2019

White paper series
**Édition 7**

# — LUTTE CONTRE LA VIOLENCE EN LIGNE —
# À L'ÉGARD DES FEMMES
## UN APPEL À LA PROTECTION

OEA
Plus de droits
pour plus de personnes

Canada

— LUTTE CONTRE LA VIOLENCE EN LIGNE —

# À L'ÉGARD DES FEMMES

## UN APPEL À LA PROTECTION

# CRÉDITS

**Luis Almagro**
**Secrétaire général**
de la Organisation des États Américains (OEA)

**Farah Diva Urrutia**
Secrétaire à la Sécurité Multidimensionnelle

**Alejandra Mora Mora**
Secrétaire Exécutive
Commission Interaméricaine des Femmes (CIM)

**Alison August Treppel**
Secrétaire Exécutive
Comité Interaméricain Contre le Terrorisme (CICTE)

**Betilde Muñoz-Pogossian**
Directrice du Département de l'inclusion Sociale

## Équipe technique

Belisario Contreras
Nathalia Foditsch
Kerry-Ann Barrett
Hilary Anderson
Pamela Molina
Claudia Gonzalez
Mariana Cardona
Miguel Angel Cañada
Rolando Ramirez
David Moreno

# CONTENU

— LUTTE CONTRE LA VIOLENCE EN LIGNE —

# À L'ÉGARD DES FEMMES

UN APPEL À LA PROTECTION

# Introduction

# 1

Alors que près de la moitié de la population mondiale est composée de femmes **(Banque mondiale, 2019)**, seules 48% d'entre elles ont accès à Internet (contre 58% d'hommes) **(UIT, 2019),**[1] et cette fracture numérique entre hommes et femmes s'aggrave lorsqu'une perspective transversale est adoptée, par exemple le sexe et la race, l'appartenance ethnique, le handicap et l'âge. Cette fracture a des conséquences importantes en termes d'autonomisation et de développement des femmes, ainsi que pour les sociétés, les entreprises et les économies. Outre les lacunes en matière d'accès, le manque d'alphabétisation numérique est également une réalité pour de nombreuses femmes.

Le concept d'alphabétisation numérique désigne à la fois les compétences techniques nécessaires et la capacité d'interagir de manière critique avec les contenus en ligne **(UNICEF, 2017)**. En outre, **GSMA (2015)** a constaté, par exemple, que de nombreuses femmes dans les pays en développement ne comprennent pas la profondeur et la portée de ce qu'Internet pourrait leur offrir en termes de contenu, car elles sont bloquées dans des "îlots d'application", ce qui signifie qu'elles connaissent Internet à travers un nombre limité d'applications mobiles. Avoir de bonnes connaissances en informatique est essentiel, d'autant plus que l'accès à Internet et son utilisation ont créé de nombreuses possibilités que nous n'aurions jamais imaginées. En effet, cela a profondément affecté la manière dont nous communiquons, dont nous accédons aux informations, dont nous comprenons nos propres identités.

En n'étant pas suffisamment alphabétisées, les femmes ne sont pas pleinement conscientes des risques liés à l'utilisation d'Internet. En effet, malgré le large éventail de possibilités qu'il offre, l'adoption et l'utilisation d'Internet ont également été accompagnées de défis tels que la nécessité de renforcer la protection de la vie privée et la sécurité, car nos vies sont de plus en plus visibles à travers nos identités en ligne. Les fuites de données sont un exemple de la façon dont les femmes peuvent être exposées en ligne sans le vouloir. En 2019, plus de 12 millions de dossiers médicaux hébergés par un organisme gouvernemental et relatifs à la santé reproductive des femmes ont été exposés en ligne en Inde. Le problème a été traité par l'équipe nationale d'intervention en cas d'urgence informatique (CERT) en coopération

[1] Bien que ces chiffres soient des estimations, la plupart des pays ne soumettent pas de données ventilées par sexe à l'Union internationale des télécommunications UIT (Web Foundation, 2018).

avec un chercheur étranger, mais il a fallu des semaines pour le régler **(Cimpanu, 2019)**. La divulgation des informations personnelles des femmes constitue en soi une violation de leur droit à la vie privée, mais cela les rend également plus vulnérables à différents types de violence et de harcèlement en ligne.

Nous n'avons pas encore une définition convenue des différents comportements pouvant être considérés comme de la "violence en ligne" contre les femmes, bien que l'on s'accorde généralement sur le fait que ce sont les comportements qui ciblent une femme en particulier. Cela peut arriver, par exemple, lorsqu'une femme reçoit un message direct via Internet ou ses informations sont diffusées sur Internet sans son consentement, ce qui peut entraîner des sentiments négatifs et traumatisants **(PRC, 2018)**. Compte tenu de l'importance actuelle du sujet et de la demande croissante d'un cadre juridique et réglementaire pour lutter plus efficacement contre la violence en ligne à l'égard des femmes, le présent Livre blanc vise à éclaircir la nécessité de lutter contre cette violence. Il explique brièvement comment les femmes peuvent être harcelées en ligne et décrit certains des principaux problèmes dans les sphères publique et privée. Il passe aussi brièvement en revue la façon dont ces questions ont été abordées dans les pays d'Amérique latine et des Caraïbes. Enfin, une boîte à outils fournit des mesures pratiques qui peuvent être suivies par les femmes qui souhaitent se protéger contre les risques d'exposition en ligne.

# Violence en ligne contre les femmes

# 2

La Convention interaméricaine de 1994 sur la prévention, la sanction et l'élimination de la violence à l'égard des femmes (Convention de Belém do Pará) définit la violence à l'égard des femmes comme "tout acte ou comportement, fondé sur le sexe, qui provoque la mort ou des atteintes physiques, sexuelles ou psychologiques à la femme, que ce soit dans la sphère publique ou privée" (article 1)[2] Lorsque la Convention a été rédigée et adoptée au début des années 90, la "sphère publique" n'incluait pas le monde en ligne. Cependant, la société a radicalement changé au cours des 25 dernières années et nos identités, activités et interactions en ligne occupent une place de plus en plus importante dans notre vie publique, en particulier pour les personnalités politiques, les journalistes et les autres personnes qui vivent la plus grande partie de leur vie dans la sphère publique. Notre activité en ligne a également contribué à brouiller la frontière entre les sphères publique et privée, dans la mesure où, pour certains, cette distinction n'est peut-être plus utile.

Le système interaméricain des droits de l'homme n'a pas encore une définition commune des comportements pouvant être considérés comme de la "violence en ligne" à l'égard des femmes dans le cadre des instruments juridiques existants tels que la Convention de Belém do Pará, et il est urgent de fixer ces normes afin de fournir une base conceptuelle et normative solide aux politiques publiques et aux autres mesures visant à lutter contre la violence en ligne à l'égard des femmes.

Concrètement, la violence en ligne se manifeste de différentes manières. Il "peut s'agir de menacer ou de harceler par des mails, des messages instantanés ou de publier des informations en ligne" **(PRC, 2018)** et "cibler une personne en particulier soit en la contactant directement, soit en diffusant ses informations personnelles et causer de la détresse, de la peur ou de la colère" **(PRC, 2018)**. Les termes équivalents utilisés sont "harcèlement en ligne" et "cyber harcèlement". Aux fins du présent document, nous avons inclus tout type de harcèlement ou d'abus sous le terme plus large de "violence en ligne à l'égard des femmes".

**Le Centre de recherche Pew (2017)** décrit six comportements différents qu'il qualifie de "harcèlement en ligne" : "injures" ; "embarras volontaire" ; "menaces physiques" ; "harcèlement incessant" ; "harcèlement sexuel" et "harcèlement criminel". **Citron (2014)** explique que le "cyber-harcèlement" "c'est les menaces de violence, les atteintes à la vie privée, les mensonges portant

[2] https://www.oas.org/en/mesecvi/convention.asp

atteinte à la réputation, les appels à faire du mal à des victimes et les attaques technologiques" (p.3). Les conséquences d'un tel harcèlement vont de la détresse mentale aux atteintes à la réputation, en passant par la crainte d'effets réels, et le problème est encore plus répandu chez les femmes **(Centre de recherche Pew, 2017 et INEGI, 2015).**

Les médias sociaux peuvent être utilisés comme un outil de harcèlement. Une étude menée par **Amnesty International (2019)** a révélé que les femmes sont plus susceptibles d'être harcelées et maltraitées sur Twitter, avec "des menaces directes ou indirectes de violence physique ou sexuelle, des abus discriminatoires visant un ou plusieurs aspects de l'identité d'une femme, du harcèlement ciblé, et des violations de la vie privée telles que le fait de doxer ou de partager des images sexuelles ou intimes d'une femme sans son consentement". Alors que les tribunaux essaient encore de comprendre les différences souvent subtiles entre la liberté d'expression/ protection de la parole et ce qui constitue une "menace réelle" **(Drake, 2015)**, de nombreuses femmes se sentent en danger en ligne et souffrent des violations de leurs droits fondamentaux à vivre sans violence, à l'intégrité physique, mentale et morale, et à la vie privée.

L'abus discriminatoire peut être pire lorsque la femme appartient à une population autochtone, est une personne handicapée ou appartient à toute autre identité intersectionnelle. En outre, compte tenu de la quantité d'informations et de données nous concernant disponibles en ligne, du temps que nous passons en ligne, ainsi que du fait que nous dépendons d'Internet pour différents types d'interactions sociales et professionnelles, le problème du harcèlement est de plus en plus répandu, ce qui augmente le besoin d'une réponse immédiate juridiquement solide et techniquement applicable.

## a. Quelles sont certaines des méthodes utilisées pour la violence en ligne ?

• **"Cyberintimidation"** – Le **Centre de recherche sur la cyberintimidation, citant Hinduja et Patchin (2014)**, définit ce phénomène comme "un préjudice volontaire et répété causé par l'utilisation d'ordinateurs, de téléphones portables et d'autres appareils électroniques", soulignant ainsi sa nature répétitive. **Ipsos (2018)** a constaté que la sensibilisation autour de la question a augmenté au cours des dernières années. Toutefois, les adolescentes sont plus susceptibles que les garçons de déclarer avoir été victimes de cyberintimidation **(Patchin, 2016)**. De plus, **Betts et. al (2017)** ont constaté un impact négatif sur la perception de la valeur de l'apprentissage chez les femmes victimes d'intimidation, ce qui n'est pas le cas chez les hommes. **Kwon et al. (2019)** ont également constaté qu'être victime de cyberintimidation est en corrélation avec un sommeil de mauvaise qualité, ce qui augmente les risques de dépression chez les adolescents.

• **"Cyberstalking"**-PrivacyRightsClearinghouse explique qu'un des types de harcèlement en ligne est le cyberharcèlement, qui "suppose l'utilisation de moyens électroniques pour traquer une victime et fait généralement référence à un ensemble de comportements menaçants ou malveillants" **(PRC, 2018)**. Il existe différentes définitions du terme et, dans certains cas, la menace doit être considérée comme crédible. Dans d'autres cas, une menace implicite entre dans cette catégorie **(PRC, 2018)**. Il est relativement facile de traquer une personne, étant donné que beaucoup ont plusieurs comptes de médias sociaux et une présence en ligne importante. En outre, de nombreuses personnes ne connaissent pas bien les fonctionnalités de confidentialité fournies par les plates-formes utilisées.

• **"Cyber mobs"** est un concept associé qui se produit lorsque des groupes en ligne publient des contenus offensants/destructeurs en ligne, souvent en concurrence avec d'autres groupes dans l'intention d'humilier quelqu'un **(Citron, 2014)**. Un exemple de la façon dont cela affecte les femmes est présenté par **Coding Rights et InternetLab (2017)**, dans lequel une artiste brésilienne de l'État de Bahia (nord-est du Brésil) occupait la première place d'un concours en ligne quand un cybermob a été organisé contre elle afin de voter en masse pour sa concurrente, et elle a fini par être deuxième au concours.

• **"Doxing/Doxxing"** – "Dox" vient de "documents" / ".doc" et doxing est "l'extraction non autorisée et la publication, souvent par piratage, des informations personnelles d'une personne, y compris, mais sans s'y limiter, les noms complets, les adresses, les numéros de téléphone, les mails, les noms des conjoints et des enfants, les informations financières" **(Women's Media Center, 2019)**. En 2017, Amnesty International a constaté qu'un quart des femmes avaient été victimes de doxing au moins une fois **(Amnesty International, 2017)**.

• **"Vol d'identité"** – survient lorsque les données personnelles d'une personne sont utilisées de façon trompeuse par une autre personne **(Women's Media Center, 2019)**. Par exemple, une femme russe a découvert que ses photos étaient utilisées par un autre compte Twitter devenu viral et qu'il a fallu un certain temps pour qu'elle retrouve son identité **(Kochetkova, 2016)**. Un tel vol d'identité pourrait avoir des conséquences à la fois réelles et psychologiques plus longues qu'on pourrait l'imaginer.

• **"Revanche pornographique" / "Pornographie non consensuelle"** – est "la distribution d'images sexuellement graphiques d'individus sans leur consentement" et cela comprend à la fois des images/vidéos acquises avec ou sans consentement **(Netizens, 2019).** De tels scénarios sont particulièrement préjudiciables aux femmes, étant donné que leur corps et leur sexualité sont soumis à des normes culturelles souvent misogynes. Un concept voisin est la "sextorsion", où de l'argent ou d'autres demandes sont exigés pour ne pas divulguer des images ou des vidéos au contenu sexuellement explicite. Si l'on considère que dans certains pays, plus de 80% des adultes ont envoyé des messages texte avec un certain type de contenu sexuellement explicite **(Stako et Geller, 2015)**, de nombreuses personnes sont exposées à ce type de violence en ligne.

## BOX # 1 Deepfakes
## Une nouvelle arme contre les femmes

*"Deepfakes"* c'est des vidéos qui utilisent des techniques d'apprentissage automatique afin de changer le visage d'une personne pour une autre **(Knight, 2019)**. Ces technologies ont vu le jour en 2017 **(Deeptrace, 2019)** et sont utilisées dans différents contextes, mais les plus habituels sont liés à la politique et à la pornographie. Le nombre de vidéos deepfake en ligne augmente de manière exponentielle, en partie à cause du fait qu'il est maintenant plus facile pour les non-experts d'utiliser certaines technologies **(Deeptrace, 2019)**. Le département américain de la Défense est même en train de développer des outils pour automatiser des outils médico-légaux dans le but de lutter contre les deepfakes **(Knight, 2019)**.

Selon **Deeptrace (2019)**, les femmes sont les principales cibles de l'utilisation de deepfakes dans la pornographie. Des cas d'utilisation de ces technologies pour attaquer les femmes en politique commencent également à apparaître. Un homme politique américain bien connu en est un exemple. En 2019, il est apparu dans une vidéo comme si elle était ivre ; la vidéo est rapidement devenue virale sur Facebook (**Rosenberg, 2019**). Cela est particulièrement troublant étant donné que les "deepfakes" devraient avoir un impact sérieux sur les prochaines élections dans le monde entier **(Parkin, 2019)**.

Alors que toutes les femmes risquent d'être harcelées en ligne, d'autres aspects de l'identité, tels que la race, l'ethnie, la langue, l'orientation sexuelle ou l'identité du genre, le statut de migrant et le handicap, entre autres, peuvent aggraver le problème. Les femmes qui appartiennent simultanément à différentes identités sont des cibles plus vulnérables de la violence en ligne. Comme l'explique le **Women's Media Center (2019)**, une femme homosexuelle peut être victime d'homophobie, tandis qu'une femme noire peut être la cible du racisme, dans les deux cas, tout en étant une cible du sexisme. Cela met en évidence l'importance d'examiner la violence en ligne à l'égard des femmes de façon intersectorielle.

Les femmes engagées dans la vie politique sont aussi fréquemment la cible de harceleurs en ligne. L'**Organisation des États américains (OEA)** a adopté une **déclaration sur le harcèlement politique et la violence à l'égard des femmes** en 2015, qui reconnaît "les facteurs structurels qui affectent la violence à l'égard des femmes et les normes socioculturelles et symboliques ainsi que les stéréotypes sociaux et culturels qui la perpétuent" **(OEA, 2015)**. Elle encourage les **réseaux sociaux**, entre autres parties prenantes, à adopter des mesures visant à éliminer la discrimination et les stéréotypes sexistes **(OEA, 2015)**. Ceci est particulièrement important compte tenu du fait que les débats politiques sont de plus en plus diffusés sur les plateformes des médias sociaux et que de nombreuses personnes obtiennent désormais leurs informations sur la politique principalement via ces plateformes.

Cet aperçu permet de conclure que les femmes sont ciblées en utilisant plusieurs méthodes et technologies. On trouvera ci-dessous une brève description de la manière dont certaines de ces questions sont traitées dans les pays d'Amérique latine et des Caraïbes.

# Comment ces problèmes sont-ils abordés dans les pays d'Amérique latine et des Caraïbes ?

3

Des progrès ont été constatés ces dernières années dans les pays d'Amérique latine et des Caraïbes dans la lutte contre la violence en ligne à l'égard des femmes. En ce qui concerne la législation contre la "revanche pornographique", par exemple, la loi 13.772/2018[3] a été promulguée au Brésil en décembre 2018, modifiant la législation précédente afin de criminaliser l'enregistrement et la diffusion non autorisés de contenus nus ou sexuels. Ces actes sont désormais considérés comme de la "violence domestique" au sens de la loi dans les cas où il y avait une relation préexistante entre la victime et l'auteur. Les médias ont joué un rôle crucial dans la promotion du débat sur la revanche pornographique après que des cas concrets se sont produits. Ces débats ont conduit à des modifications de la législation concernant directement la question (Neris et. al, 2018). L'Argentine, le Chili, le Mexique et l'Uruguay sont des exemples d'États membres de l'OEA qui discutent actuellement de projets de loi relatifs à la vengeance pornographique (Neris et. al, 2018). Le Mexique en particulier a proposé un amendement spécifique à son code pénal et à la loi générale sur l'accès des femmes à une vie sans violence[4] qui s'attaque au cyber-harcèlement à l'égard des femmes **(Cruz, 2019)**.

En outre, divers pays d'Amérique latine ont soit adopté une législation sur le harcèlement politique contre les femmes (Bolivie), soit sont en train d'examiner des projets de loi similaires (Costa Rica, Équateur, Honduras, Mexique et Pérou) **(OEA, 2017)**. Selon ce qui a été décrit ci-dessus, ceci est important, entre autres raisons, à cause de l'impact de la technologie sur les débats démocratiques.

En ce qui concerne la police spécialisée dans la cybercriminalité et/ou la violence en ligne contre les femmes, des progrès ont également été enregistrés ces dernières années. Le Mexique a une division de sa police qui se focalise exclusivement sur la cybercriminalité et s'occupe des cas de violence en ligne,[5] et un portail gouvernemental en ligne a des contenus spécialement destinés à la sensibilisation à la cyberintimidation[6]. Au Brésil, certains États ont des départements de police spécialisés, d'autres non.[7] Au Pérou, toute personne peut déposer une plainte pour violence en ligne via un formulaire en ligne, même si la personne qui enregistre la plainte n'est pas la victime.[8]

[3] https://www2.camara.leg.br/legin/fed/lei/2018/lei-13772-19-dezembro-2018-787488-publicacaooriginal-157031-pl.html

[4] Ley General de Acceso de las Mujeres a una Vida Libre de Violencia

[5] http://www.ssp.df.gob.mx/ciberdelincuencia.html

[6] https://www.gob.mx/ciberbullying

[7] https://new.safernet.org.br/content/delegacias-cibercrimes

[8] http://www.noalacosovirtual.pe/

Ce n'est pas une analyse exhaustive de ce qui se passe dans les pays d'Amérique latine et des Caraïbes. Il s'agit plutôt d'un bref aperçu destiné à démontrer la complexité de la question. Il est possible de noter que les pays s'orientent vers la reconnaissance et la définition du problème, ainsi que vers le renforcement de la protection des femmes en ligne. En même temps, de nouvelles méthodes et technologies apparaissent, et plusieurs formes de violence en ligne sont utilisées chaque jour.

Afin de contribuer à la protection des femmes en ligne, ce livre blanc se termine par une série de mesures pratiques que les femmes peuvent prendre, ainsi que des ressources utiles disponibles en ligne.

# Mesures pratiques pouvant être prises immédiatement

4

Commencer par les étapes pratiques décrites ci-dessous est une bonne idée si vous souhaitez vous protéger contre la violence en ligne. Vous trouverez également ci-dessous des contenus utiles en ligne que vous pouvez rechercher. Parmi ces contenus, vous trouverez des guides et des manuels qui vous aideront à mieux comprendre ce qu'est la violence en ligne contre les femmes et les mesures à prendre.

## |Mesures préventives :|

• **Utilisez des mots de passe forts et ne les partagez pas.** Assurez-vous d'avoir un mot de passe fort et gardez-le secret. De plus, ne répétez pas les mots de passe sur différents plates-formes et services. Pour plus d'informations, consultez **"Ce qu'il faut faire et ce qu'il ne faut pas faire avec les mots de passe"** (p. 11) OEA (2019).

• **Apprenez à comprendre et à modifier les paramètres de confidentialité des plates-formes de médias sociaux.** Une partie des informations exposées en ligne peut être contrôlée via les paramètres de confidentialité. Il est important de connaître les options en matière de protection de votre vie privée. Par exemple, il est important de garder les publications privées afin que les personnes qui sont hors de votre réseau n'aient pas accès au contenu que vous publiez et d'utiliser une authentification à deux facteurs pour vous connecter. Pour plus d'informations, consultez **"Vérifiez vos paramètres de confidentialité"** (p. 09) OEA (2019).

• **Utilisez des applications de messagerie chiffrées pour communiquer.** Les applications chiffrées sont une option plus sûre, car il est plus difficile pour une personne d'accéder aux contenus échangés en les utilisant. Bien que les messages texte normaux des téléphones portables ne soient pas chiffrés, les applications telles que *Signal*, *Telegram*, *WhatsApp* et *Wire* le sont.

• **Utilisez un réseau privé virtuel (VPN) pour chiffrer votre activité en ligne.** Cette mesure est importante, en particulier lorsque vous n'utilisez pas de réseau privé (quand vous accédez à Internet depuis un café ou un autre réseau sans fil public, par exemple). Les services VPN permettent de chiffrer votre trafic afin que les autres utilisateurs du réseau ne puissent pas voir ce que vous faites en ligne. Bien que la plupart des services VPN ne soient pas gratuits, ils sont un bon investissement. Pour plus d'informations, consultez **"Utilisation des services VPN"** (p. 13) OEA (2019).

**En cas de violence / harcèlement / menace / abus :**

• **Conservez les preuves de la violence / harcèlement / menace / abus.** N'effacez aucune preuve. Il est essentiel de conserver tous les messages que vous avez et toute autre forme de preuve, telle que des captures d'écran, pouvant être utilisée pour prouver la violence / le harcèlement / la menace / l'abus.

• **Signalez la violence à la plateforme/ au service en ligne.** Dans la plupart des cas, il est possible de signaler la violence à la plate-forme ou au service en ligne lui-même. Signalez ce qui s'est passé immédiatement. La plate-forme enquêtera pour déterminer si le contenu échangé enfreint les "normes communautaires" existantes et pourra ou non prendre des mesures pour supprimer le contenu et/ou restreindre les privilèges et l'activité de l'auteur. Bien que chaque plate-forme ait ses propres règles, vous pouvez chercher un exemple de la façon dont la suppression de contenu et d'autres aspects de l'application des règles sont abordés en consultant **"Application de nos règles" (p. 28) OEA (2019).**

• **Ne répondez à aucun message de menace ou de harcèlement.** Il est important de ne pas "nourrir" la personne qui commet la violence. Ne répondez à aucun message intimidant ou menaçant. Si possible, bloquez la personne afin que les messages ne puissent plus être reçus. Dans la plupart des cas, la personne que vous avez bloquée ne sera pas notifiée.

• **Contacter les autorités locales [cette mesure doit être prise avec prudence car seules les menaces graves doivent être signalées].** Outre les services de détection et de répression, il existe dans de nombreux pays des services de détection et de répression spécialisés, comme la police spécialisée dans la cybercriminalité. Faites appel à eux ou à toute autre autorité locale qui peut fournir de l'aide. Dans certains cas, il existe également des divisions de police spécialisées dans la violence à l'égard des femmes, ainsi que des formulaires en ligne pouvant être utilisés pour enregistrer les plaintes relatives à la violence en ligne.

• **Demandez l'aide de personnes de confiance et de professionnels de la santé mentale.** Etre victime de violence en ligne est troublant et peut affecter profondément la santé mentale et le bien-être d'une personne. Il est important de bénéficier du soutien externe de professionnels et de personnes de confiance autour de vous. Ils peuvent vous aider à prendre les mesures appropriées pour résoudre le problème.

• **Rechercher des ressources utiles en ligne.** Il existe des manuels, des boîtes à outils et un large éventail de documents en ligne qui peuvent être consultés. Certains de ces outils sont énumérés ci-dessous à la **section 5. "Contenu en ligne utile".** Consultez, en outre, "Éducation aux médias et à la sécurité numérique" **(OEA, 2019).**

# Contenu en ligne utile

5

## [Rapports, manuels et boîtes à outils]

• Littératie et Sécurité Numérique. Bonnes pratiques dans l'utilisation de Twitter. OEA 2019 https://www.oas.org/fr/ssm/cicte/docs/20190916FRA-Alfabetismo-y-seguridad-digital-Twitter.pdf

• Acoso Online. Pornografia no consentida. Cinco claves para denunciar y resistir su publicación. 2017. (Espagnol) Fundación Datos Protegidos; Equipo Latinoamérico de Justicia y Género (ELA); InternetLab; Hiperderecho; Acceso Libre; Ipandetec; Son Tus Datos; Fundación Datos Protegidos Bolivia; Non aux abus et au harcèlement en ligne (NOAH); Fundación Karisma; TEDIC. https://acoso.online/cl/

• Un premier regard sur la sécurité numérique. Consultez maintenant. 2018. (Anglais) https://www.accessnow.org/your-spring-welcoming-gift-is-here-the-freshest-version-of-a-first-look-at-digital-security/

• Boîte à outils pour la recherche sur l'accès et l'utilisation d'Internet par les femmes. A4AI; Fondation World Wide Web, GSMA et APC. 2018. (Anglais) https://webfoundation.org/research/a-toolkit-for-researching-womens-internet-access-and-use/

• Faire progresser les droits des femmes en ligne : Lacunes et opportunités dans la recherche et la défense des intérêts. Fondation du World Wide Web. 2018. (Anglais) https://webfoundation.org/research/advancing-womens-rights-online-gaps-and-opportunities-in-research-and-advocacy/

• Manuel de terrain sur le harcèlement en ligne. PEN America. 2019. (Anglais) https://onlineharassmentfieldmanual.pen.org/

• Manuels avec une perspective de genre. Technologie tactique. (Anglais et Espagnol) https://gendersec.tacticaltech.org/wiki/index.php/Manuals_with_a_gender_perspective

• Violencia Cibernetica. Lersy G. Boria Vizacarrondo. Procuradora de las Mujeres, Puerto Rico. (Espagnol) http://www.mujer.pr.gov/Educaci%C3%B3nPrevenci%C3%B3n/Opusculos/Violencia%20Cibernetica.pdf

• Guide de sécurité en ligne de Netizens. 2019. (Anglais) https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view

• Safernet. Divers contenus sur le cyber harcèlement (Portugais) https://new.safernet.org.br/

## |TEDTalks|

• Comment la violence faite aux femmes en ligne est devenue incontrôlable. Ashley Judd. TEDTalk. 2016 (Anglais). https://www.ted.com/talks/ashley_judd_how_online_abuse_of_women_has_spiraled_out_of_control/transcript?language=en

• Anita Sarkeesian à TEDxWomen 2012. Anita Sarkeesian. 2012. (Anglais) https://www.youtube.com/watch?v=GZAxwsg9J9Q

• Grooming, el acoso ¿virtual?. Sebastián Bortnik. TEDxRíodelaPlata. 2016. (Espagnol) https://www.youtube.com/watch?v=0wZjKOulodo

## |Documentaires|

• Netizens. Cynthia Lowen. 2019. (Anglais) https://www.netizensfilm.com/

# Références

6


Amnesty International. (2017). Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet. Extrait de https://www.amnesty.org/es/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Amnesty International. (2019). Why Twitter is a toxic place for women. Extrait de https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

Betts, L. R., Spenser, K. A., & Gardner, S. E. (2017). Adolescents' Involvement in Cyber Bullying and Perceptions of School: The Importance of Perceived Peer Acceptance for Female Adolescents. Sex Roles, *77*(7), 471–481. https://doi.org/10.1007/s11199-017-0742-2

Cimpanu, C. (n.d.). Indian govt agency left details of millions of pregnant women exposed online. ZDNet. Extrait de https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

Citron, D. K. (2014). Hate Crimes in Cyberspace. Harvard University Press.

Coding Rights, & InternetLab. (2017). Violências de gênero na Internet: Diagnóstico, soluções e desafios. Contribuição Conjunta Do Brasil Para A Relatora Especial Da ONU Sobre Violência Contra a Mulher. Extrait de https://www.academia.edu/35642655/Viol%C3%AAncias_de_g%C3%AAnero_na_Internet_diagn%C3%B3stico_solu%C3%A7%C3%B5es_e_desafios

Comparitech. (2019). Cyberbullying Statistics and Facts for 2016—2019. Extraído em 3 de novembro de 2019, do site da Comparitech: https://www.comparitech.com/internet-providers/cyberbullying-statistics/

Cruz, H. (2019). Proponen ley contra ciberacoso a la mujer. Extraído em 12 de novembro de 2019, from El Universal website: https://www.eluniversal.com.mx/metropoli/proponen-ley-contra-ciberacoso-la-mujer

Cyberbullying Research Center. (2014, December 23). What is Cyberbullying? Extraído em 3 de novembro de 2019, do site Cyberbullying Research Center: https://cyberbullying.org/what-is-cyberbullying

Deeptrace. (2019). The State of Deepfakes: Landscape, Threats and Impact. Extrait de https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf

Drake, B. (n.d.). The darkest side of online harassment: Menacing behavior. Extrait le 3 de novembro de 2019, do site Pew Research Center: https://www.pewresearch.org/fact-tank/2015/06/01/the-darkest-side-of-online-harassment-menacing-behavior/

EQUALS. (n.d.). 10 Lessons Learnt: Closing the Gender Gap in Internet Access and Use Insights from the EQUALS Access Coalition. Extrait de https://2b37021f-0f4a-4640-8352-0a3c1b7c2aab.filesusr.com/ugd/04bfff_33ded6f6855b4de5b7a09186e1c6add7.pdf

Franceschi-Bicchierai, L. (2017, 21 septembre). Ce ransomware exige des images nues au lieu de Bitcoin. Extrait le 5 novembre 2019 du site Web de Vice : https://www.vice.com/en_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin

GSMA. (2015). Accélérer l'alphabétisation numérique : Donner aux femmes les moyens d'utiliser l'internet mobile.

Hinduja, S., & Patchin, J. W. (2014). L'intimidation au-delà de la cour d'école : Prévenir et combattre la cyberintimidation (Deuxième édition). Thousand Oaks, Californie : Corwin.

INEGI. (2015). Módulo sobre Ciberacoso 2015 MOCIBA Documento metodológico. 20.

InternetLab. (2018). Como países enfrentam a disseminação não consentida de imagens íntimas? Extrait le 4 novembre 2019 du site Web de InternetLab : http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/

Ipsos. (2018). La sensibilisation sur la cyberintimidation augmente à l'échelle mondiale, bien qu'un ADULTE sur quatre n'en ait jamais entendu parler. Extrait de https://www.ipsos.com/en-us/news-polls/global-awareness-of-cyberbullying

UIT. (2019). Selon un rapport de l'UIT sur la connectivité numérique mondiale, le fossé numérique entre les sexes se creuse. Extrait de http://digitalinclusionnewslog.itu.int/2019/11/05/itu-report-on-global-digital-connectivity-finds-gender-digital-gap-is-growing/

Judd, A. (2015). Oubliez votre équipe : vous pouvez lécher mon cul avec votre violence en ligne envers les filles et les femmes. Mic. Extrait de https://www.mic.com/articles/113226/forget-your-team-your-online-violence-toward-girls-and-women-is-what-can-kiss-my-ass

Knight, W. (2018). Le département de la Défense a mis au point les premiers outils permettant de lutter contre les deepfakes. MIT Technology Review. Extrait de https://www.technologyreview.com/s/611726/the-defense-department-has-produced-the-first-tools-for-catching-deepfakes/

Kochetkova, K. (n.d.). Um caso assustador de roubo de identidade no Twitter. Extrait le 12 octobre 2019 de https://www.kaspersky.com.br/blog/stolen-social-identity/5949/

Kwon, M., Seo, Y. S., Dickerson, S. S., Park, E., & Livingston, J. A. (2019). 0802 Cyber Victimization and Depressive Symptoms: A Mediation Model Involving Sleep Quality. Sleep, 42(Supplement_1), A322–A322. https://doi.org/10.1093/sleep/zsz067.800

Neris, N., Ruiz, J., & Valente, M. (2018). Enfrentando Disseminação Não Consentida de Imagens Íntimas: Uma análise comparada. Extrait du site Web de InternetLab : http://www.internetlab.org.br/wp-content/uploads/2018/05/Neris_Ruiz_e_Valente_Enfrentando1.pdf

Netizens. (2019). Guide de sécurité en ligne de Netizens. Extrait de https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view?usp=embed_facebook

OEA. (2015). Déclaration sur le harcèlement politique et la violence à l'égard des femmes. Extrait de http://www.oas.org/en/cim/docs/DeclaracionViolenciaPolitica-EN.pdf

OEA. (2017). Fiche descriptive—Violencia y acoso político contra las mujeres en el marco de la Convención de Belém do Pará. Extrait de https://www.oas.org/en/cim/docs/ViolenciaPolitica-FactSheet-ES.pdf

OEA. (2019). Éducation aux médias et sécurité numérique : Meilleures pratiques Twitter. Extrait de https://www.oas.org/en/sms/cicte/docs/20190913-DIGITAL-ENG-Alfabetismo-y-seguridad-digital-Twitter.pdf

Parkin, S. (2019). La montée du deepfake et la menace pour la démocratie. The Guardian. Extrait de https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy

Patchin, J. W. (2016). Données de 2016 sur la cyberintimidation. Extrait le 3 novembre 2019 du site Web du Centre de recherche sur la cyberintimidation : https://cyberbullying.org/2016-cyberbullying-data

Centre de recherche Pew. (2017). Harcèlement en ligne 2017. Extrait le 12 novembre 2019 de https://www.pewinternet.org/wp-content/uploads/sites/9/2017/07/PI_2017.07.11_Online-Harassment_FINAL.pdf

PPRC. (2018). Harcèlement en ligne et cyber-harcèlement. Extrait le 5 novembre 2019 du site Web de Privacy Rights Clearinghouse : https://privacyrights.org/consumer-guides/online-harassment-cyberstalking

Rosenberg, A. (2019). La défense scandaleuse de la vidéo “Pelosi ivre” par la direction de Facebook n’a pas de sens. Extrait de https://mashable.com/article/facebook-monika-bickert-drunk-pelosi-video/?europe=true

Stasko, E. C., & Geller, P. A. (2015). Considérer le sexting comme un comportement relationnel positif : (528002015-001) [Ensemble de données]. https://doi.org/10.1037/e528002015-001

Unicef. (2017). Accès à Internet et à l’alphabétisation numérique. Extrait le 12 novembre 2019 de https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_ACCESS.pdf

Fondation Web. (2018a). Faire progresser les droits des femmes en ligne : Lacunes et opportunités dans la recherche et la défense des intérêts. Extrait de http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf

Fondation Web. (2018b). Mesurer la fracture numérique : Pourquoi nous devrions utiliser une analyse centrée sur les femmes. Extrait de https://webfoundation.org/2018/05/measuring-the-digital-divide-why-we-should-be-using-a-women-centered-analysis/

Women’s Media Center. (2019). Abus en ligne 101—Women’s Media Center. Extrait le 3 novembre 2019 de http://www.womensmediacenter.com/speech-project/online-abuse-101

Banque mondiale. (2019). Population, femmes (% de la population totale) | Données. Extrait le 12 octobre 2019 de https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS

OEA | Plus de droits pour plus de personnes

Canada

# LUTTE CONTRE LA VIOLENCE EN LIGNE À L'ÉGARD DES FEMMES

## UN APPEL À LA PROTECTION

White paper series

**Édition 7**

**2019**