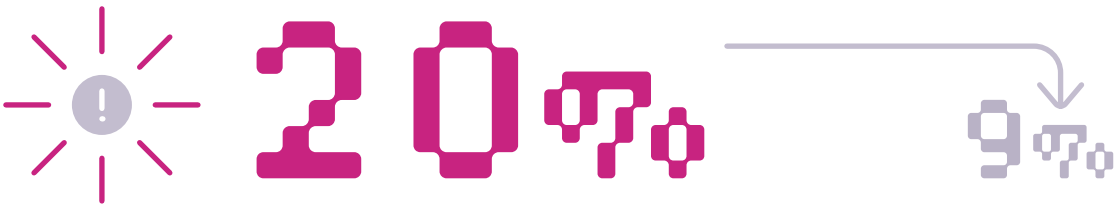
Les adolescentes constituent un groupe cible croissant soumis à la VBGFT en raison de leur engagement et de leur utilisation croissants des technologies et des espaces numériques.[74] Par exemple, 80 pour cent des images de documents relatifs à des cas d'abus sexuels sur des enfants concernent des filles âgées de 11 à 13 ans.[75] De plus, les adolescentes sont plus souvent victimes d'abus sexuels numériques dans le contexte de la violence dans les relations.[76] Pas moins de 58 pour cent des jeunes femmes et des adolescentes ont été harcelées en ligne, selon l'étude de Plan International, et 85 pour cent d'entre elles ont subi plusieurs types de VBGFT, notamment des propos injurieux et insultants (59pour cent), des humiliations corporelles (39 pour cent), des menaces de violence sexuelle (39 pour cent) et physique (21pour cent), du harcèlement sexuel (37 pour cent) ou de la traque furtive (32 pour cent).[77] Une autre étude réalisée par la World Wide Web Foundation et l'Association mondiale des guides et des éclaireuses a révélé que 52 pour cent des jeunes femmes et des filles ont été victimes d'abus en ligne et que 68 pour cent de ces abus ont eu lieu sur des plateformes de réseaux sociaux.[78] Bien que le harcèlement commence généralement entre 14 et 16 ans, certaines filles ont rapporté leur première expérience de VBGFT à l'âge de 8 ans. La VBGFT à l'égard des adolescentes est également intersectionnelle. Ainsi, un grand nombre de celles qui ont été harcelées et qui s'identifient comme faisant partie d'une minorité ethnique, des LGBTQIA+ ou de ceux en situation de handicap, ont déclaré avoir été harcelées à cause de cela.[79] En outre, l'utilisation des plateformes de réseaux sociaux peut avoir un impact négatif important sur la santé mentale des jeunes, en particulier des adolescentes.[80]

Les femmes dans la vie publique et professionnelle

Les femmes sont ciblées de manière disproportionnée par la VBGFT lorsque leur vie professionnelle est soutenue par une présence en ligne. Les femmes défenseurs des droits humains, activistes, journalistes, blogueuses, artistes et politiciennes, par exemple, sont des groupes de professionnelles et de dirigeantes qui sont touchés de manière disproportionnée par la VBGFT.[81] C'est particulièrement le cas lorsque les femmes et les professionnelles s'expriment sur les droits humains, le féminisme, le racisme et d'autres formes d'inégalités. Ces groupes de femmes utilisent des plateformes numériques et de réseaux sociaux pour soutenir leur vie professionnelle dans le cadre de leur engagement auprès du grand public. Les plateformes sur lesquelles elles s'appuient pour accroître le niveau de sensibilisation du public sont également utilisées par les auteurs pour menacer, harceler, traquer et promouvoir les discours de haine.[82]

Une enquête récente menée par l'UNESCO auprès de 901 journalistes dans 125 pays a révélé que 73 pour cent des femmes journalistes avaient subi des violences en ligne et que 20 pour cent d'entre elles avaient été attaquées hors ligne, en conséquence directe de ces violences en ligne.[83] De même, une étude mondiale de l'Union interparlementaire a montré que 41,8 pour cent des femmes en politique ont vu des images ou des commentaires à connotation sexuelle, diffamatoire ou humiliante les concernant être diffusés sur les réseaux sociaux, et 44,4 pour cent ont reçu des menaces de « mort, de viol, de coups ou d'enlèvement pendant leur mandat parlementaire ».[84]

Les femmes qui utilisent les plateformes numériques à des fins de militantisme et de défense d'une cause sont également visées de manière particulièrement disproportionnée. Pas moins de 88 pour cent des femmes interrogées dans le cadre d'une enquête menée au Royaume-Uni, qui utilisent régulièrement les réseaux sociaux pour exprimer leurs idées féministes, ont été victimes de VBGFT sur Twitter (60 % sur Facebook et 46 pour cent sur les blogs), sous la forme de trolls, d'insultes, de harcèlement et de menaces de violence physique et sexuelle.[85] En outre, l'âge est un facteur de protection dans la commission de la VBGFT. Comme l'a constaté Plan International, les jeunes femmes et les adolescentes qui s'expriment en ligne sur des questions politiques, le féminisme, la race ou la santé et les droits sexuels et reproductifs, sont confrontées à une réaction négative considérable. En fait, 47 pour cent des personnes interrogées dans l'enquête de Plan International ont déclaré avoir été attaquées pour leurs opinions.[86]

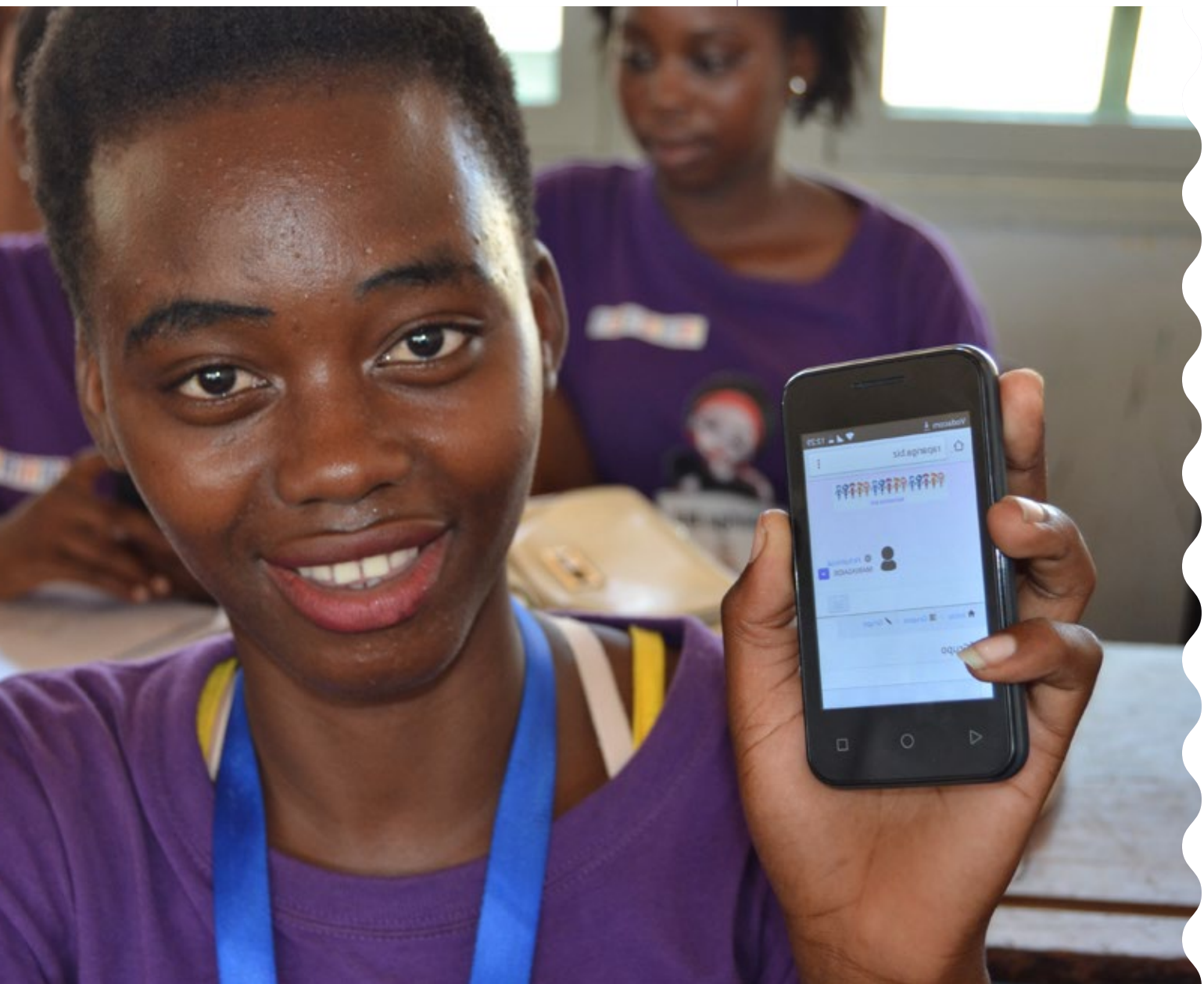


20 % des personnes BAME LGBTQIA+ étaient victimes de TFGBV, contre 9 % des personnes blanches LGBTQIA+.

L'importance de l'intersectionnalité

La VBGFT va au-delà de la misogynie et du sexisme. Elle est également ancrée dans l'homophobie, la transphobie, le racisme, la discrimination fondée sur la capacité physique et d'autres formes de discrimination. Les femmes et les personnes dont les facteurs identitaires se croisent sont attaquées et discriminées à des taux plus élevés et sous des formes distinctes qui combinent un langage sexiste, raciste et homophobe.[87] Les femmes de couleur, les femmes autochtones, les femmes issues de minorités religieuses, les femmes LGBTQIA+ et les personnes non binaires, ainsi que les femmes en situation de handicap sont ciblées de manière unique et aggravée.[88] Les jeunes femmes et les adolescentes qui sont racialisées, qui ont un handicap et qui s'identifient comme LGBTQA+ sont ciblées de manière disproportionnée par ce type d'abus.[89]

Les recherches montrent que les personnes LGBTQIA+ sont plus susceptibles d'être soumises à différentes formes de VBGFT, notamment l'ABI, le harcèlement et les discours de haine.[90] Par exemple, une étude menée auprès de 332 activistes sexuels et LGBTQ+ du monde entier a révélé que tous les répondants trans et intersexes avaient reçu des menaces et des commentaires intimidants en ligne, et que les répondants LGBTQIA+ sont soumis à des taux plus élevés de VBGFT que leurs homologues hétérosexuels.[91] En outre, les femmes et les filles noires, asiatiques ou issues de minorités et de groupes ethniques subissent davantage d'attaques que les femmes et les filles blanches. Une étude britannique portant sur 5 000 personnes LGBTQIA+ a montré que 20 pour cent des personnes LGBTQIA+ noires, asiatiques ou issues de minorités et de groupes ethniques étaient victimes de VBGFT, contre 9 pour cent des personnes LGBTQIA+ blanches.[92]



La vie numérique est la vie réelle : l'impact de la VBGFT

Bien qu'elle soit souvent perçue comme une forme moins grave et moins nocive de violence basée sur le genre, la VBGFT peut avoir des conséquences aussi graves sur la santé et la vie des femmes et des filles que la violence physique et sexuelle. La nature *publique*, *omniprésente*, *répétitive* et *permanente* de la VBGFT, ainsi que le continuum de la violence en ligne et hors ligne, provoquent une peur et une insécurité constantes qui sont aggravées par le manque de services de réponse spécialisés et accessibles et par la perception erronée qui prévaut selon laquelle la VBGFT n'est pas « réelle ».

La nature multiple et répétitive de la VBGFT signifie que la plupart des femmes subissent plusieurs types d'abus et que pour nombre d'entre elles, qui ont une présence en ligne à des fins professionnelles ou qui sont des activistes et des défenseurs des droits humains, elle fait partie de la routine de leur vie en ligne. La VBGFT sera probablement vécue comme un profil et un parcours de comportement plutôt que comme une série d'actes individuels. Cela a également pour effet que les réponses juridiques, qui traitent souvent chaque communication comme une infraction distincte, ne permettent pas de traiter l'accumulation des dommages à long terme.[93]

La VBGFT s'inscrit souvent dans un continuum dans lequel les actions qui commencent dans l'espace numérique peuvent conduire à la perpétration de violence sexiste hors ligne et vice versa.[94] Par exemple, la VBGFT est souvent commise dans le cadre de relations abusives où la technologie et les espaces numériques permettent la poursuite de la violence malgré l'absence de proximité physique avec une victime. Une étude menée auprès d'étudiants d'université aux États-Unis a montré que 92,6 pour cent des personnes ayant subi une VPI avaient également été victimes d'une agression facilitée par la technologie, ce qui démontre le continuum de la violence dans les espaces physiques et non physiques.[95] Dans d'autres cas, les partenaires intimes peuvent utiliser les technologies de l'information et de la communication pour traquer, surveiller, suivre et contrôler les femmes, en combinaison avec le harcèlement en personne.[96] Par exemple, au Royaume-Uni, une petite étude menée auprès de 307 victimes de la VPI a révélé que 45 pour cent d'entre elles avaient été maltraitées par le biais de la technologie au cours de leur relation, et que 48 pour cent avaient subi une VBGFT après la fin de leur relation.[97]

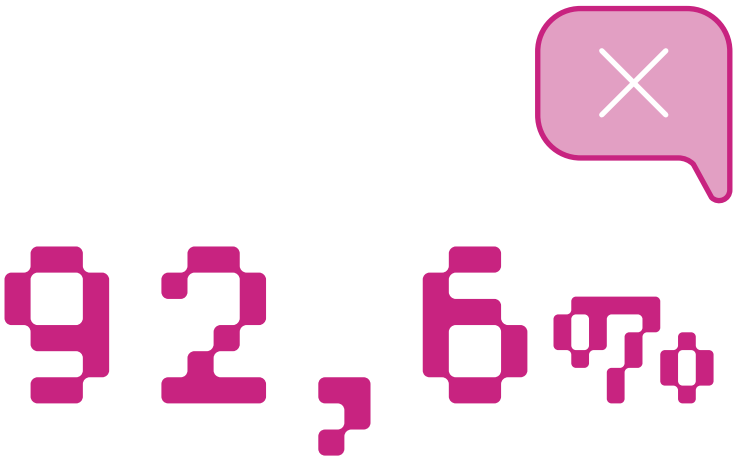
À l'inverse, le harcèlement et les menaces en ligne exacerbent, déclenchent et alimentent les agressions physiques et sexuelles hors ligne.[98] Par exemple, une enquête menée au Malawi a révélé que 53,7 pour cent des femmes ont subi des abus physiques exacerbés par la violence en ligne et que 34,3 pour cent d'entre elles ont été blessées physiquement à la suite de cette violence.[99] Dans d'autres cas, les formes sexualisées de laVBGFT, comme l'ABI, ont conduit à des violences liées à l'honneur à l'égard des femmes.[100]

Les victimes de VBGFT font généralement état d'une grave détresse émotionnelle et psychologique, d'anxiété, de dépression, de stress post-traumatique et, dans les cas extrêmes, d'idées suicidaires, d'automutilation ou de tentatives de suicide.[101] Amnesty International a mené une étude dans huit pays à revenu élevé et a découvert que 54 pour cent des femmes victimes de VBGFT avaient subi des crises de panique, de l'anxiété ou du stress.[102] De même, une étude portant sur 326 femmes du sud de l'Inde a révélé que 28 pour cent des personnes interrogées se sentaient anxieuses ou déprimées et que 6 pour cent avaient tenté de s'automutiler.[103] Selon une étude récente menée par Plan International dans 31 pays, 42 pour cent des jeunes femmes et des jeunes filles ont fait état d'un stress mental ou émotionnel et d'une baisse de l'estime de soi ou d'une perte de confiance.[104] Plus précisément, les victimes d'abus sexuel basé sur l'image peuvent connaître des troubles de la santé mentale et une détresse psychologique comparables à ceux que connaissent les survivants d'agressions sexuelles.[105]

Les femmes et les filles qui ont été soumises à des formes sexuelles de VBGFT, à savoir l'ABI, décrivent cette expérience comme ayant un impact dévastateur sur leur vie. Elles rapportent que leurs relations se détériorent, qu'elles ont un sentiment constant d'isolement, de peur, de méfiance et d'insécurité. Ces expériences sont décrites comme étant similaires en nature et en impact à celles ressenties par les victimes de violences sexuelles.[106]

La VBGFT contribue également à accroître l'isolement en ligne et hors ligne à un moment où les réseaux de soutien sont essentiels. En d'autres termes, les femmes qui ont subi ou qui ont été témoins de la VBGFT[107] réduisent leur participation en ligne et leur engagement dans la technologie, et elles restreignent ou autocensurent leurs activités sur les plateformes en ligne. Bien que cela soit particulièrement préoccupant dans la situation des femmes qui dépendent de leur présence en ligne dans le cadre de leur vie professionnelle, notamment les journalistes et les politiciennes, cette violence sert à réduire au silence toutes les femmes. Les ramifications de cette situation ne peuvent être sous-estimées.

Cette situation, associée aux conséquences psychologiques et de santé mentale de laVBGFT, a des conséquences importantes sur l'engagement politique et social des femmes, leurs possibilités d'emploi ainsi que leur accès à l'éducation et à l'information.[108] Par exemple, à l'échelle mondiale, 18 pour cent des jeunes femmes et des filles victimes de VBGFT ont ensuite rencontré des problèmes à l'école.[109] Au Malawi, 6 pour cent des victimes ont perdu toute possibilité d'éducation à cause de la VBGFT.



Those who experienced IPV, 92.6 per cent also experienced technology-facilitated aggression, demonstrating the continuum of violence across the physical and non-physical spaces.

Les femmes qui ont été victimes de VBGFT, en particulier des formes sexuelles de VBGFT, sont souvent stigmatisées et leur réputation est entachée. Comme pour d'autres formes de violence basée sur le genre (VBG), les femmes sont souvent rendues responsables de la violence qu'elles subissent et celle-ci est rejetée comme n'étant pas « réelle ». En effet, des cas ont été documentés de victimes renvoyées ou expulsées de l'école après que leurs images intimes ont été distribuées sans leur consentement.[110] Les femmes peuvent également être directement ciblées dans le seul but de nuire à leur réputation et de leur faire perdre leur emploi. L'atteinte à la réputation due à la violence liée au sexe peut entraîner une perte économique importante pour les femmes qui possèdent une entreprise, en particulier dans les zones rurales.[111] Au Malawi, 76,1 pour cent des femmes victimes de VBGFT ont subi une forme ou une autre de perte de revenus et 12 pour cent n'ont pas pu trouver un nouvel emploi.[112] À l'échelle mondiale, 7 pour cent des jeunes femmes et des filles victimes de VBGFT ont eu des difficultés à trouver ou à conserver un emploi.[113]

En outre, la VBGFT a un impact important sur la productivité des femmes. En effet, 55 pour cent des participants à une étude menée dans huit pays à revenu élevé ont déclaré que la VBGFT diminuait leur capacité à se concentrer sur les tâches quotidiennes. Cette même étude suggère que, lorsque les femmes se replient sur elles-mêmes et s'autocensurent après avoir subi la VBGFT, elles peuvent perdre des contacts et des opportunités d'emploi.[114] Cependant, les préjudices économiques de la VBGFT ne s'arrêtent pas là, car les victimes doivent souvent assumer des coûts élevés pour les frais de justice, les soins de santé, la réinstallation ou la suppression de leurs informations ou images en ligne.[115] Elles peuvent également subir des dommages économiques dus à des abus financiers ou à la perte de leur maison et de leurs biens.[116]

La VBGFT constitue également un obstacle majeur à la participation égale des femmes à la vie publique, réduisant au silence les voix des femmes et limitant leur droit démocratique à la représentation et à la participation. Les femmes sont ciblées pour les opinions, les contributions et le contenu qu'elles créent par le biais d'une présence en ligne. Les femmes politiques, les activistes et les journalistes ne sont pas les seules cibles des auteurs de VBGFT , mais 47 pour cent des jeunes femmes qui se sont exprimées politiquement ont également été victimes d'attaques en raison de leurs opinions.[117] Les attaques sexistes contre les femmes dans la vie publique ne visent pas seulement les opinions des femmes, mais elles ont tendance à être de nature sexuelle et à faire référence à l'apparence physique et à la vie personnelle des femmes.[118] Cette réduction au silence des femmes dans l'espace numérique est une attaque contre leur liberté d'expression et a des répercussions importantes sur la présence des femmes dans les forums de discussion et les espaces de prise de décision, ainsi que sur leur volonté d'assumer des rôles de direction, ce qui renforce encore les rôles et structures patriarcaux.[119]

Les impacts de la VBGFT ne sont pas seulement personnels. Il existe également d'importantes répercussions systémiques et structurelles. La faible participation des femmes à l'espace numérique ne fait pas que creuser le fossé numérique entre les sexes, mais elle renforce également l'inégalité entre les sexes et les structures de pouvoir patriarcales ainsi que les normes de genre.[120] Compte tenu de la prévalence et de l'utilisation croissantes des espaces et des technologies en ligne et numériques pour accéder aux services, à l'emploi et à l'éducation, cela constitue un obstacle à la réalisation des droits fondamentaux des femmes dans toute leur diversité. En tant que telle, la prévalence de la VBGFT prend des proportions de crise et constituera un obstacle majeur au développement durable et au mouvement vers l'égalité des sexes.[121]

Établir le profil des auteurs de VBGFT

La VBGFT peut être un outil de VPI ou de la violence dans les fréquentations et rencontres, mais elle est également perpétrée par des connaissances, des collègues de travail et des inconnus, y compris par des individus ou des organisations (c'est-à-dire pour des intérêts politiques, sur la base d'une idéologie) sous la permissivité, et parfois la complicité, des plateformes de réseaux sociaux et des entreprises technologiques.[122]

La technologie a également offert la possibilité de perpétrer des actes de violence anonymes et collectifs dans une relative impunité.

Le caractère abordable et l'accessibilité de la technologie pour les auteurs de violences font entrer la VPI dans de nouveaux espaces. Les données disponibles suggèrent que la plupart des VBGFT sont perpétrées par des partenaires intimes actuels ou anciens. Par exemple, une étude australienne menée auprès de prestataires de services liés à la VBGFT, a révélé que les anciens partenaires intimes, les partenaires intimes actuels et les connaissances sexuelles de courte durée ou occasionnelles étaient les auteurs les plus courants de la VBGFT.[123]

Les partenaires intimes ou ex-partenaires intimes

Dans le contexte de la VBGFT, la VPI est souvent utilisée pour intimider, contraindre et maintenir le contrôle sur les victimes afin de conserver une relation ou comme une punition ou une vengeance pour les avoir quittés. Elle est aussi utilisée comme une plateforme pour inciter les autres à leur nuire ou à interférer avec les procédures judiciaires, entre autres raisons.[124] Les partenaires intimes abusifs traquent, surveillent et menacent les victimes par le biais de services de géolocalisation, de réseaux sociaux et de logiciels espions facilement disponibles sur les boutiques d'applications officielles, dont certains sont même présentés aux auteurs d'abus comme des outils pour « attraper les conjoints infidèles ».[125] Les partenaires intimes violents peuvent restreindre ou empêcher l'accès des victimes à leurs téléphones portables et à leurs appareils technologiques, limitant ainsi leur capacité à communiquer avec d'autres personnes et à demander de l'aide. Les auteurs de violences ont souvent accès aux comptes et aux cercles sociaux de la victime, ce qui leur permet d'accéder facilement et illicitement à ses appareils et à ses comptes, notamment à ses comptes de messagerie et de réseaux sociaux, ainsi qu'à ses informations bancaires. L'accès à ces données privées peut permettre aux auteurs d'installer des logiciels espions, de suivre et de surveiller la localisation des victimes et leur utilisation de la technologie, de voler ou de supprimer les informations des victimes et d'usurper leur identité. Ils peuvent également menacer et faire chanter la victime pour qu'elle révèle des photos intimes ou des informations privées, et harceler la victime et son entourage par différents moyens numériques.[126]

Les partenaires intimes sont souvent en mesure de poursuivre les abus même après la fin de la relation.[127] En fait, une petite étude menée au Royaume-Uni auprès de 307 femmes ayant subi des violences entre partenaires a révélé que 45 pour cent d'entre elles avaient également été victimes de VBGFT pendant leur relation et que 48 pour cent avaient subi des VBGFT après la fin de leur relation.[128]

Les acteurs étatiques

L'État peut également être l'auteur de la VBGFT. Les acteurs étatiques ont la possibilité d'accéder à de grandes quantités d'informations détaillées sur les victimes, y compris les données de santé en ligne par exemple, qui contiennent des informations très sensibles et confidentielles parce que les données sont systématiquement collectées dans les dossiers de santé et les systèmes de gestion de l'information. Les acteurs étatiques ont aussi généralement une grande capacité à surveiller, traquer, suivre et obtenir des données sur les individus pour perpétrer des violences, dont les conséquences peuvent avoir des implications sexistes. Les acteurs étatiques peuvent utiliser la technologie et les données pour perpétrer des violences à l'égard d'activistes, de défenseurs des droits des femmes, de journalistes, de personnes non conformes du point de vue du genre, de minorités sexuelles ou de femmes leaders politiques qui sont leurs rivales.[129] En outre, les gouvernements ont la capacité de bloquer l'accès aux informations et aux services de santé sexuelle et reproductive, tels que les services d'avortement et de contraception d'urgence en ligne.

Bien que les systèmes de gestion de l'information sur la VBG ([130]) appliquent les normes les plus élevées possibles en matière de collecte et de stockage de données robustes et éthiques afin de garantir la confidentialité des informations relatives aux victimes, la cybersécurité et l'utilisation abusive de la technologie et des informations par les acteurs étatiques et autres, y compris les parties non étatiques à un conflit, restent un risque. De nombreux pays ont « des capacités insuffisantes pour mettre en œuvre efficacement des systèmes d'information sécurisés, des cadres juridiques faibles ou inexistants pour la protection des données et il n'y a pas une unité spécialisée dans les ministères de la santé, avec un personnel suffisamment qualifié, pour superviser l'éthique des données ».[131]

Les étrangers et les trolls

La société devenant de plus en plus numérique, de nouvelles formes de socialisation et d'engagement avec de nouvelles personnes et des inconnus sont apparues. Les formes traditionnelles de harcèlement dans les espaces publics physiques se sont déplacées vers la sphère en ligne, permettant aux auteurs d'identifier et de cibler facilement les femmes et les filles sur les plateformes de réseaux sociaux, les sites web et les applications tout en restant anonymes.[132]

Les trolls sont généralement des inconnus qui publient délibérément des commentaires ou des messages, téléchargent des images ou des vidéos et créent des hashtags dans le but d'agacer, de provoquer ou d'inciter à la violence à l'égard des femmes et des filles pour leur propre plaisir.[133] Les étrangers et les trolls sont des auteurs de VBGFT depuis le début d'Internet : des commentaires misogynes et sexistes, des menaces de viol et des informations diffamatoires ont été signalés depuis le début des années 2000 (i.e. AutoAdmit), avec des cas récents de radicalisation accrue et de campagnes de harcèlement organisées contre les femmes (i.e. GamerGate).

Une étude menée par Plan International dans 31 pays de toutes les régions a révélé que les inconnus sont les auteurs les plus courants de la violence sexuelle et sexiste contre les jeunes femmes et les filles (36 pour cent), suivis par les utilisateurs anonymes des réseaux sociaux (32 pour cent) et les connaissances sur les réseaux sociaux (29 pour cent). Il convient de noter que 16 pour cent des abus en ligne contre les jeunes femmes et les filles sont perpétrés par des groupes d'inconnus.[134]

Le harcèlement de la part d'inconnus est signalé comme étant plus effrayant et difficile à arrêter, et il tend à provenir d'hommes, qui sont particulièrement enragés lorsque les femmes et les filles expriment leurs opinions et ne se conforment pas aux normes et idées traditionnelles de la féminité.[135] Parmi les femmes âgées, 59 pour cent de celles qui ont été victimes d'abus ou de harcèlement sur Twitter ont déclaré avoir été attaquées par des inconnus.[136]

Redevabilité

La redevabilité ou obligation de rendre des comptes aux victimess de VBGFT est peut-être l'un des domaines les plus difficiles à aborder. Non seulement les technologies et les espaces numériques sont en constante évolution, mais les auteurs peuvent être anonymes et il peut être difficile pour les autorités judiciaires de prévoir des lois.

La responsabilité de l'État

Les États ont la responsabilité d'élaborer des cadres législatifs, politiques et réglementaires pour lutter contre la VBGFT afin de garantir la responsabilité des auteurs mais aussi la sécurité des plateformes en ligne, des espaces numériques et de l'utilisation des technologies. Cependant, les cadres juridiques et les politiques actuels prennent rarement en compte la VBGFT dans les lois et politiques existantes qui traitent de la VBG. Bien que certains pays puissent avoir des lois et des politiques pour la sauvegarde et la sécurité en ligne, celles-ci sont souvent génériques et ne tiennent pas compte du genre. Elles ne prennent pas non plus les mesures appropriées pour mettre fin au préjudice numérique.[137] Ces cadres sont souvent insuffisants et ne tiennent pas compte des technologies émergentes, des plateformes en ligne et des autres moyens par lesquels de nouvelles formes de VBG sont perpétrées et amplifiées. Selon l'Economist Intelligence Unit, « dans 64 des 86 pays, les organismes chargés de l'application des lois et les tribunaux semblent ne pas prendre les mesures correctives appropriées pour lutter contre la violence en ligne à l'égard des femmes. »[138] Ces preuves mettent en évidence une importante lacune structurelle qui laisse les mécanismes de responsabilité au bon vouloir des entreprises technologiques privées.

Certaines formes de VBGFT sont interdites par la loi et souvent criminalisées, en particulier celles qui répondent aux définitions d'infractions pénales ou de causes d'action civile préexistantes. Par exemple, certaines formes d'abus sexuels basés sur l'image, d'actes d'usurpation d'identité, de diffamation, de menaces de violence, de harcèlement et d'autres atteintes à la vie privée, sont des infractions civiles et/ou pénales dans certains pays.[139] Cependant, d'autres formes de VBGFT, telles que le harcèlement en ligne non criminel, le *trolling*, le *mobbing* en ligne ou la création et la diffusion de *deepfakes* non sexualisés, peuvent être considérées comme de « simples discours ou expressions ».[140]

En outre, lorsque des politiques et des lois existent, elles ne sont pas uniformément mises en œuvre. Les raisons de cette mise en œuvre limitée sont, entre autres, la perception, parmi les responsables de l'application de la loi, que la VBGFT n'est pas une infraction grave, ainsi que les préjugés sexistes internes et les idées fausses, le sexisme et la dynamique de pouvoir au sein des systèmes patriarcaux d'application de la loi et de justice qui renforcent le blâme des victimes. En outre, les interprétations de la VBGFT peuvent ne pas correspondre aux éléments des définitions des infractions pénales de la violence à l'égard des femmes ou de la violence basée sur le genre dans la loi. En outre, la capacité des organismes chargés de l'application de la loi et des systèmes judiciaires à inculper et à condamner les délinquants de manière adéquate lorsque l'identité du ou des délinquants ne peut être retrouvée signifie que les comportements en ligne sont commis en toute impunité. Enfin, lorsque l'infraction est commise dans une juridiction différente de celle de la victime, les moyens d'accéder à la responsabilité deviennent encore plus improbables.

L'Allemagne a mis en place la « loi visant à améliorer l'application de la loi dans les réseaux sociaux », ou Netzwerkdurchsetzungsgesetz (NetzDG). Cette loi oblige les plateformes de réseaux sociaux comme Twitter, Reddit et Facebook à supprimer les discours de haine et autres contenus offensants dans les 24 heures. Le fait de ne pas retirer un contenu interdit peut entraîner des amendes pouvant atteindre 50 millions d'euros. Les plateformes de réseaux sociaux s'y conforment donc - par exemple, en mettant en place des centres de suppression pour surveiller le contenu et en appliquant dans une plus large mesure leurs propres normes communautaires. En 2020, la loi a été modifiée pour exiger une plus grande redevabilité des entreprises de réseaux sociaux, qui sont désormais obligées de signaler les contenus préjudiciables à l'Office fédéral allemand de police criminelle pour permettre des poursuites pénales.[141] Cela dit, le succès du NetzDG dans la réduction des discours de haine et des contenus préjudiciables et violents est difficile à suivre et à évaluer.[142]

Dans l'Union européenne, la proposition de *loi sur les services numériques* (2020) reconnaît explicitement les préjudices systémiques que les plateformes numériques peuvent causer et impose aux grandes plateformes en ligne des obligations d'évaluer régulièrement les risques qui découlent de l'utilisation de leurs services et d'y répondre.[143]

En Australie, la réglementation de la sécurité en ligne a été, et continue d'être, une priorité permanente pour les régulateurs. En effet, *la loi sur la sécurité en ligne de 2021 (Cth)* (la « loi ») qui a été récemment adoptée en juillet 2021 exigeait que les fournisseurs de services en ligne, les fournisseurs de services de réseaux sociaux et les autres fournisseurs de services Internet désignés disposent des six prochains mois pour s'assurer que leurs politiques et procédures sont à jour et conformes aux lois australiennes. Les entreprises visées par la loi doivent protéger de manière proactive les utilisateurs finaux australiens et avoir la capacité de répondre aux avis de la Commission à court terme pour supprimer les contenus préjudiciables. En effet, l'obligation de maintenir des espaces sûrs est clairement imposée aux entreprises. La loi continue également de soutenir l'organisme statutaire indépendant, la Commission eSafety (la « Commission »), dont les principales fonctions consistent à faire appliquer la loi et à administrer un système de plaintes portant sur :

- des documents de cyberintimidation visant un enfant australien ;
- le partage non consensuel d'images intimes ;
- des documents de cyberabus ciblant un adulte australien ; et
- un système de contenu en ligne.

Il est essentiel que la charge du retrait du document nuisible soit transférée de la victime à l'organisme de réglementation pour gérer le retrait immédiat du document offensant directement avec l'entreprise fautive. En outre, la Commission travaille en étroite collaboration avec les entreprises privées pour intégrer des dispositifs de sécurité dans la conception des plateformes, créant ainsi des partenariats pour lutter contre la VBGFT.[144]

Les entreprises technologiques privées

Les entreprises technologiques privées englobent un large éventail d'organisations, dont les suivantes, sans être exhaustif :[145]

- les fournisseurs d'accès à l'internet désignés, c'est-à-dire les entités qui permettent aux utilisateurs finaux d'accéder à des documents en ligne, et les fournisseurs d'accès à l'internet, c'est-à-dire les entités qui fournissent des services de transport sur l'internet, y compris, entre autres, Google, Safari et Internet Explorer ;
- les fournisseurs de services de réseaux sociaux - entités qui fournissent des services mettant en relation deux utilisateurs finaux par des moyens en ligne, dont Facebook, LinkedIn et Instagram, entre autres ;
- les fournisseurs de services électroniques - entités qui permettent aux utilisateurs finaux de communiquer entre eux (par exemple, Outlook et les services de chat de jeux) ;
- les fournisseurs de services de distribution d'applications - entités qui donnent accès à des services d'applications, notamment Google (par le biais du Google PlayStore) et Apple (par le biais de l'IOS App Store) ;
- les fournisseurs de services d'hébergement - entités qui permettent l'hébergement et le stockage de documents fournis sur des services de réseaux sociaux, des services électroniques pertinents ou des services Internet désignés, y compris Apple et Microsoft, chacun par le biais de leur fourniture de services en nuage, entre autres ;
- les sociétés de développement de matériel informatique - entités qui créent, développent et/ou entretiennent des équipements technologiques, des actifs physiques et d'autres articles tangibles ;
- les sociétés de développement de logiciels - entités qui créent, conçoivent, développent et entretiennent des programmes, des applications, des cadres ou d'autres composants de logiciels.

Ces entreprises sont des intermédiaires dans les actes de VBGFT et leurs actions (ou inaction) sont essentielles pour arrêter ou amplifier les actes violents. Si de nombreuses plateformes et technologies en ligne ont été conçues pour une « application général », certaines « plateformes spécialisées » ont été délibérément conçues pour commettre et propager des actes de VBGFT, tels que l'abus sexuel basé sur l'image et la divulgation non consensuelle d'images intimes, et donc pour tirer profit de comportements abusifs.[146] Cependant, même les plateformes d'application générale contribuent à amplifier les actes de VBGFT grâce à des caractéristiques et des modèles commerciaux distincts qui privilégient la croissance et le profit au détriment des droits humains, maximisent l'engagement des utilisateurs et favorisent le contenu sensationnel, et permettent l'automatisation des abus ainsi que l'anonymat des auteurs.[147] Souvent, ces plateformes ne réagissent pas aux cas de VBGFT et, par exemple, suspendent les comptes des victimes au lieu de supprimer le document offensant et de tenir les agresseurs responsables, ou autorisent les pages qui promeuvent des contenus misogynes tout en censurant les utilisateurs qui voient le sexe de façon positive et la LGBTQIA+ favorablement. En outre, les entreprises technologiques sont souvent réticentes à traiter les questions d'égalité et reproduisent la misogynie, le racisme et la discrimination dans leurs algorithmes. Par exemple, il a été démontré que les systèmes d'IA (intelligence artificielle) commerciaux présentent d'importants biais liés au sexe et au type de peau,[148], ce qui est probablement dû à un manque de diversité au sein du secteur technologique. Les produits et services basés sur les algorithmes et l'IA perpétuent les préjugés implicites existant dans la société et peuvent entraîner une discrimination supplémentaire, car ils s'appuient sur les données et informations disponibles et peuvent eux-mêmes être fondés sur des hypothèses biaisées.[149]

En l'absence d'une réglementation claire, les entreprises technologiques privées ne sont guère obligées de lutter contre la VGBFT en supprimant les contenus préjudiciables ou en intégrant des dispositifs de sécurité dans la plateforme ou la technologie.

Les obligations de promouvoir et de protéger la sécurité des utilisateurs finaux sont essentielles si l'on veut lutter efficacement contre la VBGFT. Alors que de nombreuses entreprises, en particulier les plateformes de réseaux sociaux, ont introduit la modération de contenu pour identifier et éliminer les contenus abusifs, la conception et l'application de ces mesures n'ont pas toujours été couronnées de succès et ont imposé une charge supplémentaire aux victimes et aux utilisateurs individuels pour mettre fin aux abus. En outre, ces mécanismes s'appuient sur des politiques et des pratiques de « liberté d'expression » qui incluent de nombreuses exceptions à ce qui constitue un abus et un discours de haine, exceptions qui sont manipulées par les auteurs des abus pour faire taire les victimes. La modération du contenu est également très sélective et incohérente, et les décisions sont souvent biaisées, déterminées par l'opinion publique, l'influence politique et les conflits d'intérêts, ce qui entraîne la suppression de contenus inoffensifs alors que les contenus abusifs restent incontestés.[150]

Bien que la modération du contenu soit une première étape pour mettre fin à la VBGFT, les entreprises de technologie et de plateformes doivent faire davantage pour garantir la sécurité dans l'utilisation de la technologie et des plateformes en ligne. Les entreprises technologiques doivent collaborer avec les gouvernements et la société civile pour mettre en place des mécanismes qui répondent efficacement et préviennent la VBGFT d'une manière sensible au genre et à la culture, tout en étant transparents et proactifs dans la lutte contre cette violence depuis la conception de leurs produits jusqu'au signalement des cas et à la gestion de leurs données.

1 Département des affaires économiques et sociales des Nations Unies (2020). *Façonner les tendances de notre temps*. Rapport du réseau des économistes de l'ONU pour le 75e anniversaire de l'ONU. Disponible sur : https://www.un-ilibrary.org/content/books/9789210053556

2 Ibid.

3 Flynn, A., Powell, A., et Hindes, S. (2021). La violence facilitée par la technologie : une enquête auprès des intervenants des services de soutien (Rapport de recherche, 02/2021). ANROWS. Disponible sur : https://20ian81kynqg38bl3l3eh-8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_Survey.pdf

UNFPA, ONU Femmes, Quilt.AI (2021). COVID-19 et la violence contre les femmes : les preuves derrière le discours. Disponible sur : https://asiapacific.unfpa.org/en/publications/covid-19-and-violence-against-women-evidence-behind-talk?_ga=2.130256973.39170622.1628523607-1469909938.1607087406

ONU Femmes, UNFPA (2021). Impact du COVID-19 sur l'égalité des sexes et l'autonomisation des femmes en Afrique orientale et australe. Disponible sur : https://data.unwomen.org/publications/covid-19-gender-equality-east-and-southern-africa

4 Khoo, C. (2021). Deplatforming misogyny : report on platform liability for technology-facilitated gender-based violence. FAEJ. Disponible sur : https://www.leaf.ca/publication/deplatforming-misogyny/

5 Amnesty International (2018). Toxic Twitter. Disponible sur : https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-1/

6 Plan International (2020). Libre d'être en ligne ? Les expériences des filles et des jeunes femmes en matière de harcèlement en ligne. Disponible sur : https://plan-international.org/publications/freetobeonline

7 Ibid.

Khoo, Deplatforming Misogyny.

8 Khoo, Deplatforming Misogyny.

9 E.L. Backe, P. Lilleston et J. McCleary-Sills, "Networked individuals, gendered violence: a literature review of cyber violence", *Violence Gender*, vol. 5, n° 3, (2018), p. 135-145.

C. McGlynn, E. Rackley et R. Houghton, " Beyond 'revenge porn': the continuum of image-based sexual abuse ", *Feminist Legal Studies*, vol. 15, (2017), pp. 1-22.

10 Conseil des droits de l'homme des Nations Unies, 20e session, point 3 de l'ordre du jour, U.N. Doc A/HRC/20/L.13 (29 juin 2012).

Nations Unies (1948). Déclaration universelle des droits de l'homme. Disponible sur : https://www.un.org/en/about-us/universal-declaration-of-human-rights [consulté le 11 novembre 2021].

Assemblée générale des Nations Unies (1966). Pacte international relatif aux droits civils et politiques, 16 décembre 1966, Nations Unies, Recueil des Traités, vol. 999, p. 171, disponible sur : https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx [consulté le 11 novembre 2021].

11 HCDH (2018). Rapport de la Rapporteuse spéciale sur la violence à l'égard des femmes, ses causes et ses conséquences sur la violence en ligne contre les femmes et les filles dans une perspective de droits humains. Disponible sur https://www.ohchr.org/EN/Issues/ Women/SRWomen/Pages/SRWomenIndex.aspx

12 La terminologie et les définitions qui se réfèrent à la VBGFT sont multiples et diverses. Voir la partie 4.

13 Voir le glossaire de la partie 4 pour les définitions des termes liés à la technologie.

14 Flavia Fascendini et Kateřina Fialová (2011). Les voix des espaces numériques : La violence contre les femmes liée à la technologie. Publié par l'Association pour le progrès des communications. Disponible sur : https://www.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf

15 L., Sardinha et H.E. Nájera Catalán, " Attitudes towards domestic violence in 49 low- and middle-income countries: A gendered analysis of prevalence and country-level correlates ", *PloS One*, vol. 13, n° 10, (2018), e0206101. https://doi.org/10.1371/journal.pone.0206101

16 J. Bailey, N. Henry et A. Flynn, "Technology-Facilitated Violence and Abuse : International Perspectives and Experiences", dans *The Emerald International Handbook of Technology Facilitated Violence and Abuse,* J. Bailey, A. Flynn et N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021) pp. 1-17. https://doi.org/10.1108/978-1-83982-848-520211001

17 Suzie Dunn et Kristen Thomasen, "Reasonable expectations of privacy in an era of drones and deepfakes- expanding the Supreme Court of Canada's decision in R v Jarvis", in *The Emerald International Handbook of Technology Facilitated Violence and Abuse,* J. Bailey, A. Flynn et N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021).

18 Webinaire : La liberté financière - créer la sécurité économique et échapper aux abus financiers. Sommet national sur la sécurité des femmes, septembre 2021. Disponible sur : https://regonsite.eventsair.com/national-summit-on-womens-safety/

19 Voir la partie 3 « Glossaire des termes » pour une liste plus complète des formes de VBGFT et leurs définitions.

20 Réseau d'apprentissage VAW (2013). La violence à l'égard des femmes liée à la technologie. Disponible sur : http://www.vawlearningnetwork.ca/our-work/issue-based_newsletters/issue-4/index.html

21 Flynn, Powell, et Hindes, Technology-facilitated abuse.

22 N. Henry et A. Powell, " La violence sexuelle facilitée par la technologie : une analyse documentaire de la recherche empirique ". *Trauma, Violence & Abuse*, vol. 19, n° 2, (2018), p. 195-208. https://doi.org/10.1177/1524838016650189

23 Ibid.

24 Flynn, Powell, et Hindes, Technology-facilitated abuse. Les populations LGBTQI+ sont particulièrement sensibles au harcèlement en ligne et à ses méfaits, notamment lorsqu'il s'agit de menaces et/ou d'actes de divulgation publique de leur identité de genre ou de leur orientation sexuelle qui peuvent se produire avec ou sans extorsion et sextorsion : S. Dunn (2020). *Technology-Facilitated Gender-Based Violence* : *An Overview* (Waterloo, ON : Centre pour l'innovation dans la gouvernance internationale). Disponible sur : https://apo.org.au/node/309987

25 VAW Learning Network, Technology-related violence against women.

26 Henry et Powell, Technology-facilitated sexual violence.

27 C. Parsons, A. Molnar, J. Dalek, J. Knockel, M. Kenyon, B. Haselton, C. Khoo et R. Deibert (2019). The Predator in Your Pocket : Une évaluation multidisciplinaire de l'industrie des applications de stalkerware. The Citizen Lab. Disponible sur : https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/

28 Flynn, Powell, et Hindes, Technology-facilitated abuse.

29 McGlynn, C., et Rackley, E., " Image-Based Sexual Abuse ", *Oxford Journal of Legal Studies*, vol. 37, n° 3, (2017), p. 534-561. https://doi.org/10.1093/ojls/gqw033.

30 Flynn, Powell, et Hindes, Technology-facilitated abuse.

31 En 2019, lors d'un festival populaire en Espagne, un auteur a installé des caméras cachées sur un espace public dans le but d'enregistrer des images de femmes en train d'uriner - les hommes ont été retirés des enregistrements. Ces images, qui montraient le visage et les organes sexuels des victimes, ont ensuite été téléchargées sur des sites web pornographiques. Plus de 80 victimes ont été identifiées, dont des mineures. Cette affaire a été rejetée par le tribunal, ce qui montre la capacité limitée des systèmes judiciaires à répondre aux cas de VBGFT. Cependant, des femmes activistes et des victimes ont rejoint un mouvement pour réclamer leurs droits et ont contribué à identifier des cas similaires

dans d'autres parties du pays.
De El Pais (2021). Revuelta en Galicia contra las cámaras ocultas que denigran a las mujeres. Disponible sur : https://elpais.com/sociedad/2021-04-04/revuelta-en-galicia-contra-las-camaras-ocultas-que-denigran-a-las-mujeres.html

32 Henry et Powell, Technology-facilitated sexual violence.
N. Henry, A. Flynn et A. Powell, "Technology-facilitated domestic and sexual violence : a review", *Violence Against Women*, vol. 26, n° 15-16, (2020), pp. 1828-1854. https://doi.org/10.1177/1077801219875821

33 Ibid.

34 Henry et Powell, Technology-facilitated sexual violence. Henry, Flynn et Powell, Technology-facilitated domestic and sexual violence.

35 Henry, Flynn et Powell, Technology-facilitated domestic and sexual violence.

36 S. Craven, S. Brown et E. Gilchrist, "Sexual grooming of children: review of literature and theoretical considerations", *Journal of Sexual Aggression*, vol. 12, (2006), pp. 287-299, 10.1080/13552600601069414.

37 M.A. Franks, "Sexual harassment 2.0", *Maryland Law Review*, vol. 71, p. 2012655.

38 J.M. MacAllister, The doxing dilemma: seeking a remedy for the malicious publication of personal information. *Fordham Law Review*, vol. 85, (2017), p. 2451-2383.

39 S. Eckert et J. Metzger-Riftkin (2020). Doxxing. The International Encyclopedia of Gender, Media, and Communication. https://doi.org/10.1002/9781119429128.iegmc009

40 D. Douglas, " Doxing : une analyse conceptuelle ", *Ethics Information Technology*, vol. 18, (2016), p. 199-210.

41 MacAllister, Le dilemme du doxing.

42 VAW Learning Network, Technology-related violence against women.

43 N. Henry et A. Powell, " Sexual violence in the digital age: the scope and limits of criminal law ", *Social & Legal Studies*, vol. 25, n° 4, (2016), pp. 397-418. doi:10.1177/0964663915624273

44 Flynn, Powell, et Hindes, Technology-facilitated abuse.

45 Fascendini et Fialová, Voices from digital spaces (voir note de bas de page 14).

46 VAW Learning Network, Technology-related violence against women.

47 Fascendini et Fialová, Voices from digital spaces (voir note de bas de page 14).

48 APC (2020). Comment la technologie est utilisée pour perpétrer la violence contre les femmes - et pour la combattre. Disponible sur : https://www.apc.org/en/pubs/research/how-technology-being-used-perpetrate-violence-agai

49 Nicki Dell, Karen Levy, Damon McCoy et Thomas Ristenpart (2018). Comment les agresseurs domestiques utilisent les smartphones pour espionner leurs partenaires. Disponible sur : https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google
Parsons, Molnar, Dalek, Knockel, Kenyon, Haselton, Khoo et Deibert, Le prédateur dans votre poche.

50 Save the Children (2021). Inde : les filles en Inde font face à un plus grand risque en ligne de mariage et de trafic d'enfants pendant la pandémie. Disponible sur : https://www.savethechildren.net/news/india-girls-india-facing-greater-online-risk-child-marriage-and-trafficking-during-pandemic

51 Gulfer Ulas (2019). Radicalisation féminine : Pourquoi les femmes rejoignent-elles ISIS ? Centre du Moyen-Orient de la LSE. Disponible sur : https://blogs.lse.ac.uk/mec/2019/08/15/female-radicalisation-why-do-women-join-isis/
Lisa Blaker, "The Islamic State's use of online social media ", *Military Cyber Affairs*, vol. 1, n° 1, (2015), p. 4. Disponible sur : https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1004&context=mca

52 A. Van der Wilk (2018). La cyber-violence et les discours de haine en ligne contre les femmes. Étude pour la commission FEEM. Disponible sur : https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_FR.pdf.

53 A. Gurumurthy, A. Vasudevan et N. Chami (2019). Born digital, Born free ? Une étude socio-juridique sur les expériences des jeunes femmes en matière de violence en ligne en Inde du Sud. Bangalore, Inde : IT for Change. Disponible sur : https://itforchange.net/sites/default/ files/1662/Born-Digital_Born-Free_SynthesisReport.pdf

54 D. Freed, J. Palmer, D.E. Minchala, K. Levy, T. Ristenpart et N Dell, "Digital technologies and intimate partner violence : a qualitative analysis with multiple stakeholders", *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, (2017), pp. 1-22, https://doi.org/10.1145/3134681.

55 D.K. Citron, *Hate Crimes in Cyberspace* (Cambridge, MA: Harvard University Press, 2014).
J. West, *Cyber-Violence Against Women* (Vancouver, BC: Battered Women's Support Services, 2014). www.bwss.org/wp-content/uploads/2014/05/ CyberVAWReport-JessicaWest.pdf

56 Safety Net Canada, *Évaluer la technologie dans le contexte de la violence faite aux femmes et aux enfants : Examiner les avantages et les risques* (Vancouver, BC : Safety Net Canada, 2013). https://bcsth.ca/wp-content/uploads/2016/10/Assessing-Technology-in-the-Context-of-Violence-AgainstWomen-Children.-Examining-Benefits-Risks.pdf.

57 Dunn, Technology-facilitated gender-based violence : an overview ; Bien que la technologie et les outils numériques aient été utilisés dans des contextes humanitaires pour soutenir des programmes et améliorer la réponse, ils ont également le potentiel d'exacerber les conflits et d'augmenter le risque de dommages intentionnels et non intentionnels pour les populations touchées. Les acteurs étatiques et non étatiques peuvent faire un mauvais usage de la technologie pour perpétrer des violences et causer des dommages supplémentaires à la population, et les pratiques des acteurs humanitaires - en particulier en ce qui concerne la protection des données - peuvent exposer les populations vulnérables à un risque accru. Pour en savoir plus : https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/

58 ONU (2019). Stratégie et plan d'action des Nations unies sur le discours de haine. Disponible sur : https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml

59 Dunn, Technology-facilitated gender-based violence: an overview.

60 Douglas, Doxing: a conceptual analysis.
Dunn, Technology-facilitated gender-based violence: an overview.

61 Dunn, Technology-facilitated gender-based violence: an overview.

62 K. Levy et B. Schneier, "Privacy threats in intimate relationships", *Journal of Cybersecurity* (Oxford), vol. 6, n° 1, (2020), https://doi.org/10.1093/cybsec/tyaa006.
D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart et N. Dell, "'A stalker's paradise': how intimate partner abusers exploit technology", présentation à la CHI Conference on Human Factors in Computing Systems 2018.

63 L. Hinson, L. O'Brien-Milne, J. Mueller, V. Bansal, N. Wandera et S. Bankar (2019). *Définir et mesurer la violence sexiste facilitée par la technologie* (Washington DC : Centre international de recherche sur les femmes). Disponible sur : http://www.svri.org/sites/default/files/attachments/2019-03-25/ICRW_TFGBVMarketing_Brief_v3_WebReady_0.pdf

64 Les pays inclus sont l'Afrique du Sud, l'Algérie, l'Allemagne, l'Arabie saoudite, l'Argentine, l'Australie, le Bangladesh, la Belgique, le Brésil, le Canada, le Chili, la Chine, la Colombie, l'Égypte, la France, le Ghana, le Guatemala, l'Inde, l'Indonésie, l'Italie, le Japon, le Kazakhstan, la Malaisie, le Maroc, le Mexique, le Myanmar, le Nigeria, le Pakistan, le Pérou, les Philippines, la Pologne, les Pays-Bas, la Roumanie, le Royaume-Uni,

la Russie, la Corée du Sud, l'Espagne, Taiwan, la Tanzanie, la Thaïlande, la Turquie, l'Ukraine, le Venezuela et le Vietnam.

65 Economist Intelligence Unit (2021). Measuring the prevalence of online violence against women. Disponible sur : https://onlineviolencewomen.eiu.com/

66 Plan International, Free to be online? (voir note de bas de page 6).

67 Ibid.

68 OMS (2021). Estimations mondiales, régionales et nationales de la violence des partenaires intimes à l'égard des femmes et estimations mondiales et régionales de la violence sexuelle sans partenaire à l'égard des femmes. Disponible sur : https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence

69 M. Duggan (2017). Le harcèlement en ligne 2017. Centre de recherche Pew. Disponible sur : https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

70 Dunn, Technology-facilitated gender-based violence: an overview.

71 Plan International, Free to be online? (voir note de bas de page 6).

72 Ibid.

73 Société pour l'enfance, Young Minds (2018). Filet de sécurité : l'impact de la cyberintimidation sur la santé mentale des jeunes : Résumé du rapport d'enquête. Disponible sur : https://www.youngminds.org.uk/media/gmvdnzcv/executive-summary-pcr144a_social_media_cyberbullying_inquiry_summary_report.pdf

74 Pew Research Centre (2018).Teens, Social Media and Technology 2018. Disponible sur : https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

75 International Web Foundation (2020). IWF 2020 Annual Report | Face the facts. Disponible sur : https://www.iwf.org.uk/report/iwf-2020-annual-report-face-facts

76 Janine M. Zweig, Meredith Dank, Pamela Lachman et Jennifer Yahner, *Technology, Teen Dating Violence and Abuse, and Bullying* (Washington DC: Urban Institute, 2013). Disponible à l'adresse : https://www.urban.org/sites/default/files/publication/23941/412891-Technology-Teen-Dating-Violence-and-Abuse-and-Bullying.PDF

77 Plan International, Free to be online? (voir note de bas de page 6).

78 The World Wide Web Foundation (2020). The online crisis facing women and girls threatens global progress on gender equality. Disponible sur : https://webfoundation.org/2020/03/the-online-crisis-facing-women-and-girls-threatens-global-progress-on-gender-equality/

79 Plan International, Free to be online? (voir note de bas de page 6).

80 *Wall Street Journal* (2021). Les dossiers Facebook : Facebook sait qu'Instagram est toxique pour les adolescentes, selon des documents de l'entreprise. Par Georgia Wells, Jeff Horwitz et Deepa Seetharaman. Disponible sur : https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline

81 Amnesty International, Toxic Twitter (voir note de bas de page 5).

82 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

83 J. Posetti, N. Shabbir, D. Maynard, K. Bontcheva et N. Aboulez (2021). Le froid : tendances mondiales de la violence en ligne contre les femmes journalistes. UNESCO. Disponible sur : https://en.unesco.org/news/unesco-releases-pioneering-discussion-paper-online-violence-against-women-journalists

84 Union interparlementaire (2016). Sexisme, harcèlement et violence à l'égard des femmes parlementaires.

85 R. Lewis, M. Rowe et C. Wiper, " Online abuse of feminists as an emerging form of violence against women and girls ", *British Journal of Criminology*, vol. 57, n° 6, (2017), p. 1462-1481. https://doi.org/10.1093/bjc/azw073.

86 Plan International, Free to be online? (voir note de bas de page 6).

87 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

88 Amnesty International, Toxic Twitter (voir note de bas de page 5).

89 Plan International, Free to be online? (voir note de bas de page 6).

90 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

91 Delfina Schenone Sienra et Mariana Palumbo (2017). Enquête mondiale EROTICS 2017 : Sexualité, droits et réglementation de l'internet. Association pour le progrès des communications. Disponible sur : https://www.apc.org/sites/default/files/Erotics_2_FIND-2.pdf

92 Stonewall (2017). LGBT en Grande-Bretagne - crimes de haine et discrimination. Disponible sur : https://www.stonewall.org.uk/lgbt-britain-hate-crime-and-discrimination

93 Lewis, Rowe et Wiper, Online abuse of feminists as an emerging form of violence against women.

94 HCDH (2018). Rapport de la rapporteuse spéciale sur la violence à l'égard des femmes (voir note de bas de page 11).

95 A. Marganski et L. Melander, " Intimate partner violence victimization in the cyber and real world : examining the extent of cyber aggression experiences and its association with in-person dating violence ", *Journal of Interpersonal Violence*, vol. 33, n° 7, (2018), p. 1071-1095. https://doi.org/10.1177/0886260515614283.

96 Flynn, Powell, et Hindes, Technology-facilitated abuse.

97 Laxton, C. (2014). Monde virtuel, peur réelle. Rapport de Women's Aid sur les abus, le harcèlement et la traque en ligne. Disponible sur : https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf

98 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

99 D.F. Malanga (2020). Lutte contre la cyber-violence sexiste à l'encontre des femmes et des filles au Malawi dans le contexte de la pandémie de COVID-19. Disponible sur : https://africaninternetrights.org/sites/default/files/Donald_Flywell-1.pdf

100 GBV AoR Helpdesk (2021). Série d'apprentissage sur la violence basée sur le genre facilitée par la technologie. Dossier d'apprentissage 1 : Comprendre la violence liée au sexe facilitée par la technologie.

101 Ibid.

102 Amnesty International, Toxic Twitter (voir note de bas de page 5).

103 Gurumurthy, Vasudevan et Chami, Born digital, born free? (voir note de bas de page 53).

104 Plan International, Free to be online? (voir note de bas de page 6).

105 Dunn, Technology-facilitated gender-based violence : an overview (voir note de bas de page 24).
S. Bates, " Revenge porn and mental health: a qualitative analysis of the mental health effects of revenge porn on female survivors ", *Feminist Criminology*, vol. 12, n° 1, (2017), p. 22-42. https://doi.org/10.1177/1557085116654565.

106 C. McGlynn, E. Rackley, N. Henry, N. Gavey, A. Flynn et A. Powell, "It's torture for the soul' : the harms of image-based sexual abuse", *Social and Legal Studies*, vol. 30, No. 4, (2021), pp. 541-562.

107 Malanga, Lutter contre la cyber-violence basée sur le genre.

108 GBV AoR Helpdesk (2021). Série d'apprentissage sur la violence basée sur le genre facilitée par la technologie. Learning Brief 3 : Implications de la VBG facilitée par la technologie et actions pour les agences humanitaires, les donateurs et les industries en ligne.

109 Plan International, Free to be online? (voir note de bas de page 6).

110 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

111 Flynn, Powell et Hindes, Technology-facilitated abuse.

112 Malanga, Lutter contre la cyber-violence basée sur le genre.
113 Plan International, Free to be online? (voir note de bas de page 6).
114 Amnesty International, Toxic Twitter (voir note de bas de page 5).
115 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).
116 Malanga, Lutter contre la cyber-violence basée sur le genre.
117 Plan International, Free to be online? (voir note de bas de page 6).
118 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).
Plan International, Free to be online? (voir note de bas de page 6).
119 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (voir note de bas de page 108).
120 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).
121 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (voir note de bas de page 108).
122 *Wall Street Journal*, The Facebook files (voir note de bas de page 80).
123 Flynn, Powell et Hindes, Technology-facilitated abuse.
124 Ibid.
125 Parsons, Molnar, Dalek, Knockel, Kenyon, Haselton, Khoo et Deibert, The Predator in Your Pocket (voir note 27).
126 Freed, Palmer, Minchala, Levy, Ristenpart et Dell, A stalker's paradise (voir note de bas de page 62).
127 Freed, Palmer, Minchala, Levy, Ristenpart et Dell, Digital technologies and intimate partner violence (voir note de bas de page 54).
128 C. Laxton (2014). Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking. Disponible sur : https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf
129 Dunn, Technology-facilitated gender-based violence : an overview (voir note de bas de page 24).
130 https://www.gbvims.com/
131 Compte tenu de la numérisation croissante des services de santé, par exemple, il existe un risque accru de problèmes liés à la vie privée et à la confidentialité des données, ainsi que de violations de la protection des données. En effet, l'OMS a indiqué que même si 70 % des 113 pays étudiés disposaient d'une législation relative aux droits fondamentaux à la vie privée, seuls 30 % d'entre eux avaient une législation sur la confidentialité des dossiers médicaux électroniques. Les pays sont encore moins nombreux à disposer d'un cadre juridique pour les dossiers médicaux électroniques qui ne se limite pas au respect de la vie privée. L'absence de politiques et de cadres juridiques sur des sujets tels que la propriété, la confidentialité et la sécurité des données a été identifiée comme un obstacle majeur à la généralisation des dossiers médicaux numériques.
D'après l'Organisation mondiale de la santé (2012). Cadres juridiques de la santé en ligne : d'après les résultats de la deuxième enquête mondiale sur la santé en ligne. (Série de l'Observatoire mondial de la santé en ligne, v.5). Disponible sur : https://www.who.int/goe/publications/legal_framework_web.pdf
132 Alisha C. Salerno-Ferraro, Caroline Erentzen et Regina A. Schuller, "Young women's experiences with technology-facilitated sexual violence from male strangers", *Journal of Interpersonal Violence*, (2021), https://doi.org/10.1177/08862605211030018.
133 Commission eSafety Australie. Abus en ligne ciblant les femmes. Disponible sur : https://www.esafety.gov.au/women/online-abuse-targeting-women
134 Plan International, Free to be online? (voir note de bas de page 6).
135 Ibid.
136 Amnesty International, Toxic Twitter (voir note de bas de page 5).
137 UNICEF East Asia & Pacific (2021). What we know about the gender digital divide for girls: a literature review. Disponible sur : https://www.unicef.org/eap/reports/innovation-and-technology-gender-equality-0
138 Economist Intelligence Unit, Measuring the prevalence of online violence (voir note de bas de page 65).
139 Khoo, Deplatforming misogyny (voir note de bas de page 4).
140 Ibid.
141 Oltermann, P. 5 janvier 2018. Une nouvelle loi allemande sévère met les entreprises technologiques et la liberté d'expression sous les projecteurs. Disponible à l'adresse : https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight
142 Khoo, Deplatforming misogyny (voir note de bas de page 4).
143 Ibid.
144 Commissaire à l'eSafety. Disponible à l'adresse : https://www.esafety.gov.au/ [consulté le 4 novembre 2021].
145 Loi sur la sécurité en ligne de 2021 (Cth). No. 76, 2021. (Austl.)
146 Khoo, Deplatforming misogyny (voir note de bas de page 4).
147 Ibid.
148 Larry Hardesty (2018). Une étude révèle des biais liés au sexe et au type de peau dans les systèmes commerciaux d'intelligence artificielle. Disponible sur : https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212
149 Rebecca Heilweill (2020). Pourquoi les algorithmes peuvent être racistes et sexistes. Disponible sur : https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency
Brian Resnick (2019). Oui, l'intelligence artificielle peut être raciste. Disponible sur : https://www.vox.com/science-and-health/2019/1/23/18194717/alexandria-ocasio-cortez-ai-bias
150 Khoo, Deplatforming misogyny (voir note de bas de page 4).

Partie 2

Recommandations et stratégies pour la VBGFT

Prévention et Réponse

Compte tenu des formes nouvelles et en constante évolution et des caractéristiques spécifiques de la VBGFT, les efforts de prévention et de réponse requièrent des efforts collectifs des gouvernements nationaux et des entreprises technologiques privées, y compris les entreprises de plateformes. Ces efforts doivent être guidés par des approches fondées sur les droits humains, en tenant compte des expériences des femmes et des filles dans toute leur diversité, afin de s'assurer que la réforme et la réglementation visant à prévenir et à répondre à la VBGFT répondent à leurs besoins.

Vous trouverez ci-dessous une liste non exhaustive de recommandations à l'intention des États et des entreprises technologiques privées pour faire face à la prévalence et à l'impact croissants de la VBGFT respectivement. Ces recommandations nécessitent un investissement important et durable en ressources financières, techniques et humaines de la part des organismes nationaux et internationaux, des gouvernements et du secteur privé. Elles nécessitent également des partenariats solides entre les entreprises technologiques privées, les gouvernements, les mouvements féministes et de défense des droits numériques, les prestataires de services liés à la violence basée sur le genre, les universitaires et, enfin et surtout, les victimes de VBGFT.

1 Recommandations pour les gouvernements nationaux

Politique et législation

La législation et les politiques doivent s'inscrire dans le cadre des droits humains et s'attaquer aux discriminations, violences et inégalités structurelles auxquelles les femmes sont confrontées. Les cadres juridiques doivent protéger de manière adéquate tous les droits fondamentaux des femmes en ligne, notamment le droit à une vie exempte de violence, la liberté d'expression et l'accès à l'information, ainsi que le droit à la vie privée et à la protection des données.[151] Outre le renforcement de la responsabilité des auteurs de violences, les lois doivent réglementer les entreprises technologiques privées afin qu'elles appliquent des mécanismes de sécurité et d'intervention pour prévenir et atténuer les cas de VBGFT.

Les politiques et la législation doivent être élaborées avec la pleine participation et consultation des victimes de VBGFT, des prestataires et services de première ligne, ainsi que des universitaires et des experts techniques dans les domaines de la réglementation des plateformes, de la modération des contenus et de la responsabilité algorithmique.

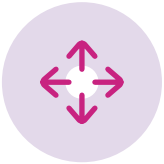
- Reconnaissance et intégration de la VBGFT dans les lois, réglementations et politiques civiles et pénales afin de réglementer les entreprises technologiques privées et de demander des comptes aux contrevenants.
- Mettre en place un organe statutaire indépendant pour traiter la question de la VBGFT, avec un mandat qui peut inclure les éléments suivants : (a) des pouvoirs pour administrer les recours juridiques et le soutien aux personnes touchées par la VBGFT sur les plateformes numériques ; (b) des pouvoirs de réglementation et d'exécution sur les entreprises technologiques privées pour intégrer des mécanismes de sécurité et supprimer immédiatement les contenus préjudiciables ; (c) des progrès dans la recherche sur la VBGFT pour soutenir une législation et une politique fondées sur des preuves ; (d) la défense et la facilitation de la suppression des contenus préjudiciables sur signalement des victimes ou des prestataires de services de première ligne ; (e) la formation et l'éducation du public, des parties prenantes et des professionnels concernés ; (f) le soutien des partenariats avec les entreprises technologiques privées pour permettre le respect des exigences de sécurité obligatoires ou volontaires.
- Lorsque de nouvelles lois et politiques sont introduites, elles doivent être claires, non discriminatoires et proportionnées. Elles doivent être dotées d'un budget adéquat pour garantir leur mise en œuvre et les autorités chargées de l'application de la loi et le pouvoir judiciaire doivent recevoir la formation et les compétences requises en conséquence.
- Les lois doivent exiger la mise en place de recours rapides, pratiques et accessibles pour les personnes visées par la VBGFT, y compris le soutien à des espaces de modération accessibles pour faire appel du refus de retirer les contenus offensants.
- Exiger des systèmes renforcés pour soutenir la sécurité des données, y compris les informations confidentielles collectées et gérées par l'État et les données collectées par le biais d'applications et de plateformes de localisation.
- Il convient de mettre en place des accords internationaux et un cadre législatif commun pour lutter contre la VBGFT transfrontalière liée. Les auteurs ne sont souvent pas tenus pour responsables en raison de problèmes de compétences entre juridictions car ils commettent les abus depuis différents États ou pays.
- Il doit également exister des possibilités effectives de faire appel des décisions considérées comme injustes.

Dans la réglementation des entreprises technologiques privées :

- rendre obligatoire et appliquer des lois et des règlements qui obligent les entreprises technologiques privées à élaborer, maintenir et mettre en œuvre des politiques visant à répondre à la VBGFT et à en atténuer les effets par le biais d'une série de processus, notamment les suivants : (1) des mécanismes de signalement des plaintes et des abus de contenus préjudiciables visibles, facilement accessibles et rédigés en langage clair, (2) le retrait **immédiat** des contenus préjudiciables lorsqu'ils sont signalés (tout en conservant des enregistrements à des fins de preuve) ; (3) des mécanismes de modération efficaces ; (4) l'obligation de former l'ensemble du personnel pour qu'il comprenne son rôle dans la surveillance et le retrait des contenus préjudiciables liés à la VBGFT; (5) la réalisation d'audits indépendants et la publication de rapports annuels complets sur la mise en œuvre des politiques ;
- veiller à ce que la réglementation permette le retrait immédiat d'un contenu préjudiciable défini d'une plateforme sans qu'il soit nécessaire de recourir à une décision de justice, ainsi qu'aux coûts et aux autres défis juridiques associés.[152] L'accent doit être mis sur l'amélioration des processus transparents de modération du contenu autant que sur les restrictions spécifiques au contenu ;
- lorsqu'un ordre est donné à l'encontre d'une société de plateforme, assurez-vous qu'il exige le retrait du contenu de toute société de plateforme mère, filiale ou sœur de cette plateforme où le même contenu apparaît également ;[153]
- envisager la mise en place d'incitations pour les entreprises technologiques privées afin d'encourager le respect et la promotion active de la protection des femmes et des filles utilisant leurs services ;
- la publicité, la vente et la distribution d'applications et de dispositifs commercialisés à des fins de surveillance doivent être soigneusement contrôlées et uniquement autorisées à des fins particulières. Leur accès doit également être restreint, notamment par leur retrait des magasins d'applications officiels.

Des mécanismes de réponse renforcés

Il est essentiel d'investir de manière soutenue et approfondie dans des mécanismes de réponse centrés sur les survivants et fondés sur le féminisme, qui traitent toutes les formes de GBVFT, qu'il s'agisse d'un incident isolé ou d'un modèle de comportement.



- Garantir des approches participatives et féministes dans la conception des lois, des politiques, des mécanismes de réponse renforcés et des documents de formation associés afin de saisir l'étendue de l'expérience des victimes.
- Renforcer les services de réponse globale et axée sur les victimes en matière de violence sexuelle et sexiste en proposant une formation continue et en renforçant les capacités des prestataires de services dans tous les secteurs (y compris les responsables de l'application de la loi, les magistrats, les travailleurs sociaux chargés des cas de VBG , les prestataires de soins de santé et de services psychosociaux, les travailleurs du secteur du logement et des services sociaux) afin de favoriser l'identification, la réponse et l'intervention précoce sûres et axées sur les survivants en matière de VBGFT.
- Engager les organismes professionnels, y compris ceux destinés à soutenir les journalistes et les politiciens, à fournir un espace de rassemblement pour la collaboration entre les associations professionnelles et les services de réponse à la VBGFT.
- Veiller à l'intégration des entreprises technologiques privées dans les mécanismes de référence existants des intervenants de première ligne en matière de VBG afin de garantir une réponse active et immédiate à la VBGFT par le biais d'une série de mécanismes, notamment en soutenant un service intermédiaire capable de faciliter l'accès des services de première ligne en matière de VBG aux points focaux des entreprises technologiques privées.
- Des ressources financières, humaines et techniques pour les travailleurs de soutien de première ligne et les organisations à base communautaire afin de permettre des interventions immédiates et efficaces, avec le soutien total des services sanitaires, sociaux, policiers et juridiques, y compris les entreprises technologiques privées.
- Veillez à ce que les abris et les espaces sûrs bénéficient de la sécurité requise (physique et en ligne) pour garantir la confidentialité du lieu.
- Veiller à ce que tous les acteurs du système judiciaire reçoivent la formation et les ressources nécessaires pour garantir un haut niveau d'expertise et de familiarité avec les technologies de l'information et de la communication et leur fonctionnement, ainsi qu'avec les preuves numériques, afin de garantir que les preuves appropriées sont collectées, préservées et dûment prises en compte et d'éviter que les victimes ne soient à nouveau traumatisées au cours des procédures judiciaires.[154]

Investissement dans la prévention

La prévention de la VBGFT nécessite de travailler avec des individus et des groupes de victimes, des défenseurs et des activistes, des prestataires de services en matière de VBG ainsi que des entreprises privées, des départements et organisations publics et gouvernementaux ainsi que des associations professionnelles. Une stratégie et une approche déterminantes pour le soutien et le maintien des efforts de prévention consisteront à créer et maintenir ces partenariats, sous la coordination du gouvernement national.

Éducation

- Investir pour améliorer la culture numérique des adolescents, des femmes, en particulier des femmes âgées, des activistes et des professionnels dans toute leur diversité, en proposant des cours ou des ateliers gratuits et accessibles qui peuvent être intégrés dans les établissements d'enseignement scolaire, universitaire et professionnel, les lieux de travail et les espaces communautaires.
- Intégration de modules et de concepts dans les programmes d'enseignement (curricula) et de formation (y compris l'éducation sexuelle complète), afin de favoriser un comportement et des interactions en ligne sains.[155]
- Développement de curricula et de formations accessibles pour les établissements d'enseignement et les services communautaires afin d'offrir une formation aux membres de la communauté de tous âges et dans toute leur diversité.
- Fourniture de l'accès à des services de soutien aux membres de la communauté et en particulier aux femmes dans toute leur diversité pour naviguer dans la technologie et les espaces en ligne.
- Développement d'outils pour soutenir les femmes dans toute leur diversité, les parents et les éducateurs afin de leur permettre de protéger la vie privée en ligne des enfants, des élèves et des étudiants.
- Poursuite et intensification des travaux visant à garantir que les programmes de prévention de la VBG incluent la participation des hommes et des garçons à la transformation des masculinités néfastes afin de lutter contre les comportements en ligne.
- Investissement dans l'évaluation des programmes d'éducation et de prévention afin de déterminer leur efficacité à changer les attitudes et les comportements en ligne.

Soutenir l'action communautaire et le plaidoyer

- Promouvoir la création d'espaces pour les groupes de pairs vulnérables à la VBGFT en tant que réseau de soutien essentiel. Les groupes de soutien par les pairs dirigés par des femmes journalistes sont des exemples de réussite.[156]
- Promouvoir et protéger la voix des femmes et leur participation en toute sécurité dans la sphère en ligne, en encourageant les comportements de soutien et en fournissant aux femmes et aux filles les compétences nécessaires pour contrer les abus.
- Soutenir activement les défenseurs et activistes féministes, les femmes défenseurs des droits humains, les journalistes et les politiciennes qui maintiennent une présence en ligne pour qu'elles puissent continuer à dialoguer avec le public par ce moyen sans craindre la VBGFT , en créant des réseaux de pairs (là où il n'y en a pas encore) et en facilitant la modération proactive du contenu par les entreprises technologiques privées.

Sécurité des données

- Des ressources dédiées à l'élaboration et à la mise en œuvre de la législation, des politiques, des systèmes et des processus, ainsi que du personnel qualifié pour assurer la sécurité des données confidentielles.
- Des ressources pour permettre aux prestataires de services de première ligne de continuer à collecter et à protéger en toute sécurité les données relatives aux victimes de VBG. Cela est essentiel étant donné le continuum de la violence en ligne et hors ligne, en particulier dans le contexte de la VPI.

Données et recherche

Des données et des recherches renforcées sont nécessaires pour fournir une base sur laquelle les politiques, les programmes, les lois et les stratégies de plaidoyer peuvent être élaborés. Il est essentiel de comprendre les formes de VBGFT , ses impacts, ses cibles principales et ses auteurs, ainsi que les remèdes nécessaires et souhaités, et les mécanismes de responsabilité appropriés.

- Des définitions et une terminologie mondiales et normalisées de la VBGFT, ainsi que de ses différentes formes, tactiques et comportements associés, doivent être élaborées et acceptées.
- Inclusion de la VBGFT en tant que forme ou expérience de violence à inclure dans les enquêtes standardisées basées sur la population[157], y compris, par exemple, la méthodologie de l'étude multi-pays de l'OMS ou l'enquête démographique et de santé qui sont utilisées pour déterminer la prévalence de la VBG. Pour ce faire, des mesures standardisées de la VBGFT, y compris toutes ses formes, doivent être développées, testées et adaptées à travers les contextes et les cultures.
- Veiller à l'inclusion de la VBGFT comme forme de violence dans les systèmes de données administratives sur la VBG. Cela peut nécessiter, par exemple, de modifier les formulaires d'admission et les documents de gestion des cas pour enregistrer le contexte (en ligne ou hors ligne) dans lequel la violence a eu lieu. Cela permettra de mieux comprendre la manière dont les cas de VBGFT sont signalés, renvoyés et gérés, et d'analyser les tendances, ce qui pourra servir de base à un plaidoyer et à des interventions fondées sur des preuves.
- Une attention et une concentration accrues sur la production de recherches pour déterminer « ce qui fonctionne » pour prévenir et répondre à la VBGFT.
- Ressources pour des recherches empiriques, interdisciplinaires, juridiques et politiques approfondies menées par des universitaires de la VBGFT, des experts de la VBGFT et des organisations communautaires travaillant sur la VBGFT et sur l'impact des technologies émergentes sur les victimes de la VBGFT de tous âges et de toutes origines. Par exemple, soutenir la recherche pour prévenir les abus dans les communications cryptées.[158]

GOVERNO DO DISTRITO DE CHICUALACUALA

SERVIÇO DISTRITAL DE SAÚDE, MULHER E ACÇÃO SOCIAL

PROGRAMA DE VIOLÊNCIA BASEADA NO GÊNERO

Nº DE ORDEM	DATAS	ACTIVIDADE	RESPONSABILIDADE
01	01/12/20	Realização de palestras de sensibilização e consciencialização sobre a Violência Baseada no Género	Ponto focal de VBG
02	08/12/20	Encontro de Coordenação Multisectorial de Atendimento Integrado a Violência Baseada no Género	Mecanismo Multissectorial
03	15/12/20	Realização de Supervisão e Apoio Técnico	Ponto focal de VBG
04	22/12/20	Sessões de debates radiofónicos sobre a Violência Baseada no Género	Ponto focal de VBG
05	29/12/20	Realização de visitas domiciliares a famílias vítimas de Violência Baseada no Género	Ponto focal de VBG

Chicualacuala, 01 de Dezembro de 2020

Salomão Gonçalves Matavele

Téc. Sup. de Saúde N1

LINHAS DE DENÚN

86 274 33 94-

87 542 43 68-

86 872 10 91-

2 Recommandations pour les entreprises technologiques privées

Les entreprises privées doivent reconnaître leur rôle dans la perpétration de la VBGFT et créer et entretenir des partenariats à long terme et productifs avec les prestataires de services liés à la VBG, les femmes dans toute leur diversité, les associations professionnelles, les universitaires et le gouvernement national, afin de soutenir des mécanismes de sécurité informés, efficaces et immédiats qui répondent immédiatement, protègent et promeuvent le droit des femmes et des filles à ne pas subir de violence en ligne et hors ligne.

- Le développement et l'application des technologies et des plateformes numériques doivent se faire en partenariat et avec la participation des femmes dans toute leur diversité ainsi que des organisations et des défenseurs,[159] pour garantir des dispositifs de sécurité et des mécanismes de plainte pertinents et accessibles.
- La prévention, l'atténuation et la réponse à la VBGFT doivent être incluses dans les procédures opérationnelles standard des réseaux sociaux et des entreprises technologiques afin de garantir le retrait immédiat des contenus préjudiciables, la modération active et les mesures d'atténuation de la VBGFT.
- Les mécanismes de traitement des plaintes doivent garantir une réponse immédiate et le retrait du document nuisible, dans l'attente d'une enquête plus approfondie, conformément aux politiques de bonnes pratiques, ainsi que le retrait du document de toutes les filiales et sites associés.
- Assurer des politiques et des réponses claires et transparentes en matière de modération du contenu.
- La sécurité doit être intégrée dès la phase de conception. Pour des conseils pratiques et des recommandations réalisables, voir le rapport de résultats et de recommandations « Tech Policy Design Lab : Online Gender-Based Violence and Abuse », qui s'appuie sur les résultats d'une série d'ateliers avec les parties prenantes concernées, y compris les victimes de la VBGFT en ligne et les entreprises technologiques.[160]
- Des points focaux désignés au sein de l'entreprise, disponibles à tout moment, pour prendre en charge les plaintes et retirer les contenus offensants et violents.
- Exiger que l'ensemble du personnel des entreprises et des plateformes technologiques de démarrage participe à une formation visant à améliorer la compréhension de la VBGFT et leur rôle dans le contrôle et le retrait des contenus préjudiciables.

151 Michael Geist (2021). Tracking the submissions: what the government heard in its online harms consultation (since it refuses to post them). Disponible sur : https://www.michaelgeist.ca/2021/10/tracking-the-submissions-what-the-government-heard-in-its-online-harms-consultation-since-it-refuses-to-post-them/

152 H. Young et E. Laidlaw (2020). Creating a Revenge Porn Tort for Canada. Supreme Court Law Review, 2020, disponible sur SSRN : https://ssrn.com/abstract=3586056.

153 Khoo, Deplatforming misogyny (voir note de bas de page 4).

154 S. Dunn et M. Aikenhead, "On the internet, nobody knows you are a dog: contested authorship of digital evidence in cases of gender-based violence", *Canadian Journal of Law and Tech*. (à paraître).

155 UNFPA (2021). L'éducation sexuelle complète comme stratégie de prévention de la violence liée au sexe.

156 GBV AoR Helpdesk (2021). Série d'apprentissage sur la violence basée sur le genre facilitée par la technologie. Learning Brief 2 : Stratégies et actions pour prévenir et répondre à la VBG facilitée par la technologie.

157 https://asiapacific.unfpa.org/sites/default/files/pub-pdf/kNOwVAWdata%20Methodology.pdf

158 Cornell Tech (2021). Un nouveau projet vise à prévenir les abus dans les communications cryptées. Disponible sur : https://tech.cornell.edu/news/preventing_abuse_in_encrypted_communication/

159 Des organisations et des défenseurs tels que l'Association for Progressive Communications ou Association pour le progrès des communications (https://www.apc.org/en), la World Wide Web Foundation (https://webfoundation.org/), Derechos Digitales (https://www.derechosdigitales.org/), Internet Democracy Project (https://internetdemocracy.in/) ou Gender IT (https://genderit.org/es).

160 Voir World Wide Web Foundation, Feminist Internet et Craig Walker (2021). Tech Policy Design Lab : Violence et abus sexistes en ligne. Disponible sur : https://uploads-ssl.webflow.com/61557f76c8a63ae527a819e6/61557f76c8a63a65a6a81adc_OGBV_Report_June2021.pdf

Partie 3

Aperçu des enquêtes

visant à mesurer
la prévalence
de la VBGFT

Le tableau ci-dessous donne un aperçu de la gamme d'études de prévalence qui ont été publiées concernant la VBGFT .

Source	Localisation	Terme utilisé et définition	Population et taille de l'échantillon	Données de prévalence
Economist Intelligence Unit (2021)[161]	51 pays présentant les taux de pénétration de l'internet les plus élevés dans toutes les régions	Violence en ligne à l'égard des femmes - femmes ayant signalé des expériences personnelles de violence en ligne	4 500 femmes âgées de 18 à 74 ans	38%
Groupe de la Banque africaine de développement (2016)[162]	Kenya	Harcèlement en ligne Contacté par des imposteurs en ligne, discours de haine personnelle, cyberintimidation et *trolling* en ligne	Non défini	>33% (harcèlement en ligne) 33% (autres formes de violence, y compris discours de haine, cyberintimidation et *trolling*)
Plan International (2020)[163]	31 pays dans toutes les régions	Harcèlement en ligne, « allant des menaces de violence physique ou sexuelle aux commentaires racistes et la traque furtive »	14 000 jeunes femmes et jeunes filles âgées de 15 à 25 ans	58%
World Wide Web Foundation (2020)[164]	180 pays	Les abus en ligne, notamment les messages menaçants, le harcèlement sexuel et le partage de photos et de vidéos privées sans autorisation	8 109 répondants (51% de femmes), âgés pour la plupart de 15 à 30 ans.	52% (des femmes)
Neema Iyer, Bonnita Nyamwire et Sandra Nabulega (2020)[165]	Cinq pays africains (Afrique du Sud, Ethiopie, Kenya, Ouganda et Sénégal)	La VBG en ligne, notamment le harcèlement sexuel, les injures, la traque et le *doxxing*	3 306 femmes âgées de 18 à 65 ans, qui accèdent à l'internet et l'utilisent au moins une fois par semaine	28.2%
Digital Rights Foundation (2017)[166]	Pakistan	Traque ou harcèlement via des applications de messagerie	1 400 jeunes étudiantes (âgées de 18 ans ou plus) et leurs enseignantes dans 17 universités du Pakistan	40%

Source	Localisation	Terme utilisé et définition	Population et taille de l'échantillon	Données de prévalence
F.M. Hassan, F.N. Khalifa, E.D. El Desouky et al. (2020)[167]	Égypte	Cyberviolence contre les femmes et les filles	356 femmes adultes (≥18 ans) présentes sur les groupes Facebook de femmes.	41,6%
D. Woodlock, K. Bentley, D. Schulze, N. Mahoney, D. Chung et A. Pracilio (2020)[168]	Australie	Traque furtive et abus facilités par la technologie	442 praticiens en matière de violence conjugale, familiale et sexuelle (426 femmes)	99,3% (des participants ont travaillé avec des clients victimes d'abus facilités par la technologie)

La prévalence de formes spécifiques de VBGFT a également été saisie dans le cadre d'efforts de collecte de données régionales et nationales, dont un résumé est présenté dans le tableau ci-dessous.

Forme de VBGFT	Sous-type	Localisation et population	Prévalence ou aperçu des données	Source
Harcèlement en ligne	**Harcèlement en ligne, après l'âge de 15 ans**	Union européenne, femmes	11%	A. Van der Wilk (2018)[169]
		31 pays dans le monde, jeunes femmes et filles âgées de 15 à 25 ans	58%	Plan International (2020)[170]
	Harcèlement en ligne, langage abusif et insultant	31 pays dans le monde, jeunes femmes et filles âgées de 15 à 25 ans	59%	Plan International (2020)[171]
	Harcèlement en ligne, menaces de violence sexuelle	31 pays dans le monde, jeunes femmes et filles âgées de 15 à 25 ans	39%	Plan International (2020)[172]
	Harcèlement en ligne, menaces de violence physique	31 pays dans le monde, jeunes femmes et filles âgées de 15 à 25 ans	21%	Plan International (2020)[173]
Formes sexualisées d'abus en ligne		États-Unis, hommes et femmes	9% des hommes et 21% des femmes de 18 à 29 ans (soit plus du double)	Pew Research Center (2017)[174]
		Canada, étudiants de premier cycle, âge moyen 23,79 ans et 72% de femmes	88% des femmes	Lindsey A. Snaychuk et Melanie L. O'Neill (2020)[175]
		31 pays dans le monde, jeunes femmes et filles âgées de 15 à 25 ans	37%	Plan International (2020)[176]

Forme de VBGFT	Sous-type	Localisation et population	Prévalence ou aperçu des données	Source
Cyberharcèlement	**Cyberharcèlement, après l'âge de 15 ans**	Union européenne, femmes	5%	A. Van der Wilk (2018)[177]
	Cyberharcèlement, au cours de l'année écoulée	Union européenne, femmes	2%	A. Van der Wilk (2018)[178]
		31 pays dans le monde, des jeunes femmes et des filles âgées de 15 à 25 ans	32%	Plan International (2020)[179]
		Sénégal, Afrique du Sud, Kenya, Ouganda et Éthiopie, femmes de 18 à 65 ans.	26,7%	N. Iyer, B. Nyamwire et S. Nabulega (2020)[180]
Abus sexuel par l'image	**Partage non consensuel d'images dénudées ou sexuelles**	Pays à revenu élevé (étude de synthèse)	1–12%	N. Henry, A. Flynn et A. Powell (2020)[181]
	Menaces de partager des images dénudées ou sexuelles	Pays à revenu élevé (étude de synthèse)	1–15%	N. Henry, A. Flynn et A. Powell (2020)[182]
	Prévalence globale, estimation	Examen systématique et méta-analyse, principalement des populations occidentales.	9%	U. Patel et R. Roesch (2020)[183]
Expériences sexuelles non désirées facilitées par la technologie	**On lui demande de se livrer à des activités ou des comportements sexuels non désirés.**	Pays-Bas, adultes âgés de 18 à 88 ans	4,6% des hommes, 6,7% des femmes	S.E. Baumgartner, P.M. Valkenburg et J. Peter (2010)[184]
	Adopter au moins un comportement de victimisation sexuelle sur dix.	Espagne, adultes	38%	M. Gámez-Guadix, C. Almendros, E. Borrajo et E. Calvete (2015)[185]

Forme de VBGFT	Sous-type	Localisation et population	Prévalence ou aperçu des données	Source
Doxxing		États-Unis	29%	Amnesty International (2018)[186]
		Huit pays à revenu élevé	11%	Amnesty International (2018)[187]
VBGFT directement liées à la traite ou à des fins de recrutement et d'exploitation		Serbie, victimes de la traite des êtres humains	31%	Andrijana Radoičić (2020)[188]
Usurpation d'identité	**Au moins une menace d'usurpation d'identité**	Inde, Bangladesh et Pakistan, membres cisgenres et non cisgenres	15%	N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, L.S. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill et S. Consolvo (2019)[189]
	Attaques d'usurpation d'identité impliquant la création de faux profils avec l'identité de la victime	Inde, Bangladesh et Pakistan, membres cisgenres et non cisgenres	12%	N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, L.S. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill et S. Consolvo (2019)[190]
Discours de haine sexiste		Union européenne	3,1% des signalements aux plateformes Internet concernent des propos haineux à l'égard du genre	A. Van der Wilk (2018)[191]
		Malawi, femmes de 15 à 45 ans	46,3%	D.F. Malanga (2020)[192]
Diffamation		États-Unis, hommes et femmes adultes	26% des adultes ont vu de fausses informations les concernant publiées en ligne, les différences entre les sexes étant modestes	Pew Research Center (2017)[193]
		Malawi, femmes de 15 à 45 ans	43,3%	D.F. Malanga (2020)[194]

161 Economist Intelligence Unit, Measuring the prevalence of online violence (voir note de bas de page 65).

162 Groupe de la Banque africaine de développement (2016). Combler les lacunes : identifier les stratégies pour lutter contre la cyberviolence basée sur le genre au Kenya. Disponible sur : https://www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/Policy_Brief_on_Gender_Based_Cyber_Violence_in_Kenya.pdf

163 Plan International, Free to be online? (voir note de bas de page 6).

164 The World Wide Web Foundation, The online crisis facing women and girls (voir note de bas de page 78).

165 N. Iyer, B. Nyamwire et S. Nabulega (2020) Alternate Realities, Alternate Internets : Recherche féministe africaine pour un Internet féministe, Pollicy. Disponible sur : https://ogbv.pollicy.org/report.pdf

166 Digital Rights Foundation (2017). Mesure des expériences des femmes pakistanaises en matière de violence en ligne. Disponible sur : https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/ Hamara-Internet-Online-Harassment-Report.pdf.

167 F.M. Hassan, F.N. Khalifa, E.D. El Desouky, M.R. Salem et M.M. Ali, "Cyber violence pattern and related factors: online survey of females in Egypt", *Egyptian Journal of Forensic Sciencesvol*. 10, n° 6, (2020), https://doi.org/10.1186/s41935-020-0180-0.

168 D. Woodlock, K. Bentley, D. Schulze, N. Mahoney, D. Chung et A. Pracilio, (2020). Deuxième enquête nationale sur l'abus de technologie et la violence domestique en Australie. WESNET. Disponible sur : https://wesnet.org.au/about/research/2ndnatsurvey/

169 Van der Wilk, Cyberviolence et discours de haine en ligne contre les femmes (voir note de bas de page 52).

170 Plan International, Free to be online? (voir note de bas de page 6).

171 Ibid.

172 Ibid.

173 Ibid.

174 Duggan, Harcèlement en ligne 2017 (voir note de bas de page 69).

175 Lindsey A. Snaychuk et Melanie L. O'Neill, "Technology-facilitated sexual violence: prevalence, risk, and resiliency in undergraduate students", *Journal of Aggression, Maltreatment & Trauma*, vol. 29, No. 8, (2020), pp. 984-999, doi : 10.1080/10926771.2019.1710636

176 Plan International, Free to be online? (voir note de bas de page 6).

177 Van der Wilk, Cyber violence et discours de haine en ligne contre les femmes (voir note de bas de page 52).

178 Ibid.

179 Plan International, Free to be online? (voir note de bas de page 6).

180 Iyer, Nyamwire et Nabulega, Alternate realities, alternate internets (voir note de bas de page 165).

181 Henry, Flynn et Powell, Technology-facilitated domestic and sexual violence (voir note de bas de page 32).

182 Ibid.

183 U. Patel et R. Roesch, "The prevalence of technology-facilitated sexual violence: a meta-analysis and systematic review", *Trauma, Violence, & Abuse*, (2020), doi:10.1177/1524838020958057

184 S.E. Baumgartner, P.M. Valkenburg et J. Peter, "Unwanted online sexual solicitation and risky sexual online behavior across the lifespan", *Journal of Applied Developmental Psychology*, vol. 31, (2010), pp. 439-447.

185 M. Gámez-Guadix, C. Almendros, E. Borrajo et E. Calvete, " Prevalence and association of sexting and online sexual victimization among Spanish adults ", *Sexuality Research and Social Policy*, vol. 12, (2015), pp. 145-154.

186 Amnesty International, Toxic Twitter (voir note de bas de page 5).

187 Ibid.

188 Andrijana Radoičić (2020). Derrière les écrans : Analyse des abus des victimes de la traite des êtres humains dans l'environnement numérique. Disponible sur : http://www.atina.org.rs/en/behind-screens-analysis-human-trafficking-victims-abuse-digital-surroundings

189 N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, LS. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill et S. Consolvo, "They don't leave us alone anywhere we go: gender and digital abuse in South Asia", CHI '19 : Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 4-9 mai 2019. Disponible sur : https://storage.googleapis.com/pub-tools-public-publication-data/pdf/acf12158ab313c1e9d80b87ede-065254f64ad9a7.pdf

190 Ibid.

191 Van der Wilk, Cyber violence et discours de haine en ligne contre les femmes (voir note de bas de page 52).

192 Malanga, Tackling gender-based cyber violence (voir note de bas de page 99).

193 Duggan, Harcèlement en ligne 2017 (voir note de bas de page 69).

194 Malanga, Tackling gender-based cyber violence (voir note de bas de page 99).

Partie 4

Glossaire des termes

Définitions de la VBGFT

Source	Terme	Définition
HCDH (A/HRC/38/47, para. 23)[195]	**VBG contre les femmes en ligne**	La VBG contre les femmes en ligne, et en particulier contre les femmes journalistes qui utilisent les technologies de l'information et de la communication comme outils de travail, comprend tout acte de violence commis, aidé ou aggravé en partie ou en totalité par l'utilisation des technologies de l'information et de la communication, telles que les téléphones portables et les smartphones, l'internet, les plateformes de réseaux sociaux ou le courrier électronique, contre une femme parce qu'elle est une femme, ou qui affecte les femmes de manière disproportionnée.
A. Flynn, A. Powell et S. Hindes (2021)[196]	**Abus facilité par la technologie (AFT)**	L'abus facilité par la technologie englobe les schémas existants de violence, de harcèlement et d'abus qui sont étendus et amplifiés par les médias numériques, ainsi que de nouvelles formes d'abus, comme l'ABI. L'AFT est très large et comprend de nombreux sous-types de violence et d'abus interpersonnels utilisant les technologies mobiles, en ligne et autres technologies numériques. Il peut s'agir de harcèlement et de comportements de surveillance, d'abus psychologique et émotionnel (y compris les menaces), de violence sexuelle et d'abus basés sur l'image, ainsi que de harcèlement sexuel. Le terme se réfère aussi parfois plus largement à des formes de harcèlement en ligne général et de cyberintimidation. L'AFT se caractérise par une intersection entre les relations de pouvoir entre les sexes et les préjudices sexuels et/ou ceux subis par les partenaires intimes, car elle peut impliquer une extension numérique des comportements de contrôle coercitif employés par les auteurs de violences familiales pour surveiller, menacer et restreindre leurs partenaires ou ex-partenaires. L'AFT est également considérée comme ciblant fréquemment les femmes et ayant un impact disproportionné sur elles.
Nations unies[197]	**Violence en ligne et facilitée par les technologies de l'information et de la communication à l'égard des femmes et des filles**	La définition de la violence en ligne à l'égard des femmes s'étend à tout acte de VBG à l'égard des femmes qui est commis, aidé ou aggravé en partie ou en totalité par l'utilisation des technologies de l'information et de la communication, telles que les téléphones portables et les smartphones, l'internet, les plateformes de réseaux sociaux ou le courrier électronique, contre une femme parce qu'elle est une femme, ou qui affecte les femmes de manière disproportionnée.

Source	Terme	Définition
Institut européen pour l'égalité entre les hommes et les femmes[198]	**Cyberviolence contre les femmes et les filles**	La VBG qui est perpétrée par le biais de la communication électronique et de l'internet. Bien que la cyberviolence puisse toucher aussi bien les femmes que les hommes, les femmes et les filles en subissent des formes différentes et plus traumatisantes. Il existe diverses formes de cyberviolence à l'égard des femmes et des filles, notamment le cyberharcèlement, la pornographie non consensuelle (ou « *revenge porn* »), les insultes sexistes, les discours haineux et le harcèlement, la « *slut-shaming* », la pornographie non sollicitée, la « sextorsion », les menaces de viol et de mort, et la traite facilitée par les moyens électroniques. La cyberviolence n'est pas un phénomène distinct de la violence du « monde réel », car elle suit souvent les mêmes schémas que la violence hors ligne.
Centre international de recherche sur les femmes[199]	**Violence basée sur le genre facilitée par la technologie**	La VBGFT est une action d'une ou plusieurs personnes qui porte atteinte à d'autres personnes en raison de leur identité sexuelle ou de leur identité de genre ou en imposant des normes de genre préjudiciables. Cette action est menée en utilisant l'internet et/ou la technologie mobile et comprend la traque, l'intimidation, le harcèlement sexuel, la diffamation, les discours de haine et l'exploitation.
TEDIC[200]	**Violence de genre numérique**	La violence de genre numérique (ou en ligne) désigne les actes de violence de genre commis, incités ou aggravés, en partie ou totalement, par l'utilisation des technologies de l'information et de la communication, des plateformes de réseaux sociaux ou des services de courrier électronique. Cette violence cause des dommages psychologiques et émotionnels, renforce les préjugés, porte atteinte à la réputation, cause des pertes économiques, pose des obstacles à la participation à la vie publique, et elle peut conduire à la violence sexuelle et à d'autres formes de violence physique.
A. Powell, A.J. Scott et N. Henry (2018)[201]	**Harcèlement et abus numériques**	Terme générique désignant une série de comportements interpersonnels préjudiciables sur l'internet, ainsi que sur les téléphones portables et autres appareils de communication électronique. Ces comportements en ligne comprennent les commentaires offensants et les injures, le harcèlement ciblé, les violences verbales et les menaces, ainsi que le harcèlement et les abus sexuels liés à la sexualité et au genre. Le harcèlement et les abus sexuels fondés sur la sexualité et le genre désignent des comportements préjudiciables et non désirés de nature sexuelle ou dirigés contre une personne en raison de sa sexualité ou de son identité de genre.
Programme sur les droits des femmes de l'Association pour le progrès des communications (APC)[202]	**Violence à l'égard des femmes liée à la technologie**	Les actes de violence basée sur le genre qui sont commis, encouragés ou aggravés, en partie ou en totalité, par l'utilisation des technologies de l'information et de la communication, telles que les téléphones portables, l'internet, les plateformes de réseaux sociaux et le courrier électronique.
J. Bailey, A. Flynn et N. Henry[203]	**Violence et abus facilités par la technologie**	Terme générique utilisé pour décrire l'utilisation des technologies numériques pour perpétrer du harcèlement, des abus et de la violence interpersonnels, tels que la violence sexuelle, la violence conjugale et familiale, la haine fondée sur des préjugés et l'altérisation en ligne.

Formes de VBGFT

A

Abus financier par voie électronique
L'utilisation de l'Internet et d'autres formes de technologie pour exercer une pression financière sur une cible, généralement une femme impliquée dans un abus d'un partenaire intime. Cela peut inclure, par exemple, le refus d'accès à des comptes en ligne, la manipulation d'informations de crédit pour créer des scores négatifs et le vol d'identité.[204]

Abus basé sur l'image (ABI)
Utilisation d'images pour contraindre, menacer, harceler, chosifier ou maltraiter une victime, ce qui implique un large éventail de comportements consistant à prendre, partager ou menacer de partager des images intimes sans consentement. Ces images peuvent être de nature sexuelle, auquel cas on parle d'« abus sexuel par l'image ».[205]

Astroturfing
Diffusion ou amplification de contenus (y compris des abus) qui semblent naître organiquement au niveau de la base et se propager, mais qui sont en réalité coordonnés (souvent à l'aide de plusieurs faux comptes) par un individu, un groupe d'intérêt, un parti politique ou une organisation.[206]

Attaques dans la vie réelle
Incidents où l'abus en ligne passe dans le monde « réel » ou fait déjà partie d'une interaction continue de harcèlement ou de violence entre partenaires intimes. Le *trolling* dans la vie réelle peut également signifier le simple fait d'essayer d'inspirer la peur en faisant savoir à une cible que l'agresseur connaît son adresse ou son lieu de travail.[207]

Attaques par déni de service (DoS)
Une cyberattaque qui fait tomber un site web ou un réseau en panne ou le rend inopérant de manière temporaire ou indéfinie en submergeant un système avec des données. Les attaques par déni de service peuvent empêcher les gens d'accéder à leurs propres appareils et données, et elles peuvent compromettre les informations sensibles stockées sur ces appareils. Un déni de service distribué (DDoS) se produit lorsqu'un attaquant prend le contrôle des ordinateurs de plusieurs utilisateurs afin d'attaquer l'ordinateur d'un autre utilisateur. Cela peut forcer les ordinateurs détournés à envoyer de grandes quantités de données à un site web particulier ou à envoyer du spam à des adresses électroniques ciblées.[208]

B

Bombardement Google
L'optimisation délibérée d'informations et de sites web malveillants en ligne afin que les gens voient immédiatement le contenu diffamatoire lorsqu'ils recherchent une cible.[209]

C

***Catfishing* ou pêche au poisson-chat**
Escroquerie sur Internet où l'agresseur se fait passer pour quelqu'un qu'il n'est pas, en créant de fausses identités en ligne dans les réseaux sociaux - souvent en utilisant les photos d'autres personnes et en développant de fausses histoires de vie et d'expériences, des emplois et des amis - dans le but de séduire une autre personne ou de lui faire croire qu'elle est dans une relation en ligne et d'utiliser ce moyen pour demander de l'argent, des cadeaux ou des images intimes.[210]

***Cyberflashing* ou cyberexhibitionnisme**
Forme d'abus par l'image par laquelle une personne envoie une image non sollicitée de ses organes génitaux ou des documents sexuellement explicites à une autre personne sans son consentement.[211] Également appelé « *dick pics* », le *cyberflashing* est une forme de pornographie non sollicitée qui désigne plus largement « l'envoi de pornographie non sollicitée, de gifs pornographiques violents ou de photographies dans lesquelles la photo d'une cible a été sexualisée ».[212]

Cyberharcèlement
Forme sévère de poursuite cyberobsessionnelle, motivée par le contrôle ou la destruction relationnelle, qui consiste à utiliser la technologie pour traquer et surveiller de manière répétée les activités et les comportements d'une personne en temps réel ou par l'historique et qui amène la victime à ressentir de la peur.[213]

Cyberintimidation
Terme générique désignant un « préjudice intentionnel et répété infligé par l'utilisation d'ordinateurs, de téléphones portables et d'autres appareils électroniques »[214], généralement à l'aide de contenus textuels ou graphiques et dans le but d'effrayer et de saper l'estime de soi ou la réputation d'une personne.[215] Ce terme est principalement utilisé en relation avec les enfants et les jeunes.[216]

Deadnaming
Une forme de harcèlement direct dans lequel l'ancien nom d'une cible est révélé contre son gré dans le but de lui nuire. Cette technique est le plus souvent utilisée à l'encontre des membres de la communauté LGTBQIA+ qui peuvent avoir changé leur nom de naissance pour diverses raisons, notamment pour éviter la discrimination professionnelle et le danger physique.[217]

***Deepfakes* ou hypertrucages**
Images numériques et audio qui sont artificiellement modifiées ou manipulées par l'IA et/ou l'apprentissage profond pour faire apparaître une personne comme faisant ou disant quelque chose qu'elle n'a pas réellement fait ou dit. Les images ou les vidéos peuvent être modifiées pour mettre quelqu'un dans une position compromettante ou pour que quelqu'un fasse une déclaration controversée, même si la personne n'a pas réellement fait ou dit ce qui est montré. Il est de plus en plus difficile de distinguer le matériel fabriqué artificiellement des vidéos et images réelles.[218] Les deepfakes sont de plus en plus utilisés pour créer des images sexuelles sans consentement qui représentent la cible de manière sexuelle, par exemple en plaçant des visages de femmes sur des vidéos pornographiques.[219]

Diffamation
La diffamation implique la publication et la diffusion publique d'informations exagérées ou fausses qui portent atteinte à la réputation d'une personne et qui ont pour but d'humilier, de menacer, de discréditer, d'intimider ou de punir la victime et en particulier des personnalités publiques (par exemple, des fonctionnaires, des activistes et des journalistes).[220]

Discours de haine (genré ou sexiste)
Tout type de communication par la parole, l'écrit ou le comportement, qui attaque ou utilise un langage péjoratif ou discriminatoire à l'égard d'une personne ou d'un groupe sur la base de ce qu'ils sont, en l'occurrence, sur la base de leur sexe, de leur genre, de leur orientation sexuelle ou de leur identité de genre. Les discours de haine sexistes en ligne renforcent le sexisme systémique tout en déshumanisant et en encourageant la violence à l'égard des femmes et des filles, ainsi que des personnes LGBTQIA+.[221]

Documentation ou diffusion des agressions sexuelles (vidéos de viols)
Enregistrement et/ou diffusion d'images d'agressions sexuelles sur les réseaux sociaux, par texte ou sur des sites web. Il s'agit d'une forme supplémentaire de violence sexuelle à l'égard de la victime.[222] Ces vidéos peuvent être utilisées par la suite pour faire honte aux victimes ou les extorquer, ou sont vendues comme du porno sans consentement.[223]

Doxxing* ou *doxing
Forme sexuée de harcèlement en ligne qui consiste en une divulgation non consensuelle d'informations personnelles impliquant la diffusion publique d'informations privées, personnelles et sensibles d'une personne, telles que son adresse personnelle et électronique, ses numéros de téléphone, les coordonnées de son employeur et des membres de sa famille, ou des photos de ses enfants et de l'école qu'ils fréquentent, dans le but de la localiser et de lui causer un préjudice physique.[224]

E

Empoisonnement par hashtag
La création d'un hashtag abusif, ou le détournement d'un hashtag existant, qui est ensuite utilisé comme cri de ralliement pour des actions de cyberharcèlement en réseau.[225]

Expériences sexuelles non désirées facilitées par la technologie
Utilisation des technologies de la communication, telles que les téléphones portables, la messagerie électronique, les sites de réseaux sociaux, les espaces de discussion ou les sites et applications de rencontre en ligne, pour commettre ou occasionner une agression ou un abus sexuel.[226]

F

Fausses accusations de blasphème
Les femmes sont confrontées à des menaces en ligne dans le monde entier, mais elles courent un risque particulier dans les pays religieux conservateurs, où le blasphème est interdit par la loi et où les crimes d'honneur constituent une menace sérieuse. Accuser quelqu'un de blasphème peut devenir, en soi, un acte de violence.[227]

Flaming
Poster ou envoyer des messages choquants ou blessants sur l'Internet. Ces messages, appelés « flammes »(propos incendiaires), peuvent être publiés dans des forums de discussion ou des groupes de discussion en ligne, ou envoyés par courrier électronique ou par des programmes de messagerie instantanée. Les forums de discussion en ligne sont le lieu le plus fréquent où se produit les « flammes ».[228]

G

Grooming ou pédopiégeage (en ligne)
Type spécifique d'expérience sexuelle facilitée par la technologie par laquelle des enfants et des jeunes sont contactés par le biais de réseaux sociaux ou d'autres plateformes numériques dans le but de les agresser sexuellement.[229] Le grooming en ligne consiste à établir une relation abusive en ligne avec un enfant, afin de l'amener dans une situation d'abus sexuel ou de traite d'enfants.[230]

H

Harcèlement multiplateforme
Le harcèlement coordonné et délibérément déployé contre une cible, par un seul harceleur ou un groupe de harceleurs, à travers de multiples espaces en ligne, réseaux sociaux et plateformes de communication, en profitant du fait que la plupart des plateformes ne modèrent le contenu que sur leurs propres sites.[231]

Harcèlement (sexiste) en ligne
Le harcèlement sexiste en ligne est un comportement qui implique l'utilisation de la technologie pour contacter, ennuyer, menacer ou effrayer une autre personne de manière répétée par des commentaires verbaux et souvent des images importunes, offensantes, dégradantes ou insultantes. Il est commis par des individus isolés ou des groupes d'hommes, sur la base du sexe, de la sexualité ou de l'orientation sexuelle de la cible.[232]

L

Limitation ou contrôle de l'utilisation de la technologie
Les auteurs d'abus peuvent utiliser la technologie pour exercer un abus et un contrôle sur la victime, en suivant, surveillant ou limitant les mouvements, les communications et les activités de celle-ci. Ces comportements abusifs vont de l'obligation pour le partenaire de donner ses mots de passe et d'obtenir un accès non autorisé à ses comptes en ligne, à la limitation de son utilisation des appareils technologiques. Dans les relations intimes abusives, les menaces à la vie privée liées à l'utilisation des technologies peuvent être le précurseur d'autres formes d'abus[233]

M

Médias sexuels synthétiques
Manipulation d'images, donnant l'impression que des personnes se livrent à une activité sexuelle qu'elles n'ont pas pratiquée. Les médias sexuels synthétiques peuvent être produits à des fins de divertissement sexuel et de profit, pour harceler les femmes et leur causer volontairement du tort. Il peut s'agir d'utiliser un logiciel pour superposer le visage d'une personne sur une image sexuelle. Les *deepfakes* sont une forme de médias sociaux synthétiques.[234]

Menaces
Une menace est « une déclaration d'intention d'infliger une douleur, une blessure, un dommage ou toute autre action hostile » à une cible. Cela inclut les menaces de mort et les menaces de violence physique et/ou sexuelle.[235]

Mobbing* ou *dogpiling
Également appelé *cybermobbing* ou harcèlement en réseau, il s'agit d'attaques organisées, coordonnées et systématiques par un groupe de personnes contre des individus ou des sujets particuliers, comme par exemple les groupes qui ciblent les féministes ou les personnes qui publient en ligne des articles sur l'égalité raciale.[236] Les foules d'indignation ou de honte sont une forme de justice populaire visant à exposer, humilier et punir publiquement une cible, souvent pour avoir exprimé des opinions sur des sujets ou des idées politiquement chargés avec lesquels la foule d'indignation n'est pas d'accord et/ou qui ont été sortis de leur contexte afin de promouvoir un programme particulier.[237]

P

Piratage
Utilisation de la technologie pour obtenir un accès illégal ou non autorisé à des systèmes ou des ressources dans le but d'attaquer, de nuire ou d'incriminer une autre personne ou organisation en volant ses données, en acquérant des

informations personnelles, en altérant ou en modifiant des informations, en violant sa vie privée ou en infectant ses appareils avec des virus.[238]

Poursuite cyberobsessionnelle
Recherche non désirée d'intimité par une invasion répétée du sentiment d'intimité physique ou symbolique d'une personne, en utilisant des moyens numériques ou en ligne.[239]

R

Recrutement
Utilisation de la technologie pour attirer les victimes potentielles dans des situations violentes[240] ou pour faciliter les agressions physiques ou sexuelles en personne.[241] Les auteurs de ces abus et les trafiquants peuvent utiliser la technologie pour contacter des victimes potentielles par le biais de posts et d'annonces frauduleux sur des sites et des applications de rencontre, des « agences matrimoniales » ou publier de fausses offres d'emploi et d'études.[242]

Refus d'accès
Exploiter les « caractéristiques d'une technologie ou d'une plateforme pour nuire à la cible, généralement en empêchant l'accès à des outils ou plateformes numériques essentiels ». Il existe deux formes principales de refus d'accès à une plateforme technologique : (1) le signalement massif ou le faux signalement, qui consiste en une action coordonnée des auteurs d'abus pour signaler faussement le compte d'une cible comme étant abusif ou autrement nuisible afin d'essayer de le faire suspendre ou fermer et (2) le bombardement ou l'inondation de messages, qui consiste à « inonder » les comptes de téléphone ou de courrier électronique d'une personne ou d'une institution de messages indésirables destinés à limiter ou à bloquer la capacité de la cible à utiliser cette plateforme.[243]

Représailles contre les partisans des victimes
Menaces ou harcèlement à l'encontre des membres de la famille, des amis, des employeurs ou de la communauté de partisans d'une cible.[244]

S

***Sexting* et *sexting* abusif**
Le sexting est le partage électronique consensuel de photographies dénudées ou à caractère sexuel. Il est toutefois différent du partage sans consentement de ces mêmes images. Alors que le sexting est souvent diabolisé comme dangereux, le danger et l'infraction résident en fait dans la violation de la vie privée et du consentement qui accompagne le partage d'images du sujet sans son consentement. Par exemple, si les garçons et les filles sextent au même rythme, les garçons sont deux à trois fois plus susceptibles de partager les images qu'ils reçoivent.[245]

Sextorsion
Cela se produit lorsqu'un individu possède ou prétend posséder une image sexuelle d'une autre personne et l'utilise pour contraindre une personne à faire quelque chose qu'elle ne veut pas faire.[246]

***Slut-shaming* en ligne**
Une forme d'intimidation basée sur le genre qui vise souvent les adolescentes et les personnes LGBTQIA+, et qui consiste à les critiquer ou stigmatiser si elles ne se conforment pas aux attentes sociales en matière de comportement, d'apparence et de sexualité, souvent ancrées dans les normes de genre. Le *slut-shaming*, le *stalking*, l'utilisation de photographies sans consentement et la surveillance sexuelle se chevauchent fréquemment, amplifiant l'impact sur les cibles.[247]

Swatting
Lancer un appel canular aux forces de l'ordre en décrivant en détail un événement menaçant totalement faux qui se déroule au domicile ou dans l'entreprise de la cible, dans l'intention d'envoyer une unité de police entièrement armée (c'est-à-dire une équipe SWAT) à l'adresse de la cible. Les harceleurs signalent une menace ou une urgence sérieuse, suscitant une réponse des forces de l'ordre qui peut inclure l'utilisation d'armes et la possibilité d'être tué ou blessé. Le swatting est rare, mais extrêmement dangereux, et constitue un exemple clair de la manière dont le harcèlement en ligne peut causer des dommages dans la vie hors ligne[248]

T

***Trolling* de choc et de chagrin**

Cibler les victimes en utilisant les noms et les images des personnes disparues pour créer des mèmes, des sites web, de faux comptes Twitter ou des pages Facebook.[249]

***Trolling* de genre**

Abus ou harcèlement en ligne pour « s'amuser ». Les trolls publient délibérément des commentaires ou des messages, téléchargent des images ou des vidéos et créent des hashtags dans le but d'ennuyer, de provoquer ou d'inciter à la violence contre les femmes et les filles. Les trolls semblent apprécier que les gens s'offusquent de ce qu'ils publient et prennent souvent à la légère les plaintes concernant leur comportement, en prétendant qu'ils se sont amusés.[250] De nombreux trolls sont anonymes et utilisent de faux comptes.

U

***Upskirting*, *creepshots* et voyeurisme numérique**

Ces formes d'abus basé sur l'image (ABI) et de surveillance sexuelle consistent à prendre des photos ou des vidéos de victimes sans leur consentement, principalement des femmes et des filles, dans des lieux publics tels que des magasins, des toilettes publiques, des vestiaires, des salles de classe ou la rue, mais aussi dans leur propre appartement. Il peut s'agir de prendre des images sous la robe, la tenue vestimentaire ou la jupe d'une personne (*upskirting*)[251], de prendre une photo sexuellement suggestive d'une femme à son insu (*creepshot*)[252] ou de surveiller ou d'observer subrepticement à l'aide d'outils technologiques, et dans certains cas d'enregistrer, une autre personne dans ce qui serait généralement considéré comme un lieu privé (*voyeurisme numérique*).[253]

Usurpation d'identité

Processus consistant à voler l'identité d'une personne afin de la menacer ou de l'intimider, de la discréditer ou de porter atteinte à sa réputation.[254]

Z

Zoombombing

Cela se produit lorsque des personnes se joignent à des réunions ou à des rassemblements en ligne afin de publier des contenus racistes, sexistes, pornographiques ou antisémites pour choquer et perturber les spectateurs ; il s'agit d'une forme de harcèlement en réseau.[255]

Termes liés à la technologie

A

Algorithme
Un algorithme est une procédure ou une formule permettant de résoudre un problème, c'est-à-dire une série d'instructions indiquant à un ordinateur comment transformer un ensemble de données en informations utiles. Les algorithmes sont largement utilisés dans tous les domaines des technologies de l'information. Par exemple, tout programme informatique peut être considéré comme un algorithme élaboré.[256]

Application ou App
Logiciels, généralement destinés aux appareils mobiles, tels que les smartphones et les tablettes, dont le téléchargement et l'installation s'effectuent généralement au cours de la même étape sans que l'utilisateur ait à intervenir. Ils peuvent être supprimés sans affecter le fonctionnement de l'appareil.[257]

D

Drone
En termes technologiques, un drone est un aéronef sans pilote - c'est un robot volant qui peut être contrôlé à distance ou voler de façon autonome grâce à des plans de vol contrôlés par des logiciels dans leurs systèmes embarqués, travaillant en conjonction avec des capteurs et un GPS embarqués. Les drones sont plus officiellement connus sous le nom de véhicules aériens sans pilote (UAV) ou de systèmes d'aéronefs sans pilote (UAS). Les drones sont maintenant utilisés dans un large éventail de rôles civils, allant de la recherche et du sauvetage, de la surveillance, du contrôle du trafic, de la surveillance météorologique et de la lutte contre les incendies, aux drones personnels et à la photographie par drone d'affaires, en passant par la vidéographie, l'agriculture et même les services de livraison.[258]

E

Entreprises technologiques privées, ou entreprises technologiques[259]
Les entreprises technologiques privées englobent un large éventail d'organisations, dont les suivantes, sans s'y limiter :

- les fournisseurs de services Internet désignés. Ce sont des entités qui permettent aux utilisateurs finaux d'accéder à des documents en ligne, et les fournisseurs de services Internet, c'est-à-dire les entités qui fournissent des services de transport sur Internet, notamment Google, Safari et Internet Explorer ;
- les fournisseurs de services de réseaux sociaux. Ce sont des entités qui fournissent des services mettant en relation deux utilisateurs finaux par des moyens en ligne, y compris Facebook, LinkedIn et Instagram, entre autres ;
- les fournisseurs de services électroniques qui sont des entités qui permettent aux utilisateurs finaux de communiquer entre eux (par exemple, services de chat d'Outlook et de jeux) ;
- les fournisseurs de services de distribution d'applications qui sont des entités qui donnent accès à des services d'applications, notamment Google (par le biais du Google PlayStore) et Apple (par le biais de l'IOS App Store) ;
- les fournisseurs de services d'hébergement. Ce sont des entités qui permettent


1458
Options
Clear
SAMSUNG
OK

l'hébergement et le stockage de documents fournis sur des services de réseaux sociaux, des services électroniques pertinents ou des services Internet désignés, y compris Apple et Microsoft, entre autres, chacun par le biais de la fourniture de services en nuage (services cloud) ;

- les sociétés de développement de matériel qui sont des entités qui créent, développent et/ou entretiennent des équipements technologiques, des actifs physiques et d'autres articles tangibles ;
- les sociétés de développement de logiciels qui sont des entités qui créent, conçoivent, développent et entretiennent des programmes, des applications, des cadres ou d'autres composants de logiciels.

G

GPS et suivi GPS

Le suivi GPS est la surveillance de la localisation par l'utilisation du système de positionnement global ou mondial (GPS) pour suivre l'emplacement d'une entité ou d'un objet à distance. Cette technologie permet de déterminer la longitude, la latitude, la vitesse au sol et la direction de la cible.

Le GPS est une « constellation » de 24 satellites bien espacés qui tournent en orbite autour de la terre et permettent aux personnes disposant d'un récepteur au sol (ou d'un dispositif de localisation GPS) de déterminer avec précision leur position géographique. La précision de la localisation est de 10 à 100 mètres pour la plupart des équipements. Les équipements GPS sont désormais intégrés dans les smartphones, les tablettes et les appareils de navigation GPS. Les dispositifs GPS intégrés aux smartphones et autres appareils mobiles sont souvent utilisés pour localiser les employés, par exemple. Les défenseurs de la vie privée mettent en garde contre le fait que cette technologie peut également permettre aux annonceurs, aux pouvoirs publics, aux pirates informatiques et aux cyberharceleurs de suivre les utilisateurs à travers leurs appareils mobiles.[260]

I

Intelligence artificielle (IA)

L'intelligence artificielle est un domaine qui combine l'informatique et des ensembles de données robustes, pour permettre la résolution de problèmes. Elle englobe également les sous-domaines de l'apprentissage automatique et de l'apprentissage profond, qui sont fréquemment mentionnés en association avec l'intelligence artificielle. L'intelligence artificielle cherche à créer des systèmes experts qui font des prédictions ou des classifications sur la base de données d'entrée, et exploite les ordinateurs et les machines pour imiter les capacités de résolution de problèmes et de prise de décision de l'esprit humain.[261]

Logiciel espion

Un logiciel espion est un type de logiciel malveillant qui est installé sur un appareil informatique à l'insu de l'utilisateur final. Il envahit l'appareil, vole des informations sensibles et des données sur l'utilisation d'Internet, et les transmet à des annonceurs, des sociétés de données ou des utilisateurs externes. Une fois installé, il surveille l'activité Internet, suit les identifiants de connexion et espionne les informations sensibles.

Les logiciels espions peuvent également être utilisés pour localiser une personne, comme c'est le cas des **logiciels de harcèlement**. Les logiciels de harcèlement sont souvent installés secrètement sur les téléphones portables par les conjoints, les partenaires intimes, les ex-partenaires et même les parents ou les membres de la famille. Ce type de logiciel espion peut suivre l'emplacement physique de la victime, intercepter ses courriels et ses textes, écouter ses appels téléphoniques et enregistrer ses conversations, et accéder à ses données personnelles, comme ses photos et ses vidéos.[262]

P

Plateforme en ligne

Une plateforme en ligne est un service numérique qui facilite les interactions entre deux ou plusieurs ensembles distincts mais interdépendants d'utilisateurs (qu'il s'agisse d'entreprises

ou de particuliers) qui interagissent par le biais du service via Internet. Le terme « plateforme en ligne » a été utilisé pour décrire une gamme de services disponibles sur Internet, notamment les marchés en ligne, les moteurs de recherche, les réseaux sociaux, les points de vente de contenu créatif, les magasins d'applications, les services de communication, les systèmes de paiement, les services comprenant l'économie dite collaborative ou économie à la tâche, et bien plus encore.[263]

Plateforme numérique
Les plateformes numériques sont des entreprises en ligne qui facilitent les interactions commerciales et les échanges d'informations, de biens ou de services entre les producteurs et les consommateurs ainsi que la communauté qui interagit avec ladite plateforme. Les plateformes numériques peuvent être des plateformes de réseaux sociaux (Facebook, Twitter et LinkedIn), des plateformes de connaissances (Yahoo!Answers et Google Scholar), des plateformes de partage de médias (Spotify, YouTube et Netflix) ou des plateformes de services (Airbnb, Amazon et Uber).[264]

R

Réseaux sociaux
Les réseaux sociaux sont un terme collectif désignant les sites web et les applications axés sur la communication par Internet, l'apport communautaire, l'interaction, le partage de contenu et la collaboration. Les forums, le microblogging, le réseautage social, le *social bookmarking* (partage de signets et de favoris), la curation sociale et les wikis font partie des différents types de réseaux sociaux qui permettent la communication électronique rapide de contenu aux utilisateurs. Le contenu comprend des informations personnelles, des documents, des vidéos et des photos. Les utilisateurs s'engagent dans les réseaux sociaux par le biais d'un ordinateur, d'une tablette ou d'un smartphone via des logiciels ou des applications web. Les plateformes de réseaux sociaux les plus utilisées sont Facebook, YouTube, WhatsApp, Messenger, Instagram et TikTok[265]

T

Technologies de l'information et de la communication
Ensemble diversifié d'outils et de ressources technologiques utilisés pour transmettre, stocker, créer, partager ou échanger des informations. Ces outils et ressources technologiques comprennent les ordinateurs, l'Internet (sites web, blogs et courriels), les technologies de diffusion en direct (radio, télévision et webcasting), les technologies de diffusion enregistrées (podcasting, lecteurs et dispositifs de stockage audio et vidéo) et la téléphonie (par exemple fixe ou mobile, satellite et visioconférence).[266]

Technologies numériques
Les technologies numériques sont des outils, systèmes, dispositifs et ressources électroniques qui génèrent, stockent ou traitent des données. Elles comprennent l'infrastructure, les dispositifs, les médias, les services en ligne et les plateformes que nous utilisons pour nos besoins en matière de communication, d'information, de documentation, de mise en réseau/relations et d'identité.[267]

195 HCDH (2018). Rapport de la rapporteuse spéciale sur la violence à l'égard des femmes (voir note de bas de page 11).

196 Flynn, Powell et Hindes, Technology-facilitated abuse (voir note de bas de page 3).

197 Conseil des droits de l'homme des Nations unies. Rapport de la rapporteuse spéciale Dubravka Šimonović (18 juin 2018). Rapport de la Rapporteuse spéciale sur la violence à l'égard des femmes, ses causes et ses conséquences sur la violence en ligne à l'égard des femmes et des filles dans une perspective de droits humains. Doc ONU A/HRC/38/47.

198 https://eige.europa.eu/publications/cyber-violence-against-women-and-girls

199 L. Hinson, J. Mueller, L. O'Brien-Milne et N. Wandera (2018). *La violence sexiste facilitée par la technologie : Qu'est-ce que c'est, et comment la mesurer ?* (Washington D.C. : Centre international de recherche sur les femmes). Disponible sur : https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

200 https://violenciadigital.tedic.org/indexEng.html#violencia

201 Anastasia Powell, Adrian J. Scott et Nicola Henry, "Digital harassment and abuse : experiences of sexuality and gender minority adults", *European Journal of Criminology*, vol. 17, n° 2, (2018), pp. 199-223. https://journals.sagepub.com/doi/full/10.1177/1477370818788006

202 Association pour le progrès des communications (2017). La violence sexiste en ligne : Une soumission de l'Association for Progressive Communications à la rapporteuse spéciale des Nations unies sur la violence contre les femmes, ses causes et ses conséquences. Disponible sur : https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

203 J. Bailey, A. Flynn et N. Henry, "Prelims", in *The Emerald International Handbook of Technology Facilitated Violence and Abuse*, J. Bailey, A. Flynn et N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021) pp. i-xxiv. https://doi.org/10.1108/978-1-83982-848-520211059

204 Projet de discours du Women's Media Centre, WMC.

205 Flynn, Powell et Hindes, Technology-facilitated abuse (voir note de bas de page 3).
McGlynn, Rackley et Houghton, Beyond revenge porn (voir note de bas de page 9).

206 Penn America. Manuel de terrain sur le harcèlement en ligne. Disponible sur : https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

207 Projet de discours du Women's Media Centre, WMC.

208 Ibid.

209 Projet de discours du Women's Media Centre, WMC.

210 Commission eSafety Australie. Catfishing. Disponible sur : https://www.esafety.gov.au/young-people/catfishing

211 Flynn, Powell et Hindes, Technology-facilitated abuse (voir note de bas de page 3).

212 Centre des médias des femmes. Projet de discours du CFM : Abus en ligne 101. Disponible sur : https://womensmediacenter.com/speech-project/online-abuse-101

213 VAW Learning Network, Technology-related violence against women (voir note de bas de page n° 20).
Henry et Powell, Technology-facilitated sexual violence (voir note de bas de page 22).

214 Cyberbullying Research Centre. What is cyberbullying? Disponible sur : https://cyberbullying.org/what-is-cyberbullying : https://cyberbullying.org/what-is-cyberbullying

215 Van der Wilk, Cyber violence et discours de haine en ligne contre les femmes (voir note de bas de page 52).

216 Penn America, Manuel de terrain sur le harcèlement en ligne.

217 Projet de discours du Women's Media Centre, WMC.

218 John R. Allen et Darrell M. West (2020). Le glossaire Brookings de l'IA et des technologies émergentes. Disponible sur : https://www.brookings.edu/blog/techtank/2020/07/13/the-brookings-glossary-of-ai-and-emerging-technologies/

219 Flynn, Powell et Hindes, Technology-facilitated abuse (voir note de bas de page 3).

220 Douglas, Doxing: a conceptual analysis (voir note de bas de page 40).
Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

221 ONU, Stratégie et plan d'action des Nations unies sur le discours de haine (voir note de bas de page 58).

222 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (voir note de bas de page 100).

223 Projet de discours du Women's Media Centre, WMC.

224 MacAllister, The doxing dilemma (voir note de bas de page 38).
Douglas, Doxing: a conceptual analysis (voir note de bas de page 40).

225 Penn America, Manuel de terrain sur le harcèlement en ligne.

226 Henry, Flynn et Powell, Technology-facilitated domestic and sexual violence (voir note de bas de page 32).

227 Ibid.

228 https://techterms.com/definition/flaming

229 Craven, Brown et Gilchrist, Sexual grooming of children (voir note de bas de page 36).

230 Van der Wilk, Cyber violence et discours de haine en ligne contre les femmes (voir note de bas de page 52).

231 Penn America, Manuel de terrain sur le harcèlement en ligne.

232 VAW Learning Network, Technology-related violence against women (voir note de bas de page 20).
Henry et Powell, Technology-facilitated sexual violence (voir note de bas de page 22).
Flynn, Powell et Hindes, Technology-facilitated abuse (voir note de bas de page 3).

233 Levy et Schneier, Privacy threats in intimate relationships (voir note de bas de page 62).

234 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

235 Penn America, Manuel de terrain sur le harcèlement en ligne.

236 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (voir note de bas de page 100).

237 Penn America, Manuel de terrain sur le harcèlement en ligne.

238 Penn America, Manuel de terrain sur le harcèlement en ligne.
VAW Learning Network, Technology-related violence against women (voir note de bas de page 20).

239 Ibid.

240 VAW Learning Network, Technology-related violence against women (voir note de bas de page 20).

241 Fascendini et Fialová, Voices from digital spaces (voir note de bas de page 14).

242 APC, Comment la technologie est utilisée pour perpétrer des violences contre les femmes (voir note de bas de page 48).

243 Penn America, Manuel de terrain sur le harcèlement en ligne.

244 Projet de discours du Women's Media Centre, WMC.

245 Ibid.

246 Dunn, Technology-facilitated gender-based violence : an overview (voir note de bas de page 24).

247 Ibid.

248 Projet de discours du Women's Media Centre, WMC.
Penn America, Manuel de terrain sur le harcèlement en ligne.

249 Projet de discours du Women's Media Centre, WMC.

250 Commission eSafety Australie. Abus en ligne ciblant les femmes. Disponible sur : https://www.esafety.gov.au/women/online-abuse-targeting-women

251 Flynn, Powell et Hindes, Technology-facilitated abuse (voir note de bas de page 3).

252 Lexico. https://www.lexico.com/definition/creepshot

253 Clough,J (2015). Harcèlement, In *Principles of Cybercrime* (pp. 417 - 453). Cambridge : Cambridge University Press. doi:10.1017/CBO9781139540803.013.

254 Van der Wilk, Cyber violence et discours de haine en ligne contre les femmes (voir note de bas de page 52).

255 Dunn, Technology-facilitated gender-based violence: an overview (voir note de bas de page 24).

256 The Conversation (2020). Qu'est-ce qu'un algorithme ? Comment les ordinateurs savent quoi faire avec les données. Disponible à l'adresse : https://theconversation.com/what-is-an-algorithm-how-computers-know-what-to-do-with-data-146665

257 Techopedia (2012). App. Disponible sur : https://www.techopedia.com/definition/28104/app

258 Agenda IoT (2019). Drone (UAV). Disponible sur : https://internetofthingsagenda.techtarget.com/definition/drone

259 Loi sur la sécurité en ligne de 2021 (Cth). No. 76, 2021. (Austl.)

260 WhatIs.com (2014). Le suivi GPS. Disponible sur : https://whatis.techtarget.com/definition/GPS-tracking

261 IBM (2020). L'intelligence artificielle (IA). Disponible sur : https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

262 TechTarget (2021). Spyware. Disponible sur : https://searchsecurity.techtarget.com/definition/spyware

263 OCDE (2019). Une introduction aux plateformes en ligne et leur rôle dans la transformation numérique. Disponible sur : https://www.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en

264 Blogs BMC (2020). Digital Platforms: A Brief Introduction. Disponible sur : https://www.bmc.com/blogs/digital-platforms/#

265 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (voir note de bas de page 108).

266 Institut de statistique de l'UNESCO. Glossaire : Technologies de l'information et de la communication (TIC). Disponible sur : http://uis.unesco.org/en/glossary

267 GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (voir note de bas de page 100).

Rendre tous les espaces sûrs

Violence basée sur le genre facilitée par la technologie

United Nations Population Fund
605 Third Avenue, New York, NY 10158
1-212-297-5000 / www.unfpa.org / @UNFPA