Welens

PRATIQUES ÉDUCATIVES À TRAVERS L'ANGLE DU GENRE

BOITE À OUTILS
EXPLOITATION SEXUELLE ET VIOLENCE DE GENRE

MODULE 4

Technologies numériques et violences basées sur le genre

Cofinancé par l'Union européenne

Numéro du projet 2023-1-FR01-KA220-ADU-000165625

Table des matières

Table des matières 2

GLOSSAIRE 1

1. Introduction : Technologies numériques et violences basées sur le genre, leviers d'émancipation et outils d'oppression 10

1.1 Les TIC comme outils d'*empowerment* 10

1.2 Les TIC comme mécanismes de contrôle et d'abus 11

1.3 L'empreinte numérique : une cartographie de la vulnérabilité 12

2. Types de violences basées sur le genre en ligne 14

2.1 L'impact des réseaux sociaux 16

2.2 La double nature de l'anonymat 17

3. Synergies intersectorielles et étatiques pour lutter contre la violence basée sur le genre 20

3.1 Les cadres de l'Union européenne 21

3.2 Cadres Nationaux 23

FRANCE 23

ITALIE 25

GRÈCE 27

ESTONIE 28

GUYANA 30

4. Exploitation numérique liée à la prostitution et à la traite transfrontalière des êtres humains 34

4.1. Les défis de la coopération internationale 34

4.2. L'intégration avec les migrations 35

4.3 Sensibiliser les communautés à la sécurité numérique 45

4.4 L'impact du secteur privé 53

5. Conclusions 55

6. Bibliographie 58

GLOSSAIRE

Terme	Définition
Discrimination Algorithmique	Phénomène par lequel des systèmes automatisés de prise de décision produisent des résultats biaisés ou injustes, désavantageant des personnes ou des groupes en fonction d'attributs tels que la race, le genre, l'âge ou le statut socioéconomique. Ces biais résultent souvent de données de référence faussées, d'une conception défectueuse des modèles ou des inégalités structurelles reflétées dans les données d'entrée. Il s'agit d'un enjeu crucial dans les débats éthiques et de gouvernance liés à l'intelligence artificielle.
Technologies de l'information et de la communication (TIC)	Outils et plateformes utilisés pour transmettre, stocker et accéder à l'information, incluant les téléphones portables, les services Internet et les applications numériques.
Violence basée sur le genre (VBG)	Actes nuisibles dirigés contre des personnes en raison de leur genre. Inclut des violences physiques, sexuelles, psychologiques et économiques, touchant souvent les femmes et les filles.
Violence basée sur le genre facilitée par la technologie (VBGFT)	Toute forme de VBG amplifiée, rendue possible ou commise au moyen de technologies numériques telles que les réseaux sociaux, les applications mobiles ou les forums en ligne.
Trolling	Publication de commentaires provocateurs ou dénigrants dans le but de provoquer, de perturber ou de blesser les personnes visées.

Trafic d'êtres humains	Exploitation de personnes par la force, la supercherie ou la contrainte à des fins de travail, d'exploitation sexuelle ou pour d'autres motifs. De plus en plus facilitée par les plateformes numériques.
Exploitation en ligne	Abus ou manipulation de personnes par le biais des technologies numériques. Inclut l'exploitation sexuelle, le chantage, la manipulation psychologique ou prédation sexuelle (*grooming*) et le trafic.
Harcèlement en ligne	Terme générique désignant tout comportement non désiré, agressif ou menaçant dirigé contre une personne ou un groupe via des plateformes numériques. Cela inclut les messages persistants, les insultes, les menaces, le harcèlement sexuel et les attaques coordonnées. Le harcèlement en ligne est souvent genré, les femmes et les filles étant particulièrement victimes d'abus visant leur identité et leur apparence.
Empreinte Numérique	« Traces » de données laissées par les personnes lorsqu'elles utilisent des appareils numériques ou des plateformes en ligne. Comprend à la fois les comptes-rendus d'activités actifs et passifs.
Empreinte Numérique Active	Données générées intentionnellement par les utilisateur·rice·s, telles que les publications, les likes, les messages et les téléchargements sur des sites web ou des réseaux sociaux.
Empreinte Numérique Passive	Données collectées sans l'intervention directe de l'utilisateur·rice, incluant la géolocalisation, les cookies, les métadonnées et les habitudes de navigation.

Cyberharcèlement	Surveillance ou harcèlement persistant et non désiré d'une personne via des moyens numériques, provoquant souvent de la peur et une détresse émotionnelle.
Cyberintimidation	Harcèlement ou humiliation ciblé·e et répété·e par le biais de plateformes numériques.
Dogpiling (cyberharcèlement collectif)	Harcèlement en ligne coordonné ou spontané, mené par un groupe ciblant une personne, souvent déclenché par une simple publication, opinion ou identité. Ces attaques impliquent généralement des centaines, voire des milliers d'internautes envoyant des menaces, des insultes et des messages déshumanisants sur plusieurs plateformes, submergeant la personne visée et aggravant les dommages émotionnels et les atteintes à la réputation. Les personnes prenant publiquement position sont fréquemment la cible de ces cyberattaques collectives.
Catfishing (Usurpation d'identité en ligne)	Création d'une fausse identité sur Internet dans le but de tromper autrui, souvent à des fins de manipulation romantique, d'exploitation ou d'abus financier. Cela peut entraîner des préjudices émotionnels, du chantage ou des stratégies de manipulation (*grooming*).
Doxxing	Publication en ligne, sans consentement, d'informations personnelles ou identifiantes sur une personne, souvent dans une intention malveillante.
Pornographie *Deepfake*	Contenu sexuel manipulé numériquement représentant faussement une personne, généralement créé à l'aide de l'intelligence artificielle pour imiter son apparence.

Servitude pour dettes	Un système de travail forcé dans lequel une personne s'engage à offrir ses services, ou ceux d'une personne sous son autorité, comme garantie d'une dette, ce qui mène souvent à l'exploitation lorsque les conditions de remboursement sont trafiquées ou impossibles à remplir. Les personnes concernées se retrouvent fréquemment piégées dans des cycles de pauvreté et de servitude qui se perpétuent sur plusieurs générations.
Culture Numérique	La capacité à interagir de manière critique et sécurisée avec les technologies numériques, incluant la compréhension des paramètres de confidentialité, la reconnaissance des menaces en ligne et l'utilisation responsable des plateformes.
Désinformation	La création et la diffusion intentionnelles d'informations fausses ou trompeuses dans le but de duper, de manipuler les perceptions ou de servir un objectif stratégique.
Conception axée sur les survivant·es	Une approche de conception technologique qui accorde la priorité à la sécurité, à l'autonomie et aux besoins des personnes ayant vécu des violences ou de l'exploitation.
Intersectionnalité	Un cadre qui reconnaît comment les différents aspects de l'identité (comme le genre, l'origine, la classe sociale ou le statut migratoire) s'entrecroisent pour façonner les expériences de discriminations et de privilèges.
CEDEF (Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes)	Un traité des Nations Unies adopté en 1979, qui engage les États à éliminer les discriminations envers les femmes sous toutes ses formes, y compris la

	violence numérique, comme précisé dans la Recommandation Générale n° 35.
Convention d'Istanbul	Un traité du Conseil de l'Europe visant à prévenir et à combattre les violences faites aux femmes et les violences domestiques, en reconnaissant notamment le harcèlement en ligne et la violence psychologique.
Violence basée sur l'image	Partage d'images ou de vidéos intimes sans consentement (par exemple, la « pornodivulgation » aussi appelée *revenge porn*, ou encore la pornographie non consensuelle).
Incels (Célibataires Involontaires)	Sous-cultures en ligne d'hommes qui estiment être privés d'accès sexuel aux femmes et qui expriment du ressentiment, de la haine ou de la violence envers les femmes ainsi qu'envers toute personne sexuellement active.
Désinformation (non intentionnelle)	Informations fausses ou inexactes diffusées que ce soit dans le but de tromper intentionnellement ou non.
Convention de Budapest	Le premier traité international sur la cybercriminalité, qui établit des normes juridiques pour lutter contre les crimes impliquant les systèmes d'information et les réseaux.
VBGFT (Violences basées sur le genre facilitées par la technologie)	Violences commises, rendues possibles ou aggravées via des outils ou plateformes numériques, incluant le cyberharcèlement, la sextorsion, la violence basée sur l'image et le *grooming* en ligne (manipulation).
Règlement sur les Services Numériques (*Digital Services Act* /DSA)	Une règlementation de l'Union européenne (2022/2065) qui impose aux plateformes en ligne des obligations pour retirer les contenus illégaux, protéger

	les utilisateur·rice·s et renforcer la transparence des services numériques.
Inclusion Numérique	Pratique visant à garantir que toutes les personnes et communautés, en particulier celles marginalisées ou défavorisées, aient accès aux technologies numériques et la capacité de les utiliser. Cela inclut non seulement la connectivité, mais aussi la culture numérique, l'accessibilité financière et la disponibilité de services et contenus inclusifs.
Règlement général sur la protection des données (RGPD)	Une loi de l'Union européenne qui régit la protection des données et la vie privée des personnes, incluant des mesures contre l'utilisation abusive des données personnelles sur les plateformes numériques.
Géolocalisation / *Geo Tagging*	Processus consistant à associer des données de localisation géographique, telles que des coordonnées de latitude et de longitude, à des contenus multimédias comme des photos, des vidéos, des sites web ou des messages.
Désinformation genrée	Une forme de désinformation qui vise des personnes, en particulier des femmes et des minorités de genre, à travers des récits, des stéréotypes et du harcèlement fondés sur le genre. Elle combine des informations fausses ou trompeuses avec du sexisme, de la misogynie et des clichés genrés afin de saper la crédibilité, de réduire au silence certaines voix et de renforcer des normes discriminatoires.
Safeline	Le mécanisme officiel grec de signalement et la ligne d'assistance pour les contenus illégaux en ligne, en particulier ceux incluant de la maltraitance des enfants, de la pornographie non consensuelle et de la pédopornographie.

Sextorsion	Type de chantage impliquant des menaces de diffusion d'informations, de photos ou de vidéos à caractère sexuel si certaines exigences ne sont pas satisfaites.
Commission hellénique des télécommunications et de la poste (HTPC)	Autorité de régulation grecque chargée de surveiller la conformité des plateformes numériques dans le cadre du Règlement sur les services numériques (Digital Services Act).
Piratage et prises de contrôle de comptes (usurpation d'identité en ligne, vol d'identité)	Accès non autorisé aux comptes en ligne d'une personne (réseaux sociaux, courriels, stockage en ligne) dans le but de voler des informations personnelles, d'usurper l'identité de la victime ou de nuire à sa réputation. Dans les cas de violences basées sur le genre, le piratage est souvent utilisé pour divulguer des contenus intimes, surveiller les communications ou bloquer l'accès aux plateformes personnelles comme forme de punition ou de contrôle.
Discours haineux et mèmes misogynes	Diffusion de contenus sexistes, violents ou discriminatoires.
Blocage Dynamique	Mécanisme juridique permettant aux autorités grecques de restreindre l'accès à des sites web hébergeant des contenus illégaux ou piratés, en particulier dans le secteur du divertissement pour adultes.
Abus par *Deepfake*	Utiliser l'IA pour créer de fausses vidéos ou images, souvent à caractère sexuel, représentant une personne sans son consentement. Cette forme de violence basée sur l'image peut gravement nuire à la réputation et à la santé mentale.

Partage/diffusion non consenti d'images intimes	Également connu sous le nom de « *Revenge Porn* », cela consiste à diffuser du contenu sexuellement explicite sans le consentement de la personne concernée, ce qui est criminalisé par la législation grecque.
Grooming (prédation et manipulation)	Établir une relation de confiance avec des mineur·e·s ou des personnes vulnérables en ligne dans le but de les exploiter ou de les abuser sexuellement. Les abuseur·euse·s utilisent souvent la flatterie, l'attention ou des cadeaux pour manipuler leurs victimes.
Droit à l'oubli	Principe du droit à la protection des données permettant à une personne de demander la suppression de données personnelles lorsqu'elles ne sont plus nécessaires, inexactes ou ont été traitées de manière illégale.

INTRODUCTION

1. Introduction : Technologies numériques et violences basées sur le genre, leviers d'émancipation et outils d'oppression

L'essor des technologies numériques a profondément transformé les manières dont les individu·e·s interagissent, accèdent à l'information et se mobilisent pour le changement social. Mais cette transformation ne va pas sans complexité, en particulier pour les femmes et les filles qui évoluent dans la sphère numérique. Les technologies numériques, également appelées Technologies de l'Information et de la Communication (TIC), possèdent un potentiel considérable pour donner du pouvoir d'agir aux survivant·e·s de violences basées sur le genre (VBG), en facilitant l'accès à des réseaux de soutien, à une protection juridique et à des formes de résistance collective. Pourtant, ces mêmes outils peuvent être, et sont de plus en plus, détournés pour perpétrer des abus, faciliter la traite des êtres humains et renforcer les déséquilibres de pouvoir.

Ce chapitre vise à analyser le double rôle des TIC, à la fois comme instruments de lutte contre les violences basées sur le genre et l'exploitation, mais aussi comme vecteurs de ces mêmes violences. Il interroge également la notion d'empreinte numérique, en montrant comment les traces laissées en ligne par les femmes peuvent être utilisées pour leur sécurité ou, au contraire, comme outils de contrôle. Pour ce faire, le texte s'appuie sur des recherches internationales, des études de cas et les évolutions des politiques afin d'offrir une compréhension approfondie de la manière dont les écosystèmes numériques façonnent à la fois la vulnérabilité et la résilience.

1.1 Les TIC comme outils d'*empowerment*

Dans leurs usages les plus positifs, les technologies de l'information et de la communication (TIC) offrent des possibilités transformatrices pour lutter contre les violences basées sur le genre (VBG). Les survivant·e·s ont désormais accès à des lignes d'assistance numériques, à des services de messagerie en cas de crise, ainsi qu'à des applications mobiles permettant une communication discrète avec les structures de soutien. Ces outils permettent de contourner des obstacles tels que l'isolement géographique, la stigmatisation sociale ou la peur de représailles, en particulier dans les contextes où l'accès à des services physiques peut être dangereux, voire impossible.

Les plateformes de médias sociaux jouent également un rôle de plus en plus important dans la mobilisation collective. Des mouvements comme #MeToo, #SayHerName ou #NiUnaMenos montrent comment les espaces numériques sont devenus des lieux de prise de parole, de solidarité et d'action. Ces campagnes ne se contentent pas de sensibiliser : elles influencent aussi les réformes politiques et les changements culturels. Dans les régions

où les institutions traditionnelles négligent ou ignorent les préoccupations des femmes en matière de sécurité, les TIC deviennent une porte d'entrée vers la visibilité et la justice.

Les initiatives d'inclusion numérique renforcent encore ces effets. Par exemple, les femmes vivant dans des zones reculées ou mal desservies peuvent accéder à un soutien juridique à distance, à un accompagnement psychosocial et à des programmes d'apprentissage en ligne qui combattent l'isolement historiquement utilisé pour les réduire au silence ou les paralyser. Les plateformes interactives permettent aussi aux survivant·e·s de documenter leurs expériences, de suivre les incidents d'abus ou de violences et de se connecter anonymement à des communautés d'entraide. Les recherches confirment qu'une meilleure maîtrise du numérique est associée à une plus grande propension à chercher de l'aide et à de meilleurs résultats en matière de sécurité.

1.2 Les TIC comme mécanismes de contrôle et d'abus

Malgré les promesses du progrès technologique, les espaces numériques sont également devenus un terrain fertile à la misogynie et à l'exploitation. **La violence basée sur le genre facilitée par la technologie (VBGFT)** englobe un ensemble de pratiques abusives : cyberharcèlement, harcèlement en ligne, partage non consenti d'images intimes (« *revenge porn* »), usurpation d'identité et menaces de violences physiques. Ces violations sont amplifiées par leur ampleur et leur permanence - les contenus diffusés en ligne peuvent atteindre instantanément des milliers de personnes et rester accessibles indéfiniment. **Internet est éternel** ; une fois partagé, un contenu nuisible peut être copié, archivé ou retéléchargé, rendant presque impossible pour les victimes de l'effacer complètement.

De plus, les auteur·rice·s de ces violences utilisent de plus en plus des outils de chiffrement, la navigation anonyme et le *dark web* pour échapper à toute responsabilité. Dans les cas de traite des êtres humains, les plateformes numériques servent à recruter, préparer et contrôler les victimes sans contact physique. Les trafiquant·e·s promeuvent leurs services sur les réseaux sociaux, utilisent les données de géolocalisation pour suivre les déplacements et exploitent les applications de rencontre pour attirer les femmes dans de fausses relations afin de les exploiter.

Le coût psychologique des VBGFT ne doit pas être sous-estimé. Les victimes rapportent souvent des sentiments d'hypervigilance, de honte et d'impuissance, aggravés par la difficulté à faire supprimer les contenus nuisibles ou à en identifier les auteur·rice·s. Les forces de l'ordre manquent fréquemment des compétences numériques ou de l'autorité juridictionnelle nécessaire pour intervenir, laissant les survivant·e·s dans un état d'exposition permanente. Cette exposition constante peut entraîner une retraumatisation, puisque les

survivant·e·s sont contraint·e·s de revivre le préjudice initial à chaque fois que le contenu abusif réapparaît en ligne.

1.3 L'empreinte numérique : une cartographie de la vulnérabilité

Au cœur de la compréhension de l'exploitation en ligne se trouve le concept d'empreinte numérique : la trace de données générée par les interactions d'une personne avec les plateformes numériques. Cela inclut les empreintes actives telles que les publications sur les réseaux sociaux, les achats en ligne et les messages, ainsi que les empreintes passives, comme les métadonnées, la localisation, les cookies et l'historique de navigation.

Si les empreintes numériques peuvent aider à recueillir des preuves médico-légales contre les auteur·ice·s de ces crimes, elles présentent aussi des risques importants. Pour les femmes fuyant des relations abusives ou des environnements coercitifs, leur présence numérique peut être exploitée pour les localiser et les harceler. Les photos géolocalisées, les algorithmes prédictifs et la collecte de données inter-plateformes font que les survivant·e·s sont vulnérables non seulement aux auteur·ice·s connu·e·s, mais aussi au marketing ciblé, à la surveillance et même à la discrimination algorithmique.

Les jeunes femmes et filles font face à des défis particuliers. Les études montrent que les adolescentes ont généralement moins de contrôle sur les paramètres numériques, sont plus susceptibles d'emprunter des appareils et manquent souvent d'un accès à une éducation numérique complète. De plus, les filles issues de milieux marginalisés (comme les migrant·e·s, les jeunes LGBTQ+ ou les personnes vivant dans la pauvreté) sont confrontées à des risques amplifiés en raison de l'exclusion systémique et d'un faible contrôle sur l'outil numérique.

TYPES DE VIOLENCES BASÉES SUR LE GENRE EN LIGNE

2. Types de violences basées sur le genre en ligne

La violence basée sur le genre facilitée par la technologie (VBGFT), ou **violence sexiste en ligne**, est une forme de violence systémique qui utilise les technologies numériques pour cibler, réduire au silence et contrôler des personnes en raison de leur genre. Elle touche de manière disproportionnée les femmes et les filles, renforçant les déséquilibres de pouvoir et perpétuant les discriminations déjà présentes hors ligne. La violence sexiste en ligne n'est ni accidentelle, ni isolée : elle s'inscrit dans un continuum plus large de violences qui traverse les espaces physiques et virtuels. Ses impacts sont bien réels, durables, et souvent dévastateurs. Les formes les plus courantes incluent :

- **Harcèlement en ligne :** Terme générique désignant tout comportement non désiré, agressif ou menaçant dirigé contre une personne ou un groupe via des plateformes numériques. Cela inclut les messages persistants, les insultes, les menaces, le harcèlement sexuel et les attaques coordonnées. Le harcèlement en ligne est souvent genré, les femmes et les filles étant particulièrement victimes d'abus visant leur identité et leur apparence.

- **Cyberintimidation :** Harcèlement ou humiliation ciblé·e et répété·e par le biais de plateformes numériques.

- **Cyberharcèlement :** Surveillance ou contacts persistants et non souhaités, souvent via des applications de géolocalisation ou les réseaux sociaux.

- ***Trolling* :** Publication de commentaires provocateurs ou dénigrants dans le but de provoquer, de perturber ou de blesser les personnes visées.

- ***Dogpiling* (cyberharcèlement collectif) :** Harcèlement en ligne coordonné ou spontané, mené par un groupe ciblant une personne, souvent déclenché par une simple publication, opinion ou identité. Ces attaques impliquent généralement des centaines, voire des milliers d'internautes envoyant des menaces, des insultes et des messages déshumanisants sur plusieurs plateformes, submergeant la personne visée et aggravant les atteintes émotionnelles et à la réputation. Les personnes prenant publiquement position sont fréquemment la cible de ces cyberattaques collectives.

- **Piratage et prises de contrôle de comptes (usurpation d'identité en ligne, vol d'identité) :** Accès non autorisé aux comptes en ligne d'une personne (réseaux sociaux, courriels, stockage en ligne) dans le but de voler des informations personnelles, d'usurper l'identité de la victime ou de nuire à sa réputation. Dans les cas de violences basées sur le genre, le piratage est souvent utilisé pour divulguer

des contenus intimes, surveiller les communications ou bloquer l'accès aux plateformes personnelles comme forme de punition ou de contrôle.

- ***Doxxing*** **:** Publication en ligne, sans consentement, d'informations personnelles ou identifiantes sur une personne, souvent dans une intention malveillante (harcèlement ou menaces).

- **Abus par *Deepfake* :** Utiliser l'IA pour créer de fausses vidéos ou images, souvent à caractère sexuel, représentant une personne sans son consentement. Cette forme de violence basée sur l'image peut gravement nuire à la réputation et à la santé mentale.

- **Violence basée sur l'image :** Partage d'images ou de vidéos intimes sans consentement (par exemple, la « pornodivulgation » ou *revenge porn*, ou encore la pornographie non consensuelle).

- **Sextorsion :** Chantage impliquant des menaces de diffusion d'informations, de photos ou de vidéos à caractère sexuel si certaines exigences ne sont pas satisfaites.

- ***Catfishing*** **(Usurpation d'identité en ligne*)* :** Création d'une fausse identité sur Internet dans le but de tromper autrui, souvent à des fins de manipulation romantique, d'exploitation ou d'abus financier. Cela peut entraîner des préjudices émotionnels, du chantage ou des stratégies de manipulation (*grooming*).

- ***Grooming*** **(prédation et manipulation) :** Établir une relation de confiance avec des mineur·e·s ou des personnes vulnérables en ligne dans le but de les exploiter ou de les abuser sexuellement. Les abuseur·euse·s utilisent souvent la flatterie, l'attention ou des cadeaux pour manipuler leurs victimes.

- **Discours haineux et mèmes misogynes :** Diffusion de contenus sexistes, violents ou discriminatoires.

Ces formes de violences peuvent se chevaucher et ont souvent des conséquences graves sur le plan psychologique, social, et même économique pour les personnes qui en sont victimes.

Quelle est la différence entre un·e harceleur·euse et une personne haineuse (*hater*) en ligne ?

Un·e **harceleur·euse** cible généralement une personne spécifique de manière répétée, cherchant souvent à la dominer, l'intimider ou l'humilier sur la durée.

Une **personne haineuse** (« *hater* »), en revanche, peut publier des commentaires nuisibles, hostiles ou toxiques sans focalisation continue sur une personne en particulier, souvent motivée par des préjugés ou la culture du *trolling* plutôt que par une vendetta personnelle. Bien que les deux soient nuisibles, le harcèlement tend à être plus persistant et personnel.

2.1 L'impact des réseaux sociaux

Les espaces numériques sont désormais un lieu de vie publique. Les plateformes de réseaux sociaux sont devenues centrales dans la manière dont les personnes se connectent, s'expriment et accèdent à l'information. Cependant, elles ont aussi créé de nouveaux environnements où la violence basée sur le genre peut se produire, souvent avec une portée étendue et un impact dévastateur. La violence basée sur le genre en ligne n'est pas seulement le reflet des inégalités hors ligne, elle est aussi un mécanisme qui les renforce par le biais de la technologie.

- **Amplification des violences**

Les réseaux sociaux peuvent amplifier rapidement le harcèlement, les menaces et l'humiliation. Un seul commentaire abusif peut être repartagé, liké ou suivi par d'autres, transformant une attaque personnelle en un événement viral.

- **Anonymat et absence de responsabilité**

Si l'anonymat peut protéger les utilisateur·rice·s vulnérables, il permet aussi aux auteur·rice·s de harcèlement d'agir avec peu ou pas de crainte de conséquences. Les faux profils et les systèmes de modération faibles contribuent à une culture où les menaces et les violences sont rarement traitées de manière efficace.

- **Normalisation des contenus violents**

Les blagues sexistes, la culture du viol et les mèmes misogynes circulent souvent largement et ne sont pas pris en compte puisque considérés comme étant « juste de l'humour » ou relevant de la « liberté d'expression ». Cela banalise la violence, renforce les stéréotypes de genre et décourage les survivant·e·s de prendre la parole.

    - **Communautés *incel*** : Des sous-cultures en ligne comme les *incels* (célibataires involontaires) sont un moteur clé des contenus misogynes et des discours haineux genrés. Les forums incels et certains espaces sur les réseaux sociaux normalisent l'hostilité envers les femmes, véhiculent des stéréotypes toxiques et peuvent même aller jusqu'à glorifier les violences sexuelles.

- **Surveillance et contrôle**

Les réseaux sociaux peuvent être utilisés pour surveiller, traquer ou contrôler le comportement d'une personne, en particulier dans des relations abusives et/ou violentes. Des fonctionnalités comme la géolocalisation, la possibilité de savoir si un message a été « vu » ou l'identification sur des photos peuvent être détournées pour intimider et suivre à la trace.

- **Réduction au silence, autocensure et peur de s'exprimer**

Face au harcèlement constant, de nombreuses femmes et personnes marginalisées limitent ce qu'elles partagent, quittent les plateformes ou évitent de participer aux débats publics. D'autres choisissent de ne pas parler du tout de leurs expériences de violences sexistes facilitées par la technologie, par crainte d'être harcelé·e·s, humilié·e·s, blâmé·e·s ou de ne pas être cru·e·s. Cela conduit à réduire au silence des voix et des perspectives essentielles, et renforce l'idée que les espaces en ligne ne sont pas sûrs pour les femmes.

- **Propagation de la désinformation et de la mésinformation genrée**

Les réseaux sociaux sont un outil puissant pour diffuser de fausses informations, y compris des stéréotypes sexistes nuisibles ou des campagnes de désinformation ciblant spécifiquement des femmes activistes, journalistes ou responsables politiques, dans le but de nuire à leur crédibilité et à leur sécurité.

2.2 La double nature de l'anonymat

L'anonymat joue un rôle complexe et souvent controversé dans le contexte de la violence basée sur le genre en ligne. Ses effets peuvent aussi bien être favorables aux auteur·rice·s de violences que protéger les personnes vulnérables, selon les perspectives et les contextes.

Comment l'anonymat est favorable aux auteur·rice·s de violences

- Responsabilité réduite : La possibilité de dissimuler son identité en ligne peut encourager certaines personnes à adopter des comportements abusifs, tels que le harcèlement, les menaces ou la traque, sans craindre de conséquences dans la vie réelle.

- Escalade des violences : L'anonymat peut favoriser des formes de violences plus agressives ou persistantes, car les auteur·rice·s se sentent protégé·e·s contre l'identification et les sanctions.

- Difficultés d'application de la loi : Les forces de l'ordre et les modérateur·rice·s des plateformes rencontrent souvent des difficultés à identifier et poursuivre les

responsables lorsque leur identité est dissimulée, ce qui complique la mise en place de sanctions.

Comment l'anonymat protège les victimes

- Sécurité pour les survivant·e·s : Pour les victimes et survivant·e·s de VBG, l'anonymat peut être essentiel pour chercher du soutien, partager leurs expériences ou participer à des actions de plaidoyer, sans craindre de représailles ou de nouvelles violences.

- Vie privée pour les groupes vulnérables : Les femmes, les activistes et les personnes vivant dans des contextes oppressifs peuvent dépendre d'identités anonymes pour s'exprimer en sécurité et accéder à des ressources.

- *Empowerment* : L'anonymat permet à certain·e·s utilisateur·rice·s de participer à des espaces en ligne qu'iels éviteraient autrement, par crainte d'être pris·es pour cible ou de subir des discriminations.

SYNERGIES INTERSECTORIELLES ET ÉTATIQUES POUR LUTTER CONTRE LA VIOLENCE BASÉE SUR LE GENRE

3. Synergies intersectorielles et étatiques pour lutter contre la violence basée sur le genre

La violence basée sur le genre (VBG) n'est pas seulement un traumatisme personnel ou isolé : c'est une crise mondiale profondément enracinée et continue, qui résonne à travers chaque couche de la société et affecte chacune d'entre elles. Qu'il s'agisse de la pression exercée sur les systèmes de santé, des répercussions sur les systèmes éducatifs ou du coût pour la croissance économique, la VBG n'épargne aucun secteur. C'est d'autant plus vrai lorsque ses formes en ligne s'immiscent dans la vie des femmes, quel que soit l'endroit où elles vivent, à travers les pays et les continents. Ainsi, lutter contre la VBG en ligne nécessite bien plus que des efforts isolés au niveau national ; cela exige une collaboration sincère et durable entre gouvernements, communautés et institutions, fondée sur une responsabilité partagée et une confiance mutuelle.

La plupart des États reconnaissent aujourd'hui la VBG comme une violation des droits humains. Des instruments juridiques tels que la Convention d'Istanbul et la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (CEDAW) ont poussé les gouvernements à adopter des lois et des stratégies au niveau national. Mais disposer d'un cadre légal ne suffit pas. C'est au moment de la mise en œuvre que de nombreux pays échouent. Certains manquent encore d'approches centrées sur les survivant·e·s ou n'allouent pas les financements adéquats. D'autres disposent de lois sur le papier (souvent pour se conformer à des cadres ou initiatives internationaux ou régionaux), mais sans mécanismes d'application suffisants.

La collaboration intersectorielle est essentielle, car aucun secteur ne peut, à lui seul, répondre efficacement à la VBG en ligne. Les services de santé, les forces de l'ordre, l'éducation et les aides et actions sociales doivent travailler ensemble, de manière complémentaire, pour obtenir des résultats concrets. Par exemple, les hôpitaux doivent disposer de protocoles pour identifier les violences et orienter les survivant·e·s ; la police doit être formée pour traiter les cas avec sensibilité et réactivité ; les établissements scolaires devraient enseigner dès le plus jeune âge le consentement et le respect. Lorsque ces secteurs agissent de manière isolée, les survivant·e·s passent entre les mailles du filet. C'est pourquoi des systèmes d'orientation intégrés et des programmes de formation conjoints peuvent avoir un impact réel en comblant ces lacunes.

La coopération internationale est de plus en plus cruciale, car la violence en ligne ne connaît pas de limites et ne se borne pas aux frontières d'un seul pays. La traite, les violences en ligne et les migrations forcées présentent toutes des dimensions transfrontalières. C'est là qu'intervient la coopération internationale : les agences des Nations Unies, les alliances régionales et les ONG jouent un rôle clé dans le partage de données, le financement de

programmes et la responsabilisation des États. Les Objectifs de développement durable (notamment l'ODD 5) ont contribué à aligner les efforts à l'échelle mondiale, mais davantage doit être fait pour que les engagements se traduisent en actions concrètes.

Il est clair que la lutte contre la VBG en ligne est complexe. Il ne s'agit pas seulement de sanctionner les auteur·rice·s après les faits, il s'agit aussi de transformer les systèmes en profondeur. Pour cela, les États doivent aller au-delà des discours. Les secteurs doivent cesser d'agir de manière isolée, et les acteur·rice·s internationaux·ales doivent continuer à exiger des redditions de comptes.

3.1 Les cadres de l'Union européenne

Il existe, à l'échelle de l'Union européenne, des lois et des mécanismes pertinents pour protéger les utilisateur·rice·s - en particulier les femmes et les mineur·e·s - sur les plateformes en ligne, y compris les sites pornographiques, ainsi que des procédures pour signaler des contenus ou en demander le retrait.

Conformément aux lois européennes sur les plateformes en ligne et les sites pornographiques, il existe le règlement sur les services numériques (Digital Services Act - DSA), pleinement applicable depuis le 17 février 2024, et qui concerne toutes les plateformes. Les très grandes plateformes en ligne (VLOPs), telles que Pornhub, Stripchat et XVideos, doivent :

- Procéder à des évaluations des risques, non seulement en ce qui concerne les contenus potentiellement illégaux, mais aussi spécifiquement en matière de VBG et de protection de l'enfance en ligne.
- Mettre en place des systèmes de vérification de l'âge afin de bloquer l'accès des mineur·e·s aux sites contenant du contenu pornographique.
- Supprimer immédiatement les contenus signalés comme illégaux ou non consensuels.
- Faire preuve de transparence et de responsabilité en se soumettant à des audits indépendants.
- Être en permanence soumis à un examen concernant les biais et les préjudices causés.

Le non-respect de l'une ou l'autre des obligations mentionnées ci-dessus peut entraîner des amendes allant jusqu'à 6 % du chiffre d'affaires annuel mondial, voire des interdictions d'accès à l'échelle de l'Union européenne.

De plus, pour protéger les femmes en ligne, la directive sur la cyberviolence de 2024, dont la mise en œuvre est prévue d'ici 2027, inclut la pénalisation des « *revenge porn* », du cyberharcèlement, du harcèlement sexuel en ligne et des *deepfakes* non consensuels. Dans ce cadre, les sites web doivent également supprimer les images intimes ou manipulées publiées en ligne sans consentement. Grâce à une directive applicable dans toute l'Union européenne, les victimes auront accès à la justice et à des services de soutien dans l'ensemble de l'UE.

Le signalement de contenus nuisibles ou illégaux en ligne peut se faire de différentes manières :

- Directement auprès des plateformes concernées, en utilisant leurs outils conformes au DSA,

- Par l'intermédiaire de groupes de la société civile explicitement désignés par l'UE pour faire remonter les cas les plus graves,

- Auprès des coordinateur·rice·s nationaux·ales des services numériques (DSC), qui sont des organismes créés dans chaque État membre de l'UE pour surveiller la conformité des sites web au DSA,

- Pour les cas plus complexes ou sensibles, les plaintes peuvent être déposées directement via le portail de la stratégie numérique de l'UE.

Ainsi, la manière de signaler un crime en ligne étape par étape peut être représentée visuellement comme suit :

ÉTAPE 1 : Identification du Contenu

↓

Décrire le contenu nuisible ou illégal et son emplacement (URL)

↓

ÉTAPE 2 : Explication de l'Infraction

↓

Décrire en quoi le contenu enfreint le DSA ou le RGPD (Règlement Général sur la Protection des Données).

↓

ÉTAPE 3 : Informations Détaillées

↓

Indiquer votre lien avec le contenu et toute preuve justificative.

↓

ÉTAPE 4 : Demande de Retrait

↓

Demander le retrait immédiat du contenu ainsi qu'une réponse rapide.

3.2 Cadres Nationaux

FRANCE

La France a mis en place un cadre juridique complet pour protéger les mineur·e·s contre l'exposition à des contenus pornographiques ou nuisibles en ligne. Le pays combine droit pénal, régulation numérique et mécanismes d'application stricts pour garantir le respect des règles, notamment à la suite de l'entrée en vigueur récente du règlement européen sur les services numériques (DSA).

Cadre juridique et politique

- Le **Code pénal (article 227-24)** interdit de rendre accessible aux mineur·e·s des contenus à caractère pornographique. La loi s'applique à la diffusion physique comme en ligne. Les opérateurs non conformes s'exposent à une peine pouvant aller **jusqu'à 3 ans d'emprisonnement et 75 000 € d'amende**.

- La **loi n° 2024-449** (SREN - Loi visant à sécuriser et réguler l'espace numérique), promulguée en **mai 2024**, oblige les sites diffusant du contenu pornographique à mettre en place des **systèmes solides de vérification de l'âge**. Cette loi s'applique à tous les sites accessibles depuis la France, y compris ceux hébergés à l'étranger.

- L'**ARCOM** (Autorité de régulation de la communication audiovisuelle et numérique), l'autorité nationale de régulation, a été habilitée à surveiller et faire appliquer ces obligations. Elle peut émettre des mises en demeure, imposer des amendes, demander des audits ou ordonner des restrictions d'accès voire le blocage de sites non conformes.

Mesures d'application et de vérification de l'âge

- En **octobre 2024**, l'ARCOM a publié ses **lignes directrices techniques** pour une vérification de l'âge conforme :
    - Utilisation de **systèmes de double anonymat**, garantissant l'absence de lien entre l'identité de l'utilisateur·rice et son activité de navigation.
    - **Vérification par un tiers indépendant**, distinct de la plateforme elle-même.
    - **Aucune conservation de données personnelles** ou d'identifiants.

- Un **mécanisme transitoire** utilisant la vérification par carte bancaire temporaire a été autorisé jusqu'au début de l'année 2025. Les sites doivent désormais passer à une conformité totale en utilisant des systèmes de vérification anonymes certifiés.

- **Début 2025**, l'ARCOM a publié une liste de **17 sites pour adultes** (dont Pornhub, RedTube et d'autres) soumis à une obligation de conformité. À la mi-2025, **plusieurs sites ont été bloqués ou déréférencés** pour ne pas avoir mis en place les contrôles requis, conformément à une décision de justice.

- Les amendes prévues par la loi SREN peuvent atteindre 150 000 € ou jusqu'à 2 % du chiffre d'affaires mondial annuel, avec des sanctions renforcées en cas de récidive.

Comment signaler un contenu illégal ou demander son retrait

Situation	Platdformd/Autorité	Description
Contenu illégal (par exemple : matériel pédopornographique, *grooming*, contenus terroristes)	**PHAROS**	Plateforme nationale de signalement des contenus illicites, opérée par le ministère de l'Intérieur. Les signalements anonymes sont acceptés. www.internet-signalement.gouv.fr
Cyberharcèlement, *revenge porn*, exposition non souhaitée à des contenus pour adultes, sextorsion	**3018 (Association e-Enfance)**	Ligne d'assistance dédiée aux mineur·e·s et aux parents. Signalement accéléré vers des plateformes comme TikTok, YouTube ou Instagram. Gratuit, confidentiel, accessible par téléphone, SMS, chat ou application. www.3018.fr
Exposition de données personnelles, droit à l'oubli	**CNIL** (Commission nationale de l'informatique et des libertés)	Gère les demandes liées au RGPD pour l'effacement des données ou leur suppression des moteurs de recherche. www.cnil.fr

Depuis la fin de l'année 2024, **e-Enfance a été officiellement désignée comme « signaleur de confiance » par l'ARCOM**, ce qui signifie que les principales plateformes donnent la priorité aux signalements émis via le 3018.
Le cadre juridique et institutionnel de la France accorde une priorité forte à **la protection des mineur·e·s contre la pornographie en ligne et les violences numériques**. Les nouvelles lois (SREN) imposent des obligations de vérification de l'âge et donnent à l'ARCOM les moyens de les faire respecter. Le droit pénal (article 227-24) sanctionne l'exposition des mineur·e·s à ce type de contenus. Les systèmes de signalement, tels que **PHAROS** (pour les contenus illégaux) et **3018** (pour l'accompagnement et le retrait rapide), offrent des voies de protection efficaces pour les utilisateur·rice·s. La France combine **ainsi législation stricte, mise en œuvre effective et mécanismes de signalement accessibles**, en conformité avec ses obligations européennes dans le cadre du **règlement sur les services numériques** (DSA).

ITALIE

En Italie, des réglementations spécifiques encadrent la protection des données personnelles et établissent des mesures de sécurité obligatoires à adopter. L'une des

principales réglementations dans ce domaine est le Règlement général sur la protection des données (RGPD), entré en vigueur en 2018. Ce règlement définit une série de principes et d'obligations auxquels les organismes doivent se conformer afin de garantir la protection des données personnelles. Parmi les mesures de sécurité obligatoires prévues par le RGPD figure l'adoption de mesures techniques et organisationnelles appropriées afin d'assurer un niveau de sécurité adapté aux risques. Ces mesures peuvent inclure l'utilisation du chiffrement des données, la mise en œuvre de procédures de sauvegarde ou encore le contrôle d'accès aux données. En complément du RGPD, l'Italie dispose également d'autres réglementations encadrant la protection des données personnelles. Par exemple, le Code de protection des données personnelles (décret législatif nº 196/2003) établit les mesures de sécurité que les organismes doivent adopter pour protéger les données personnelles. Parmi celles-ci figure l'obligation de mettre en œuvre des mesures techniques et organisationnelles adaptées pour garantir la sécurité des données personnelles et prévenir leur perte, leur destruction ou tout accès non autorisé (Diritto.net, 2023b).

En ce qui concerne la pornographie, en Italie, le visionnage de vidéos pornographiques sur Internet en streaming, est légal, tout comme leur téléchargement. Toutefois, dans le cas du téléchargement, il faut s'assurer que le contenu soit libre de droits - c'est-à-dire non protégé par des droits d'auteur - sans quoi l'on s'expose à une sanction différente liée à la violation de ces droits. La pornographie impliquant des mineur·e·s constitue cependant une situation distincte. Dans ce cas, bien que le simple visionnage de telles vidéos sur Internet ne soit pas puni par la loi, la possession ou la diffusion de ce type de matériel l'est (La Legge Per Tutti, 2015). Le Code pénal italien, à l'article 600-bis, définit la pornographie infantile comme la production, la possession, la diffusion et le transfert de matériel pornographique impliquant des mineur·e·s de moins de 18 ans. Cette infraction est considérée comme particulièrement grave et fait l'objet de poursuites actives de la part des autorités. Afin de lutter efficacement contre la pédopornographie et les crimes en ligne visant les mineur·e·s, plusieurs mesures législatives ont été adoptées. Parmi celles-ci, la loi nº 38/2006 a introduit l'infraction de *grooming* (prédation et manipulation) d'un·e mineur·e via Internet, en sanctionnant toute personne qui entre en contact avec un·e mineur·e dans l'intention de commettre des crimes à caractère sexuel (Diritto.net, 2023a). De plus, en 2022, l'accès intentionnel à des sites contenant du matériel pédopornographique a été défini comme une composante criminelle, punie d'une amende d'au moins 1000 euros et pouvant entraîner une peine de réclusion allant jusqu'à 2 ans (Agenda Digitale, 2022).

Pour **signaler** un site illégal en Italie, la plainte doit, en dernier recours, être déposée en personne auprès de la cyberpolice ou d'un autre service des forces de l'ordre. Cependant, il est possible de commencer la procédure en ligne, en remplissant un formulaire avec ses informations personnelles et les détails de l'infraction sur le site de la police d'État. Après l'envoi, un accusé de réception électronique ainsi qu'un numéro de protocole sont fournis,

permettant de suivre la plainte lors de la présentation physique. Cette étape en ligne ne remplace pas la plainte officielle, mais sert d'ébauche préparatoire. La déclaration ne prend de valeur légale qu'une fois signée physiquement devant un·e agent·e de police. Ainsi, le formulaire en ligne permet de préparer et d'organiser soigneusement le signalement, mais la plainte officielle doit obligatoirement être finalisée en personne.

GRÈCE

En Grèce, il existe plusieurs moyens de signaler du contenu et/ou de demander de l'aide, comme indiqué ci-dessous :

- **Contenus illégaux ou nuisibles (ex. : abus sur mineur·e·s, *grooming*, discours haineux)** :
    - Faire un signalement via SafeLine.gr
    - Contacter la division de la cybercriminalité via la ligne téléphonique **11188** ou par email

- ***Revenge porn* ou contenu explicite non consensuel** :
    - Déposer une plainte auprès de la police

- **Protection des mineur·e·s et contrôle parental, afin de guider notamment en cas de *grooming* ou de demandes de photos personnelles adressées à des mineur·e·s :**
    - Utiliser parco.gov.gr pour accéder à des guides et des outils
- **Le retrait de contenu (par exemple : résultats de recherche obsolètes ou nuisibles) est possible dans tous les pays :**
    - Soumettre une demande via le Centre d'aide juridique de Google ou le formulaire relatif au droit à l'oubli

Le tableau suivant présente les domaines concernés, les cadres juridiques applicables et l'autorité compétente en Grèce.

Domaine	Cadre juridique / politique	Autorité compétente
Plateformes en ligne & services intermédiaires	La Loi 5099/2024 transpose le règlement européen sur les services numériques (DSA), encadre les contenus illégaux, la transparence et	Commission hellénique des télécommunications et de la poste (HTPC), Conseil national de la radio et de la télévision (NCRT), Autorité

	la protection des utilisateur·rice·s	hellénique de protection des données (HDPA)
Sites pornographiques & *revenge porn*	L'Article 346 du Code pénal (loi 4947/2022) criminalise la diffusion non consensuelle de contenus intimes	Division de la cybercriminalité de la police hellénique, Parquet/ Bureau du Procureur
Protection des mineur·e·s en ligne	Stratégie nationale de protection des mineur·e·s contre l'addiction à Internet ; inclut des contrôles parentaux, l'application Kids Wallet et la vérification de l'âge	Ministère de la Gouvernance numérique, Ministère de l'Éducation, Division de la cybercriminalité de la police hellénique
Signalement de contenus illégaux (par exemple : matériel pédopornographique, discours haineux, *grooming*)	SafeLine.gr (Centre grec pour un Internet plus sûr), membre de l'INHOPE, traite les signalements de contenus illégaux	Ligne d'assistance SafeLine, Division de la cybercriminalité de la police hellénique
Demande de retrait de contenu (droit à l'oubli, contenu nuisible)	RGPD & lois nationales sur la vie privée ; formulaires juridiques de retrait de Google ; SafeLine pour les contenus illégaux	Centre d'aide juridique de Google, SafeLine.gr, Autorité hellénique de protection des données

ESTONIE

En **Estonie**, le cadre juridique encadrant les plateformes en ligne, les sites pornographiques et la protection des utilisateur·rice·s - en particulier des mineur·e·s - est intégré dans un ensemble plus large de lois et de politiques portant sur la protection de l'enfance, les droits des consommateur·rice·s et la sécurité numérique, plutôt que dans une loi unique dédiée.

Domaine	Cadre juridique / politique	Autorité compétente
Protection des enfants contre les contenus violents / cruels	Loi sur la protection de l'enfance, paragraphe 25	Ministère des Affaires sociales, Agences de protection de l'enfance
Restrictions en matière de publicité visant les mineur·e·s	Loi sur la publicité	Autorité de protection des consommateur·rice·s et autorité de régulation technique
Restriction des contenus haineux / violents	Pouvoirs de l'autorité de protection des consommateur·rice·s et autorité de régulation technique	Autorité de protection des consommateur·rice·s et autorité de régulation technique
Prévention des abus sexuels sur enfants en ligne	Plan de développement pour la sécurité intérieure 2025–2028	Ministère de l'Intérieur
Mise en œuvre du règlement européen sur les services numériques (DSA)	Mise en œuvre nationale en cours	Autorité de protection des consommateur·rice·s et autorité de régulation technique
Sécurité des données et protection des utilisateur·rice·s	Système d'identité électronique, technologie *blockchain*	Ministère de la Justice et des Affaires numériques, RIA (Autorité des systèmes d'information)

Bien qu'il n'existe pas de loi estonienne spécifique régissant exclusivement les sites pornographiques, le DSA (règlement européen sur les services numériques) ainsi que les lois nationales imposent aux plateformes de prévenir l'accès des mineur·e·s aux contenus nuisibles. La loi sur les services médiatiques (*Media Services Act*) encadre les services de médias audiovisuels, y compris les contenus à la demande, en exigeant l'enregistrement et le respect de normes de contenu. La vérification de l'âge ainsi que les restrictions concernant les contenus préjudiciables aux mineur·e·s sont implicites dans ces cadres juridiques.

Comment signaler, demander le retrait d'un contenu, où et comment demander de l'aide ?

- Coordinateur estonien des services numériques : Dans le cadre du règlement européen sur les services numériques (DSA), l'Autorité estonienne de protection des consommateur·rice·s et de régulation technique agit comme coordinateur national pour les plaintes liées aux contenus illégaux sur les grandes plateformes en ligne. Des plaintes peuvent être déposées si une plateforme ne retire pas les contenus nuisibles ou illégaux, y compris ceux relevant de la violence basée sur le genre en ligne.

- Signalement à la police : Les victimes de VBG en ligne peuvent signaler des infractions telles que le cyberharcèlement, les menaces, ou la diffusion d'images non consensuelles à la police estonienne. Les forces de l'ordre peuvent enquêter et engager des poursuites judiciaires.

Où demander de l'aide :

- Ligne d'assistance d'urgence pour les victimes (116006) : Disponible 24h/24 et 7j/7 en estonien, anglais et russe, cette ligne gratuite offre des conseils confidentiels, un soutien émotionnel et une orientation aux personnes victimes de violences, y compris de VBG en ligne et de violences sexuelles. Elle fournit également des informations légales et détaille les services disponibles.

- Centres de crise pour violences sexuelles : Des centres spécialisés offrent une prise en charge gratuite et globale aux personnes victimes de violences sexuelles, y compris celles touchées par le harcèlement ou les abus sexuels en ligne.

- Campagne et site "*Notice. Intervene. Help.*" (Remarquer. Intervenir. Aider.) : Le Conseil national de l'assurance sociale mène une campagne de prévention du harcèlement sexuel, y compris sous ses formes en ligne. Le site www.palunabi.ee/ooelu propose des conseils pratiques pour les victimes et les témoins sur la manière de reconnaître une situation de harcèlement et d'intervenir en toute sécurité.

GUYANA

Le Guyana a accompli des avancées notables dans la mise en place d'un modèle de réponses interconnectées, reflétant une approche multidimensionnelle.

Cadres politiques

Le paysage législatif et politique du Guyana a évolué pour offrir des protections renforcées et des mécanismes de responsabilité plus solides :

- ***Family Violence Act*** **(2024)** : Une réforme majeure qui intègre des recours à la fois pénaux et civils, permettant aux tribunaux et à la police d'intervenir dans les cas de violence domestique.
- ***Sexual Offences Act*** (2010, amendée en 2013) et ***Domestic Violence Act*** (1996, mise à jour en 2015) : Ces lois constituent la base juridique de la protection des survivant·e·s.
- ***National Gender Equality and Social Inclusion Policy*** (2018) : Cette politique promeut la réforme législative, l'aide aux victimes et la sensibilisation du public afin d'éliminer la violence et les discriminations.

Par ailleurs, la réponse du Guyana face à la VBG repose sur une coordination multisectorielle :

- Le **ministère des Services sociaux et de la Sécurité sociale** assure la mise en œuvre à travers l'unité chargée de la politique sur les infractions sexuelles et la violence domestique.
- La **police du Guyana** dispose désormais de pouvoirs élargis pour intervenir dans les cas de VBG relevant de la sphère privée, notamment en procédant à des arrestations et à l'éloignement des auteur·rice·s.
- Le **secteur de la santé** participe à travers l'organisation de symposiums médicaux et de formations en soins tenant compte des traumatismes, à destination des professionnel·le·s.
- Le **Réseau communautaire de défense (CAN : *Community Advocate Network*)** mobilise des leaders locaux pour soutenir les survivant·e·s et sensibiliser les communautés.
- La **ligne d'assistance 914** offre un soutien rapide et confidentiel aux victimes à l'échelle nationale.

Les partenariats internationaux du Guyana s'articulent autour des éléments suivants :

- **Initiative Spotlight (UE & ONU)** : Le modèle développé par le Guyana dans le cadre de cette initiative est reconnu comme une référence régionale en matière de réponse à la VBG. Il permet de canaliser des financements, un appui technique et des outils de suivi vers les programmes locaux.

- **Cadres de la PANCAP et de la CARICOM** : Ces structures favorisent le dialogue régional, le partage de données et l'harmonisation des politiques entre les États des Caraïbes.

- **Stratégie de Montevideo & synergie Beijing +25** : Ces engagements alignent les efforts du Guyana sur les objectifs mondiaux en matière d'égalité de genre, incluant la protection des femmes autochtones et des survivant·e·s de la traite des humains.

EXPLOITATION NUMÉRIQUE LIÉE À LA PROSTITUTION ET À LA TRAITE TRANSFRONTALIÈRE DES ÊTRES HUMAINS.

4. Exploitation numérique liée à la prostitution et à la traite transfrontalière des êtres humains

La vulnérabilité des femmes **et des personnes vulnérabilisées** face à l'exploitation sexuelle numérique s'enracine également dans les inégalités structurelles. L'accès limité à l'éducation, les taux de chômage élevés, la pauvreté et les rares opportunités économiques qui en découlent limitent souvent les choix des femmes **et d'autres personnes concernées**, poussant certain·e·s d'entre elles et eux vers la production de contenus sexuels en ligne (tels que la pornographie, le camming ou les plateformes d'escorte) comme l'une des rares sources de revenus disponibles. Ces risques sont accrus pour les femmes **et les personnes** qui migrent pour trouver du travail ou qui sont déplacé·e·s par des conflits ou des crises environnementales, car elles et ils sont souvent confronté·e·s à la précarité juridique, aux barrières linguistiques et à l'absence de réseaux de soutien.Le manque de ressources et d'éducation numérique ou sexuelle augmente encore leur exposition au recrutement trompeur et à la coercition. Il est essentiel de comprendre ces facteurs systémiques pour lutter contre le fait que les plateformes numériques deviennent des lieux d'exploitation plutôt que d'autonomisation.

4.1. Les défis de la coopération internationale

Si la coopération internationale et transfrontalière dans la lutte contre la violence sexiste en ligne et l'exploitation numérique des femmes **et des personnes vulnérabilisées** est de la plus haute importance, elle est semée d'embûches et de lacunes liées, entre autres, à la diversité des cadres juridiques, aux limites et obstacles juridictionnels, aux politiques d'extradition, à l'interopérabilité des bases de données, à la lenteur des délais de réponse due aux processus internes et à la bureaucratie.

• **Obstacles juridiques et juridictionnels** : comme les définitions juridiques diffèrent, les pays peuvent interpréter différemment des concepts tels que la cyberviolence, le consentement et l'exploitation numérique. Un acte considéré comme criminel dans une juridiction peut ne pas (encore) exister dans le cadre juridique d'un autre pays, de sorte que l'acte en question reste non réglementé et sans restriction.

• **Ambiguïté juridique transfrontalière** : comme les auteur·rice·s agissent souvent à l'échelle internationale, il peut être long de déterminer quel pays est compétent pour poursuivre un acte criminel spécifique. Les avocat·e·s de la défense exploitent cette situation à leur avantage, inventant des failles dans le seul but de retarder la justice.

• **Limites de l'extradition** : à ce jour, de nombreux traités internationaux ne traitent pas encore de la cybercriminalité. Par conséquent, même si des procédures d'extradition sont en place, de nouveaux traités ou protocoles additionnels sont nécessaires pour que les victimes **et survivant·e·s** puissent obtenir un recours juridique.

• **Lacunes et disparités opérationnelles et administratives dans l'application de la loi** : tous les pays ne disposent pas des mêmes infrastructures, formations, capacités ou compétences pour lutter contre la violence sexiste facilitée par la technologie.

• **Difficultés liées à la collecte de preuves numériques** : la collecte de preuves numériques pouvant être utilisées dans le cadre de poursuites judiciaires dans différentes juridictions est complexe tant sur le plan technique que juridique.

• **Fragmentation des politiques et de la coordination** : l'absence de protocoles unifiés et de normes mondiales pour lutter contre la violence sexiste en ligne rend les efforts internationaux incohérents et souvent inefficaces. Les lacunes en matière de données sont au cœur de ce problème ; sans pratiques harmonisées de collecte de données, cette collecte demande du temps, des efforts et des ressources.

• **Sous-utilisation de la société civile** : les ONG et les organisations locales sont souvent en première ligne pour soutenir et défendre les victimes **et les survivant·e·s**, mais elles sont rarement intégrées dans les mécanismes officiels de coordination internationale ou les sessions de consultation.

• **Problèmes de responsabilité, de transparence et de conformité des plateformes** : certains services, sites web et applications peuvent fonctionner en dehors du champ d'application des lois nationales et refuser les demandes de suppression de contenus préjudiciables ou de partage de données sur les utilisateur·rice·s / suspect·e·s potentiel·le·s. Ici, bien sûr, le dilemme entre vie privée et responsabilité refait surface : le cryptage et l'anonymat sont certes essentiels pour la sécurité des femmes **et des personnes ciblées** en ligne, mais ils facilitent également la tâche des auteur·rice·s de violences et compliquent les enquêtes.

• **Absence de volonté politique** : certain·e·s pays ne traitent pas la violence et l'exploitation sexuelles en ligne comme un problème grave, et ne sont donc pas enclin·e·s à participer activement à des initiatives transfrontalières

• **Ces défis globaux de coopération** se recoupent également avec les questions migratoires, où la vulnérabilité accrue des personnes déplacées les expose à de nouvelles formes d'exploitation.

4.2. L'intégration avec les migrations

Les conflits armés, le changement climatique (perte de productivité, catastrophes, hausse des prix des denrées alimentaires), la pauvreté et les inégalités sociales sont autant de causes profondes de la migration et exposent les personnes au risque de traite et

d'exploitation. Les migrant·e·s sont considéré·e·s comme particulièrement vulnérables à l'exploitation sexuelle et à la traite en raison d'une combinaison de **facteurs de risque structurels, sociaux et personnels** que les trafiquant·e·s exploitent activement. Il s'agit notamment de la précarité juridique et économique, telle que le statut juridique irrégulier ou précaire, la vulnérabilité financière et, dans certains cas, la servitude pour dettes. Ils et elles ignorent souvent **la langue, les droits et les protections juridiques** du pays d'accueil, ce qui peut les empêcher de demander de l'aide. Le manque d'accès à des informations précises permet aux trafiquant·e·s de les induire plus facilement en erreur sur les conditions de travail ou les exigences légales. Les migrant·e·s manquent également souvent **de réseaux sociaux et familiaux** solides dans le pays d'accueil, ce qui les rend vulnérables à l'exploitation par les recruteur·euse·s, les employeur·euse·s ou les « intermédiaires communautaires ». Les migrant·e·s qui recherchent un emploi en ligne ou par le biais de groupes informels sur les réseaux sociaux sont souvent la cible de **fausses offres** (par exemple, travail domestique, hôtellerie, mannequinat) qui se transforment en situations de traite.

À l'échelle mondiale, le nombre de victimes de la traite est en augmentation depuis la pandémie de COVID-19, et de plus en plus d'enfants sont détecté·e·s comme victimes. Les filles et les garçons victimes présentent des schémas d'exploitation différents, la majorité des filles victimes détectées (60 %) étant victimes de traite à des fins d'exploitation sexuelle, alors que ce chiffre n'est que de 8 % pour les garçons. Il en va de même pour les femmes, pour lesquelles l'exploitation sexuelle représente 66 %. Cette forme de traite comprend divers types d'exploitation, allant de la prostitution forcée des adultes et de l'exploitation sexuelle des enfants à l'esclavage sexuel. En ce qui concerne l'exploitation numérique, les exemples de cas judiciaires comprennent des cas d'enfants exploité·e·s pour produire du matériel pédopornographique, des spectacles par webcam et des appels cybersexuels. (ONUDC, Rapport mondial sur la traite des personnes (ensembles de données et analyses mondiaux).

Les plateformes numériques sont devenues essentielles pour faciliter la prostitution et la traite des êtres humains. Dans certaines régions, les comptes de réseaux sociaux sont associés à plus de 60 % des cas de traite identifiés, et 77 % des trafiquant·e·s ciblent les enfants en utilisant les réseaux sociaux et d'autres outils en ligne.

Les trafiquant·e·s utilisent les petites annonces et les sites web d'escorte, les réseaux sociaux et les applications de rencontre, les services de messagerie et même les marchés du darknet pour recruter, faire de la publicité, contrôler et exploiter leurs victimes. Des analyses internationales ont régulièrement mis en évidence le recours à Internet pour le recrutement et la publicité dans les affaires de traite ; par exemple, les études de cas de l'ONUDC et la cartographie de l'OSCE identifient les sites d'escorte, les sites web de massage/services sexuels et les réseaux sociaux comme des canaux courants. Aux États-Unis, la National Human Trafficking Hotline et Polaris ont recensé des centaines de cas de

recrutement en ligne et identifié des milliers de contacts liés à la traite facilitée par la technologie. Polaris rapporte que depuis 2015, la hotline a signalé **plus de 950 victimes potentielles de traite à des fins sexuelles** qui ont été recrutées en ligne. Les outils numériques modifient la manière dont la coercition et le contrôle sont exercés (grooming à distance, publicités trompeuses, surveillance via des applications de messagerie et canaux de paiement) et compliquent également les réponses, car les plateformes sont transfrontalières et opèrent sous des régimes juridiques variés.

Plateformes numériques utilisées à des fins d'exploitation sexuelle

Les outils numériques et les plateformes en ligne sont largement utilisés dans le cadre de l'exploitation sexuelle à travers le monde, car de nombreuses plateformes manquent de modération, de mécanismes de signalement et de transparence dans leur manière de traiter les cas d'exploitation. Par exemple, OnlyFans a soumis **230 signalements** au Centre national pour les enfants disparu·e·s et exploité·e·s (NCMEC), auxquels s'ajoutent **64 signalements supplémentaires** déposés en février 2025, ce qui souligne les difficultés persistantes dans la détection des contenus impliquant des mineur·e·s.

Ils et elles reçoivent également des plaintes récurrentes concernant des contenus explicites impliquant des personnes qui ont été publiés sur la plateforme sans leur consentement.

En août 2025, le commissaire britannique chargé de la lutte contre l'esclavage a lancé une enquête sur les sites d'escorte/d'annonces (par exemple, Vivastreet), décrits comme des « sites web de proxénétisme ». Une étude écossaise de 2021 a souligné que ces plateformes ont « dopé le commerce du trafic sexuel ».

Outre les plateformes d'escorte et de contenu pour adultes, les trafiquant·e·s utilisent également massivement les plateformes de réseaux sociaux grand public telles que Tinder, Instagram et TikTok, ainsi que les places de marché en ligne et même les plateformes de jeux en ligne telles que Roblox, Minecraft ou Hago. Les plateformes qui combinent la popularité auprès des jeunes et des fonctionnalités sociales (telles que le chat, la voix, les avatars et les récompenses dans les jeux) sont devenues un terrain fertile pour les abus. L'ampleur du grooming, la rapidité avec laquelle il se développe et son lien fréquent avec des plateformes extérieures aux jeux eux-mêmes (comme Discord ou Snapchat) soulignent la nécessité urgente d'améliorer la conception de la sécurité, les systèmes de modération et la sensibilisation des parents/éducateur·rice·s. Les plateformes de jeux sont particulièrement utilisées pour cibler les jeunes et les enfants. Les signalements d'exploitation sur Roblox sont passés de **675 en 2019 à plus de 24 000 en 2024,** ce qui met en évidence l'ampleur du problème.

• Réseaux sociaux et applications de messagerie

Les trafiquant·e·s utilisent des plateformes grand public telles que Facebook, Instagram, TikTok, LinkedIn, WhatsApp et Telegram pour recruter, séduire et contrôler leurs victimes. Ils

et elles se font souvent passer pour des ami·e·s, des prétendant·e·s ou des recruteur·euse·s. Ces plateformes leur permettent de cibler facilement des personnes vulnérables et d'utiliser des canaux de communication privés qui dissimulent l'exploitation. Les profils Instagram peuvent être déguisés en annonces d'escorte, avec des coordonnées dans les biographies ou les stories. Des ONG en France et au Royaume-Uni ont documenté des cas de trafiquant·e·s créant de fausses « agences de mannequins » sur Instagram pour attirer des jeunes femmes **et des personnes concernées**. Sur LinkedIn ou Indeed, les trafiquant·e·s se font passer pour des recruteur·euse·s ou des responsables des ressources humaines, contactant directement des jeunes ou des chômeur·euse·s, leur proposant par exemple « un travail à l'étranger » ou « des revenus élevés sans expérience requise ».

●Plateformes de jeux en ligne

Les plateformes de jeux en ligne ont été utilisées à des fins de grooming, de coercition ou d'exploitation sexuelle d'enfants et d'adolescent·e·s. Les prédateur·rice·s rencontrent leurs victimes par le biais de jeux et peuvent les contraindre à partager du contenu explicite ou à les rencontrer en personne. Des adultes auraient attiré des enfants à l'aide de monnaies virtuelles (telles que le Robux de Roblox), puis les auraient dirigé·e·s vers des applications telles que Discord ou Snapchat à des fins d'exploitation.

●Sites de rencontre et d'escorte

Les sites web et les applications conçus pour les rencontres (par exemple, Tinder, Bumble) ou les services sexuels/d'escorte commerciaux sont souvent utilisés pour faire de la publicité pour des victimes sous la contrainte. Les annonces peuvent dissimuler l'exploitation sous le couvert d'un travail sexuel consensuel, ce qui rend la détection difficile. Les trafiquant·e·s sur Tinder peuvent se faire passer pour des partenaires potentiel·le·s, instaurant une relation de confiance avant de manipuler les victimes à des fins d'exploitation sexuelle. Ils et elles exploitent le système de mise en relation basé sur la localisation de Tinder pour identifier les personnes vulnérables (migrant·e·s, réfugié·e·s, voyageur·euse·s) dans les zones frontalières ou les nouveaux pays d'accueil, leur proposant une « aide » ou des « emplois » qui mènent à l'exploitation, tels que des opportunités de mannequinat ou de *sugar baby*.

● Petites annonces et marchés en ligne

Certain·e·s trafiquant·e·s publient des offres d'emploi trompeuses (par exemple, mannequinat, hôtellerie, travail au pair) sur des marchés mondiaux de petites annonces ou leurs équivalents locaux. Les victimes peuvent être attiré·e·s dans des situations d'exploitation sous le couvert d'un emploi légitime. Les fausses annonces pour des chambres, des biens d'occasion ou des « amitiés » peuvent servir de points d'entrée aux trafiquant·e·s pour identifier et approcher des personnes vulnérables. Les migrant·e·s à la recherche d'un logement abordable sur Facebook Marketplace, par exemple, ont été la cible d'« offres » liées à l'exploitation sexuelle.

•Plateformes de diffusion en direct et de contenu pour adultes

Les trafiquant·e·s exploitent les victimes en diffusant en direct des actes sexuels sur des sites de webcams ou en téléchargeant du contenu obtenu sous la contrainte sur des plateformes par abonnement. Les trafiquant·e·s forcent les victimes (notamment des enfants, des migrant·e·s ou des adultes vulnérables) à se produire devant une caméra sous la menace, la violence ou la servitude pour dettes. Les victimes peuvent être enfermées dans des pièces, surveillées ou privées de leurs gains, tandis que les trafiquant·e·s contrôlent les comptes. Dans certains cas, les trafiquant·e·s forcent les victimes à rencontrer des clients hors ligne après des « spectacles » en ligne, ce qui constitue une passerelle vers la prostitution en personne. Les plateformes peuvent également être utilisées à des fins de « sextorsion ». Le public ou les trafiquant·e·s enregistrent les victimes sans leur consentement et utilisent les images à des fins de chantage (« recommencez ou cela sera rendu public »).

•Marchés du darknet et services cryptés

Les services cachés sur le darknet facilitent la publicité et la distribution de matériel exploitant des personnes. Les forces de l'ordre ont du mal à surveiller ces marchés cachés.

Mesures de protection

La protection des individus nécessite une stratégie à plusieurs volets : une modération rigoureuse des plateformes et un signalement obligatoire, une détection améliorée par la technologie pour les forces de l'ordre, une réglementation des plateformes de services pour adultes et des ressources d'autonomisation pour les créateur·rice·s, les jeunes et les populations vulnérables. Les plateformes devraient être légalement tenues de signaler les activités suspectes aux autorités, d'exiger des contrôles d'identité proactifs, de mettre en place un filtrage rigoureux des images/vidéos et de se soumettre à des audits sur la manière dont elles traitent les plaintes pour exploitation. Les sites web d'escorte devraient être réglementés afin d'éviter les abus, et les forces de l'ordre devraient utiliser des outils de détection basés sur l'intelligence artificielle pour identifier les schémas de traite dans les annonces d'escorte.

Les migrant·e·s peuvent être mieux protégé·e·s en les sensibilisant davantage aux risques liés aux escroqueries de recrutement en ligne et à l'exploitation sexuelle. Les centres communautaires, les ONG et les services locaux devraient enseigner aux migrant·e·s comment vérifier les offres en ligne, protéger leur vie privée et utiliser les plateformes en toute sécurité. Les ateliers ou l'éducation par les pairs, impliquant les leaders des

communautés de migrant·e·s, font partie des bonnes pratiques. Le contenu devrait être clair et adapté à la culture.

Les jeunes et les enfants, en particulier, doivent être sensibilisé·e·s aux tactiques de grooming en ligne et aux « signaux d'alerte » (par exemple, la pression pour garder les conversations secrètes, les demandes d'images intimes), et les parents doivent être sensibilisé·e·s à l'importance des contrôles parentaux, des filtres de confidentialité et des fonctionnalités de sécurité des plateformes. Des campagnes de sensibilisation sur ces sujets sont nécessaires dans les écoles, dans d'autres environnements éducatifs et dans les médias, ainsi que la formation des travailleur·euse·s sociaux·ales et éducatifs.

Étude de cas : la migration au Guyana

La migration au Guyana est un phénomène complexe et historiquement important qui a façonné la démographie, l'économie et les relations internationales du pays.

Décomposition des aspects clés :

Tendances historiques en matière d'émigration

● Années 1960-1980 : le Guyana a connu des taux d'émigration élevés, en particulier après son indépendance en 1966. L'instabilité politique, les difficultés économiques et les opportunités limitées ont poussé de nombreux·ses Guyanien·ne·s à chercher une vie meilleure à l'étranger.

● **Destinations** : les premiers émigrant·e·s se sont souvent installé·e·s au Royaume-Uni en raison des liens coloniaux, mais au fil du temps, les États-Unis et le Canada sont devenus plus populaires en raison de politiques d'immigration favorables et de meilleures perspectives d'emploi.

● **Migration qualifiée** : le Guyana s'est fait connaître pour son exportation de main-d'œuvre qualifiée, de nombreux·ses professionnel·le·s quittant le pays pour poursuivre leurs études ou trouver un emploi à l'étranger.

Tendances migratoires récentes

● **Baisse du taux net de migration** : selon les données de la Banque mondiale et des Nations unies, le taux net de migration du Guyana jusqu'en 2023 était six fois inférieur à celui des années 1980 et 1990.

● **Évolution des motivations** : si l'émigration persiste, de plus en plus de Guyanien·ne·s

voyagent pour des raisons de courte durée, telles que les affaires et les vacances, plutôt que pour s'installer définitivement à l'étranger.

Gestion et politique migratoires

● **Implication de l'OIM** : le Guyana a rejoint l'Organisation internationale pour les migrations (OIM) en 2011. Depuis lors, l'OIM a apporté son soutien :

● l'engagement de la diaspora dans le développement national

● les initiatives en matière de migration et de santé

● les programmes d'aide au retour volontaire et à la réintégration (AVRR) de pays comme le Canada et le Royaume-Uni

Le Guyana sert également de centre de coordination pour les opérations de l'OIM dans les Caraïbes.

Impact sur le développement

● **Contributions de la diaspora** : les transferts de fonds et le transfert de connaissances de la diaspora jouent un rôle essentiel dans le développement du Guyana.

● **Fuite des cerveaux ou gain de cerveaux** : si l'émigration a entraîné une perte de main-d'œuvre qualifiée, des initiatives visent désormais à exploiter le potentiel de la diaspora pour la croissance et le développement nationaux.

L'intersection entre migration, pressions environnementales et exploitation numérique au Guyana révèle un ensemble de défis complexes, en particulier pour les populations vulnérabilisées des régions intérieures et côtières.

Examen de l'interaction entre ces forces :

Facteurs environnementaux de la migration au Guyana

● Vulnérabilité climatique : l'érosion côtière, les inondations et l'évolution des régimes pluviométriques, exacerbés par le changement climatique, provoquent le déplacement de communautés, en particulier dans les zones de basse altitude telles que les régions d'Essequibo et de Demerara.

● Migration des zones rurales vers les zones urbaines : les facteurs de stress environnementaux poussent les populations des zones reculées et les communautés

autochtones vers les centres urbains comme Georgetown, souvent sans bénéficier de systèmes de soutien adéquats.

● Pressions sur les ressources : la déforestation et la dégradation des sols liées à l'exploitation minière et à l'agriculture contribuent également aux déplacements internes et aux migrations.

Risques liés à l'exploitation numérique

À mesure que la migration augmente, en particulier chez les jeunes et les femmes **et les personnes vulnérabilisées**, les plateformes numériques deviennent à la fois des bouées de sauvetage et des pièges potentiels :

● Escroqueries liées au recrutement en ligne : les migrant·e·s à la recherche d'un emploi à l'étranger ou dans les zones urbaines peuvent être victimes d'offres frauduleuses en ligne, qui peuvent conduire à la traite ou à l'exploitation par le travail.

● Vulnérabilité des données : leur maîtrise limitée du numérique rend les migrant·e·s vulnérables à l'usurpation d'identité, au phishing et à l'utilisation abusive de leurs informations personnelles.

● Exploitation liée au genre : les femmes et les filles qui migrent pour trouver un emploi ou suivre des études sont exposées à des risques accrus de sextorsion, de cyberharcèlement et de harcèlement en ligne.

Difficultés et défis au Guyana

● Fracture numérique : les communautés de l'arrière-pays et les communautés autochtones manquent souvent d'un accès fiable à Internet, ce qui les rend invisibles et vulnérables sur le plan numérique.

● Protections juridiques limitées : les cadres juridiques relatifs à la migration et à la sécurité numérique au Guyana sont encore en cours d'élaboration, ce qui laisse des lacunes dans la protection des personnes déplacées par le changement climatique et celles vulnérables à l'exploitation numérique.

● Confiance et barrières culturelles : des études montrent que la confiance dans les services administratifs en ligne est faible et que des facteurs culturels entravent l'adoption de mesures de protection numériques.

● Pressions géopolitiques : les conflits territoriaux et les changements sur le marché du travail ajoutent à la complexité de la gouvernance des migrations.

Solutions émergentes

● Pôles TIC dans les régions de l'arrière-pays : plus de 200 pôles ont été créés pour améliorer l'accès au numérique, l'éducation et les systèmes d'alerte précoce en cas d'événements climatiques.

● Expansion de l'administration en ligne : le Guyana investit dans la gouvernance numérique afin d'améliorer la prestation de services et de réduire les risques d'exploitation.

● Engagement de la diaspora : des programmes sont en cours d'élaboration afin de tirer parti des compétences et des ressources des Guyanien·ne·s à l'étranger, tout en protégeant celles et ceux qui migrent.

L'expansion rapide des infrastructures numériques en Guyane a apporté à la fois des opportunités et des risques. Si les outils numériques ont donné plus de pouvoir aux citoyen·ne·s et amélioré les services publics, ils ont également été utilisés à des fins d'exploitation.

Les outils numériques sont principalement utilisés à des fins d'exploitation au Guyana

● Plateformes de réseaux sociaux (Facebook, WhatsApp, Instagram) : utilisées pour le phishing, l'usurpation d'identité, le chantage sexuel et les escroqueries liées au recrutement. Les exploiteur·rice·s se font souvent passer pour des employeur·euse·s, des partenaires amoureux ou des agents gouvernementaux afin de gagner la confiance des victimes et d'accéder à leurs données personnelles.

● E-mails de phishing et liens malveillants : envoyés par e-mail ou via des applications de messagerie, ces liens incitent les utilisateur·rice·s à révéler leurs mots de passe ou à télécharger des logiciels malveillants. Les escroqueries courantes comprennent les fausses alertes bancaires, les offres d'emploi ou les avis gouvernementaux.

● Botnets et logiciels malveillants : les criminel·le·s utilisent des appareils infectés pour lancer des attaques à distance ou voler des données. Ces réseaux peuvent être utilisés pour l'usurpation d'identité, la fraude financière ou la diffusion de contenus illégaux.

● Outils d'ingénierie sociale : les exploiteur·rice·s utilisent des données accessibles au public pour manipuler leurs victimes par le biais d'appels téléphoniques ou de messages directs. Ils et elles se font souvent passer pour des agents du service clientèle ou des fonctionnaires afin d'obtenir des informations sensibles.

● Logiciels espions et PUP (programmes potentiellement indésirables) : ceux-ci sont cachés dans les téléchargements et peuvent surveiller l'activité des utilisateur·rice·s, voler des données ou désactiver les fonctionnalités de sécurité.

Mesures de protection

● Politiques et législation en matière de cybersécurité : la Guyane a mis en œuvre 43 politiques de cybersécurité dans l'ensemble des agences gouvernementales afin de protéger les infrastructures numériques. Des lois telles que la loi sur la protection des données et la loi sur la carte d'identité numérique visent à protéger la vie privée des utilisateur·rice·s et à sécuriser les transactions en ligne.

● Formation nationale à la cybersécurité : les fonctionnaires sont formé·e·s à la détection et à la réponse aux cybermenaces. Des événements tels que le salon de la cybersécurité réunissent des expert·e·s pour des ateliers et des démonstrations en direct.

● Systèmes publics intelligents : des systèmes tels que la billetterie électronique intelligente Safe Road, le contrôle automatisé des frontières et les dossiers médicaux électroniques sont conçus avec des protocoles de sécurité intégrés.

● Plan directeur des TIC (2030) : cette feuille de route stratégique met l'accent sur l'efficacité, la sécurité et la résilience numériques dans tous les secteurs. Elle comprend des systèmes de surveillance, des cadres d'évaluation et des technologies de pointe pour détecter et prévenir la cybercriminalité.

● Sensibilisation et éducation de la communauté : les ONG et les agences gouvernementales s'efforcent d'améliorer la culture numérique, en particulier dans les communautés rurales et vulnérables. Les campagnes de sensibilisation ciblent les jeunes et les femmes, qui sont touché·e·s de manière disproportionnée par l'exploitation numérique.

Sources :
● guyanapoliceforce.gy
● guyanatimesgy.com
● dpi.gov.gy

Un exemple révélateur : les migrantes vénézuéliennes dans le secteur de la vie nocturne en Guyane

L'un des exemples les plus révélateurs de l'exploitation des migrant·e·s au Guyana concerne la migration forcée de femmes et d'enfants vénézuélien·ne·s, poussé·e·s par la crise humanitaire qui sévit actuellement au Venezuela. Beaucoup ont traversé la frontière du Guyana par des points de passage informels dans les régions 1 et 7, à la recherche de sécurité et d'opportunités économiques, mais se sont retrouvé·e·s dans une situation de vulnérabilité accrue.

Selon Stabroek News, de nombreuses femmes vénézuéliennes qui ont fui vers le Guyana en quête de sécurité et d'opportunités économiques ont fini par être exploitées dans le secteur **de la vie nocturne et du commerce du sexe.** Voici comment cette exploitation s'est déroulée :

● **Recrutement et tromperie** : les femmes étaient attirées par des promesses d'emplois légitimes, tels que serveuses ou aides ménagères, mais étaient en réalité contraintes à se prostituer.

● **Menaces et coercition** : les exploiteur·rice·s ont utilisé des menaces d'expulsion, de violence et d'isolement pour contrôler leurs victimes. Certain·e·s se sont vu dire qu'elles et ils seraient remis·es aux autorités d'immigration s'elles/ils ne se conformaient pas.

• **Implication des autorités** : il est inquiétant de constater que, selon certaines informations, **des fonctionnaires de l'État,** notamment **des policier·ère·s et des agent·e·s des services d'immigration**, se seraient rendu·e·s complices en facilitant ces arrangements abusifs ou en tirant profit de ceux-ci.

• **Recours juridiques limités** : les victimes manquaient souvent de documents, de compétences linguistiques ou de confiance dans les autorités locales, ce qui rendait difficile le signalement des abus ou la recherche d'aide.

Cette affaire met en évidence **l'intersection entre le genre, la migration et la vulnérabilité numérique,** car de nombreuses victimes ont été recrutées ou surveillées via les réseaux sociaux et les applications de messagerie.

Implications plus larges

• **Risques liés à la traite des êtres humains** : le Guyana a fait des progrès dans la lutte contre la traite, mais les régions reculées manquent encore de surveillance.

• **Lacunes politiques** : bien que le Guyana soit classé au niveau 1 dans le rapport américain sur la traite des personnes, l'application de la loi et le soutien aux victimes restent inégaux.

• **Nécessité d'une protection communautaire** : les ONG et les groupes de défense tels que *Women Across Differences* jouent un rôle essentiel dans la sensibilisation, l'éducation et le soutien aux survivant·e·s.

4.3 Sensibiliser les communautés à la sécurité numérique

Si les plateformes en ligne occupent une place de plus en plus centrale dans nos vies, elles peuvent également présenter de sérieux risques si elles ne sont pas utilisées de manière responsable. Les nouvelles technologies de l'information et de la communication ont révolutionné la distribution des médias, l'accès à l'information et la communication mondiale. Cependant, ces mêmes technologies peuvent faciliter l'exploitation sexuelle aux niveaux local, national et international (Hughes, 2002).

Il est donc essentiel que tous les acteurs et actrices communautaires accordent la priorité à la sécurité numérique. Cela implique de se former à l'aide de ressources actualisées pour lutter contre la violence en ligne et de transmettre aux mineur·e·s et aux jeunes des connaissances sur les risques numériques et les stratégies de prévention. Dans le milieu éducatif, les enseignant·e·s jouent un rôle central dans le renforcement de la culture numérique ; il est essentiel de pouvoir compter sur des éducateur·rice·s compétent·e·s et motivé·e·s (Tomczyk, 2019). Les décideur·euse·s politiques doivent également reconnaître

les enfants comme des participant·e·s actif·ve·s dans le monde numérique, capables d'interagir de manière significative avec l'information (Patterson et al., 2022).

Dans l'ensemble, l'objectif de la culture numérique dans le contexte de la sécurité sur Internet est de promouvoir une utilisation sûre, créative et éclairée des médias numériques (Kurniasih, 2023). Si de nombreuses initiatives en matière de sécurité sur Internet ont vu le jour au cours des deux dernières décennies pour encourager un comportement responsable en ligne, leurs méthodes de mise en œuvre peuvent encore être améliorées (Quayle, 2020). En fonction du public cible, les ressources vont de l'interactif à l'explicatif, chacune offrant de précieuses opportunités d'engagement.

Les plateformes numériques sont devenues centrales dans la vie quotidienne des jeunes. Elles offrent des possibilités d'apprentissage et de communication, mais, comme mentionné ci-dessus, elles exposent également les mineur·e·s à des risques importants, notamment l**e cyberharcèlement, l'exposition à des contenus préjudiciables et l'exploitation sexuelle** (Hughes, 2002).

La protection des enfants en ligne nécessite **l'engagement de l'ensemble de la communauté.** Les écoles, les familles et les autorités locales ont toutes un rôle à jouer dans **le développement de la culture numérique et de la sensibilisation :**

• **Les enseignant·e·s** peuvent donner aux élèves les moyens de reconnaître les risques en ligne et d'y répondre efficacement (Tomczyk, 2019).

• **Les parents et les personnes qui s'occupent des enfants** ont besoin de conseils pratiques pour encadrer l'utilisation des écrans et discuter ouvertement des expériences en ligne.

• **Les décideur·euse·s politiques** doivent veiller à ce que les enfants soient reconnu·e·s comme **des citoyen·ne·s numériques actif·ve·s** et bénéficient de **mesures de protection solides** (Patterson et al., 2022).

Des études recentes illustrent **l'ampleur et l'urgence** de ce défi.

Chiffres clés : risques en ligne pour les jeunes

Domaine à risque	Statistiques clés	Sources
Cyberharcèlement	15 % des adolescent·e·s (≈1 sur 6) ont été victimes	Santé Mentale, (2024) ; Jedha, (2025)

	de cyberharcèlement ; 29 % au lycée	
Exposition à des contenus préjudiciables	**Âge** moyen de la première exposition à la pornographie : **10 ans** ; 70 % des 11-18 ans ont vu des contenus perturbants (violence, pornographie, images de guerre)	Rapport Élysée, (2023) ; Le Monde, (2024)
Temps passé devant un écran	6-17 ans : **4 h 11 par jour** ; adolescent·e·s de 13 à 19 ans : **plus de 7 h par jour** ; 57 % des moins de 20 ans signalent des effets négatifs	GoStudent, (2025) ; INSEE, (2024)

Ces tendances soulignent **la vulnérabilité croissante des jeunes face au numérique.** Une éducation numérique efficace n'est pas seulement une mesure de protection ; elle **favorise une participation saine, éclairée et créative** au monde en ligne (Kurniasih, 2023).

Pour être efficaces, les stratégies communautaires doivent inclure :

• **Une intervention précoce dans les écoles,** dès l'enseignement primaire.

• **L'engagement des parents et des personnes qui s'occupent des enfants** et des campagnes de sensibilisation afin de réduire l'exposition précoce à des contenus préjudiciables.

• **Des cadres politiques clairs** reliant la protection des enfants, l'éducation aux médias et la santé publique.

En combinant **éducation, prévention et mesures politiques,** les communautés peuvent créer **des environnements numériques plus sûrs et plus autonomisants** pour les enfants et les adolescent·e·s.

Campagnes éducatives sur la sécurité numérique

Campagnes vidéo à l'échelle de l'UE

● 51Campagne « Share with Care » (Partager avec prudence) de Deutsche Telekom pour le partage de photos et de vidéos d'enfants en ligne : https://youtu.be/F4WZ_k0vUDM

● Campagne « Say No » d'Europol contre le catfishing et l'extorsion sexuelle : https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-preventionguides/online-sexual-coercion-and-extortion-crime

Exemples de ressources sur la sécurité numérique des migrants

● MIDEQ – Formation sur l'utilisation sûre, judicieuse et sécurisée des technologies numériques

Langue : anglais. Présentation PowerPoint et notes de l'animateur·rice librement accessibles, sous licence Creative Commons, conçues pour autonomiser les femmes **migrantes et les personnes migrantes** en Afrique australe.
Les thèmes abordés comprennent le harcèlement en ligne, les escroqueries, l'usurpation d'identité et la désinformation.

https://www.mideq.org/en/impact/impact-resources/training-on-safe-wise-and-secure-use-of-digitaltechnology/

● Tabliteracy – Cours sur la citoyenneté numérique (Irlande)
Langue : anglais (conçu pour les apprenant·e·s ayant un niveau d'anglais faible)
Un dispositif pédagogique sur tablette qui aborde la sécurité en ligne, la recherche d'emploi, la recherche de services, les outils de communication et l'intégration locale en Irlande. Il est basé sur des activités et adapté aux besoins de la vie réelle.

FRANCE

Bonnes pratiques et activités pratiques en France

● Cybermalveillance.gouv.fr – « Cyber Guide Famille » et campagnes destinées aux jeunes
○ Propose des outils pédagogiques tels que des bandes dessinées, des quiz, des vidéos animées et un cahier de vacances « As du Web » adapté aux 7-14 ans.

○ Les activités peuvent être adaptées en classe : quiz interactifs, discussions basées sur des scénarios et exercices d'identité « super-héros numériques ».

Assurance Prévention+7Education Ministère+7cnil. fr+7CYBERMALVEILLANCE.GOUV.FR

● CNIL – Ateliers et jeux sur la protection des données
○ Propose des kits adaptés à chaque âge (« Tous ensemble, prudence sur Internet ! ») pour les élèves de CE2 à CM2 et les jeunes de 11 à 15 ans.
○ Comprend des jeux, des vidéos, des activités imprimables et des livrets « Incollables® » pour enseigner la protection des données personnelles à travers des défis ludiques.
○ Les enseignant·e·s peuvent les utiliser comme modules pédagogiques ou proposer des ateliers aux parents.
cnil.fr+1CYBERMALVEILLANCE.GOUV.FR+1

● Internet Sans Crainte / Journée pour un Internet plus sûr en France
○ Ateliers annuels Safer Internet Day avec des kits thématiques (par exemple, IA et citoyenneté numérique, jeux d'évasion comme « Vinz et Lou »).
○ Modules prêts à l'emploi pour les cycles 2, 3 et le lycée, conçus pour être utilisés en classe ou lors de sessions animées par des pairs. CYBERMALVEILLANCE.GOUV.FR+3Better Internet for Kids+3Teachit+3

● Promeneurs du Net (PdN) – Mentorat numérique

○ Des professionnel·le·s de la jeunesse s'engagent en ligne pour soutenir les 12-25 ans grâce à une présence en ligne structurée.
○ Les activités comprennent des sessions de chat modérées, des groupes de discussion entre pairs sur les risques numériques, des simulations de jeux de rôle et des sessions de questions-réponses dans des centres pour jeunes ou en ligne. Wikipédia

● CLEMI – Ateliers sur l'éducation aux médias et la pensée critique

○Grâce au réseau géré par le ministère, le CLEMI fournit des plans de cours et des fiches d'information pour l'éducation aux médias, notamment l'analyse des réseaux sociaux, la détection des fausses informations et l'utilisation civique des médias.
○ Les enseignant·e·s mènent des projets tels que des journaux étudiant·e·s ou des exercices de décodage de photos/médias afin de développer des compétences numériques critiques. Wikipédia

● Académie de Créteil – Guide « Forming à la cybersécurité »
○ Brochure de 13 pages destinée aux écoles, couvrant les bases de la cybersécurité, la protection des données, l'identification des tentatives d'hameçonnage et les habitudes sécuritaires à adopter avec les appareils électroniques.
○ Conçu pour le travail en groupe ou les ateliers dans les collèges/lycées.

Better Internet for Kids+2dane.ac-creteil.fr+2Assurance Prévention+2cnil.fr

• Les 8 recommandations de la CNIL – Ateliers pour enfants co-conçus
○ La CNIL a développé et co-créé des ateliers avec des enfants afin d'expliquer des concepts tels que le consentement, le droit à la vie privée et l'autonomie en toute sécurité.
○ Format suggéré : sessions interactives où les adolescent·e·s contribuent à la conception d'interfaces utilisateur ou de messages qu'ils comprennent. cnil.fr

• Kit pédagogique du citoyen numérique (CNIL, Arcom, HADOPI, Défenseur des droits)

Ensemble de supports pédagogiques (vidéos, infographies, diapositives) téléchargeables gratuitement pour enseigner la citoyenneté numérique, couvrant la vie privée, les droits en ligne, la distinction entre les contenus légaux et illégaux et l'éducation aux médias. Idéal pour les animateur·rice·s travaillant avec des migrant·e·s. Portail pédagogique

• ContreLaTraite.org – Centre de ressources
Une vaste base de ressources en ligne (en français) proposant des formations en ligne, des guides, des campagnes et un soutien aux professionnel·le·s, en particulier sur la traite des êtres humains dans des contextes touchant les migrant·e·s. Elle offre un large éventail de supports (formations, outils de prévention, informations sur les campagnes) qui peuvent être adaptés ou utilisés directement dans des programmes axés sur les migrant·e·s. https://contrelatraite.org/centre-ressources

• Ressources de médiation numérique (Les Bases du numérique d'intérêt général)

Une riche base de données contenant des outils et des guides pour accompagner les personnes vulnérables dans le domaine numérique, notamment en matière de cybersécurité, de médiation numérique, de soutien parental et de jeux d'apprentissage multimédia.
https://lesbases.anct.gouv.fr/ressources/ressources-pedagogiques

• Mouvement du Nid – « Y'a quoi dans ma banane ? »

Conçu pour les jeunes de 12 ans et plus, ce sac banane virtuel contient des accessoires (téléphone, clés, cahier, etc.) qui servent d'outils pour apprendre et réfléchir à toute une série de sujets liés à la vie affective et sexuelle, à l'égalité des sexes et à la violence sexiste et sexuelle, y compris la prostitution et l'exploitation sexuelle.
https://dansmabanane.mouvementdunid.org/

• Trousse pour les jeunes – Sécurité en ligne (Canada)

Destinée aux adolescent·e·s (13-14 ans), cette trousse canadienne explique les formes

d'exploitation sexuelle en ligne telles que le sexting, la sextorsion, le capping et le grooming, à l'aide de diapositives, de notes pour le·la présentateur·rice et de conseils pour encourager les victimes à s'exprimer.
Gouvernement du Canada

• Malettes pédagogiques – CVM (Collectif contre la violence du marché sexuel)

Ces « trousses » numériques fournissent aux parents et aux professionnel·le·s des ressources pour lutter contre la prostitution enfantine et la prévenir, notamment des vidéos, des guides et des outils de sensibilisation.
association-cvm.org Droit d'Enfance

○ Exemples d'activités en classe

Tranche d'âge	Activité	Objectif	Format
7 à 11 ans	Création d'une bande dessinée : illustrer les messages sûrs et dangereux	Comprendre la confidentialité et le comportement numérique	Travail en groupe et présentation
11-15 ans	Jeu d'évasion « Get me out of AI » (Vinz et Lou)	Reconnaître les risques liés à l'IA et la citoyenneté numérique	Jeu de rôle
Collège/ Lycée	Atelier sur les fausses informations avec les fiches du CLEMI	Développer l'esprit critique et la maîtrise des médias	Débat en classe et production numérique
Les adolescents en ligne	Session en direct avec les Promeneur·euse·s du Net	Dialogue ouvert sur le cyberharcèlement, la vie privée et le sexting	Chat modéré
Parents et enfants	Quiz familial sur la protection des données de la CNIL	Stimuler la discussion à la maison et à l'école	Brochure/atelier à emporter

Comment utiliser efficacement ces ressources

● Mélangez les formats pédagogiques : combinez vidéos, quiz interactifs, bandes dessinées, discussions de groupe, activités physiques et tâches numériques.

● Créez du contenu en collaboration : laissez les jeunes concevoir leurs propres affiches de sécurité, campagnes médiatiques ou flux UX pour les paramètres de confidentialité, avec l'aide des enseignant·e·s.

● Impliquez les parents : proposez des kits à emporter à la maison ou des ateliers communs (par exemple, des brochures de la CNIL ou des fiches Cyber Guide).

● Faites appel à des pairs mentors : impliquez de jeunes « ambassadeur·rice·s numériques » issu·e·s des équipes PdN ou Safer Internet Day pour animer les sessions.

● Progression : commencez par des concepts simples (par exemple, les bases de la confidentialité à l'école primaire) et passez à des sujets plus complexes, tels que la désinformation et l'IA, au niveau secondaire.

● **Projet BEAWARE** (France, Italie, Grèce, Portugal, Belgique, Chypre) : Comprendre, prévenir, détecter et lutter contre l'exploitation et les abus sexuels en ligne (OSEA) grâce à une approche holistique, multiforme et multisectorielle.**Ressources :**

○ La boîte à outils destinée aux éducateur·rice·s est conçue pour fournir des informations théoriques sur des sujets liés à la sécurité en ligne, aux risques et aux dangers sur les plateformes en ligne. Elle donne également des suggestions pratiques sur la manière de traiter les cas d'abus en ligne et d'interagir avec les jeunes qui les signalent.
○ L'application mobile destinée aux jeunes aborde différents thèmes à travers des défis interactifs. Elle peut également être utilisée en groupe.
○ La plateforme d'apprentissage est un espace en ligne destiné aux animateur·rice·s socio-éducatif·ve·s et aux éducateur·rice·s afin qu'ils et elles acquièrent une meilleure compréhension de la culture numérique sur des thèmes pertinents et qu'ils et elles soient mieux informé·e·s sur la manière d'aborder ces questions lorsqu'ils et elles interagissent avec des jeunes.

● **Projet CESAGRAM** (Belgique, Grèce, Italie, Royaume-Uni, Lituanie) : Améliorer la compréhension du processus de grooming, et plus particulièrement la manière dont il est facilité par la technologie et comment il peut conduire à des abus sexuels sur des enfants et à leur disparition.
Ressources :
○ La bibliothèque dispose d'une multitude de sources pour rechercher et s'informer.
○ Consultation utile pour les parents sur les abus sexuels commis sur des enfants à l'aide de technologies : documents destinés aux parents sur la sécurité en ligne.

○ Cartographie des informations pratiques fournies par des organisations spécialisées sur les lieux où obtenir de l'aide et davantage de connaissances sur le sujet.

4.4 L'impact du secteur privé

Loin d'être des plateformes passives, les entreprises technologiques d'aujourd'hui sont des acteur·rice·s actif·ve·s de la sécurité numérique. Les réseaux sociaux, les applications de messagerie et autres services en ligne sont devenus les premiers défenseur·euse·s contre les cyber-préjudices liés au genre. Leur rôle de gardien·ne n'est pas seulement réglementaire, il est parfois visionnaire. En affinant leurs algorithmes, en améliorant leurs protocoles de modération et en protégeant les données des utilisateur·rice·s, ces entreprises atténuent non seulement les abus, mais les anticipent souvent avant qu'ils ne s'aggravent. L'agilité du secteur privé lui permet de réagir plus rapidement que la législation ne pourrait jamais le faire, en s'adaptant aux menaces émergentes avec précision et à grande échelle.

Concevoir avec empathie et prévoyance
La conception éthique n'est pas seulement une simple exigence, mais aussi un avantage concurrentiel. Les entreprises avant-gardistes intègrent directement des principes sensibles au genre dans leurs cycles de développement de produits. Cela signifie qu'elles créent des fonctionnalités qui découragent le harcèlement, les agressions et le partage non consensuel de données, tout en favorisant l'autonomie et la sécurité des utilisateur·rice·s. Contrairement aux mandats bureaucratiques, ces innovations sont motivées par la réactivité du marché et un désir sincère de servir une base d'utilisateur·rice·s diversifiée. La capacité du secteur privé à itérer rapidement garantit que les considérations éthiques sont fonctionnelles, testées par les utilisateur·rice·s et, par conséquent, efficaces.

La responsabilité comme impératif commercial
La transparence est un impératif fondamental de l'éthique des affaires. Les entreprises technologiques publient de plus en plus souvent des rapports détaillés sur les cas d'abus, les résultats de la modération et les indicateurs de sécurité des utilisateur·rice·s, non pas parce qu'elles y sont contraintes, mais parce que la confiance est leur monnaie d'échange. Les audits éthiques et les examens par des tiers deviennent la norme, renforçant ainsi l'engagement du secteur en faveur des droits fondamentaux. Dans de nombreux cas, les entreprises placent la barre plus haut que ne l'exigent les régulateurs,

prouvant ainsi que la responsabilité peut être une démarche volontaire plutôt qu'une obligation réactive.

Collaboration stratégique avec les acteurs de la société civile et les organisations locales

Les entreprises privées ne travaillent pas de manière isolée. Elles forgent des alliances puissantes avec des ONG et des groupes de défense. Ces partenariats ont conduit au développement d'outils de signalement plus intelligents, de systèmes de soutien plus empathiques pour les victimes et de campagnes de sensibilisation qui trouvent un écho à l'échelle mondiale. Le monde des entreprises apporte son envergure, ses infrastructures et son expertise technique ; la société civile apporte son expérience vécue et sa connaissance du terrain. Ensemble, ils comblent les lacunes en matière de capacités et continuent à construire des cadres entièrement nouveaux pour la sécurité et la sûreté numériques.

De plus, les programmes de formation menés par les ONG aident les développeur·euse·s et les modérateur·rice·s à internaliser la sensibilité au genre ; cependant, ce sont les entreprises elles-mêmes qui investissent dans ces efforts, reconnaissant que les plateformes inclusives sont plus durables et plus rentables. Même dans le domaine de la défense des politiques, le secteur privé n'est plus un participant réticent, mais un allié proactif, qui prête sa voix et ses ressources pour façonner une législation qui reflète la dynamique réelle des technologies numériques.

L'innovation comme bouclier contre l'exploitation

La contribution la plus importante du secteur privé à la sécurité numérique réside dans sa capacité d'innovation. Les outils de modération basés sur l'IA détectent désormais en temps réel les propos injurieux, l'exploitation par le biais d'images et le harcèlement coordonné, ce que les humains ne pourraient pas faire à grande échelle. Ces technologies sont également prédictives : elles apprennent à partir de modèles afin de prévenir les dommages avant qu'ils ne se produisent (et ne se contentent pas de réagir aux actes commis).

La conception axée sur la confidentialité est une autre caractéristique de l'ingéniosité des entreprises. La messagerie directe cryptée de bout en bout, le signalement anonyme et les paramètres de visibilité personnalisables permettent aux utilisateur·rice·s de reprendre le contrôle de leur vie numérique. Il ne s'agit pas là de fonctionnalités marginales, mais de composants essentiels, façonnés par la demande des utilisateur·rice·s et une vision éthique avant-gardiste. En outre, en matière de protection des données, les entreprises sont à la pointe grâce à un cryptage robuste, un accès minimal des tiers et des mesures de protection internes, qui deviennent tous des normes dans le secteur, en particulier lorsqu'il s'agit de données sensibles telles que la santé reproductive ou la localisation.

CONCLUSIONS

5. Conclusions

Dans leur lutte constante pour protéger les femmes **et les personnes vulnérabilisées** contre l'exploitation en ligne, les associations et les groupes de défense des droits se heurtent à un système souvent structurellement mal préparé aux réalités et à l'évolution de la criminalité numérique. Les trafiquant·e·s opèrent avec une certaine impunité au-delà des frontières, profitant de l'absence de législation internationale cohérente et de l'inertie de la coopération judiciaire entre les pays. Alors qu'Internet ne connaît pas de frontières, les systèmes de justice pénale restent essentiellement nationaux et donc lents à communiquer, réticents à collaborer et parfois paralysés par des définitions juridiques incompatibles de la traite, du consentement et des abus numériques.

Pour les femmes **et les personnes ciblées** qui sont prises pour cible, les conséquences sont dévastatrices. Les survivant·e·s doivent attendre longtemps que les tribunaux déterminent leur compétence, que les preuves soient recevables et que les autorités étrangères réagissent. Les associations qui travaillent en leur nom doivent naviguer dans un réseau complexe de formalités administratives, s'appuyant souvent sur des réseaux informels et des relations personnelles pour faire avancer les dossiers. Le manque d'urgence dans la coopération transfrontalière bloque les processus.

À cette complexité s'ajoute le monde opaque des cryptomonnaies. Les trafiquant·e·s utilisent de plus en plus le Bitcoin et d'autres monnaies numériques pour transférer de l'argent de manière anonyme, contournant ainsi les systèmes financiers traditionnels et échappant à la détection. Si la blockchain offre une traçabilité théorique, dans la pratique, les outils nécessaires pour suivre ces traces sont coûteux, hautement techniques et souvent hors de portée des forces de l'ordre. Les cryptomonnaies anonymes, les mixeurs et les échanges décentralisés obscurcissent encore davantage les transactions financières, permettant aux auteur·rice·s de blanchir leurs profits avec un risque minimal.

La sécurité des femmes **et des personnes exposées** en ligne ne peut être une préoccupation secondaire. Elle doit être un pilier central de la gouvernance numérique. Cela implique la mise en place de cadres juridiques internationaux qui accordent la priorité aux populations vulnérables et aux droits humains. Cela signifie investir dans la formation judiciaire transfrontalière, dans des bases de données partagées et dans des protocoles d'intervention rapide. Cela implique également de réglementer les marchés « cryptographiques » avec la même vigilance que celle appliquée à la finance traditionnelle, car lorsque l'argent circule dans l'ombre, l'exploitation des femmes **et de personnes vulnérabilisées** fait de même.

Il ne faut pas oublier que l'exploitation sexuelle en ligne ne se produit pas dans le vide ; elle est profondément ancrée et soutenue par des structures qui tirent profit de l'attention, de l'engagement et du contrôle. Les plateformes de réseaux sociaux et les services numériques sont conçus pour privilégier le profit plutôt que la sécurité, amplifiant souvent les contenus sensationnels, violents ou sexualisés afin de maximiser l'engagement des utilisateur·rice·s. Les industries exploitantes, de la pornographie à la collecte de données, capitalisent sur la marchandisation du corps, de la vie privée et de la vulnérabilité émotionnelle des femmes **et des personnes ciblées**. Dans ce système, les abus sexistes ne sont pas un dysfonctionnement, mais une caractéristique : un sous-produit rentable d'une économie numérique qui privilégie la viralité plutôt que la responsabilité et l'exposition plutôt que le consentement.

Tant que tous ces systèmes n'auront pas évolué, les associations continueront à mener un combat difficile avec des outils limités et une détermination sans faille. Leur travail ne vise pas seulement à rendre justice, mais aussi à redonner leur dignité aux femmes **et aux personnes survivantes** qui ont été victimes d'abus sur Internet, un espace pourtant conçu pour la liberté et la connexion.

BIBLIOGRAPHIE

6. Bibliographie

60 Statistiques sur le temps d'écran des enfants en 2025. (n.d.). *GoStudent.* https://www.gostudent.org/fr-fr/blog/statistiques-temps-ecran-enfants

Acquaviva, M. (15 avril 2022). *Comment signaler un site au contenu illégal ?* La Legge per Tutti. https://www.laleggepertutti.it/539189_come-segnalare-un-sito-dai-contenuti-illegali

Anonymat et protection de l'identité. (28 mai 2025). *eSafetyCommissioner.* https://www.esafety.gov.au/industry/tech-trends-and-challenges/anonymity

Camarda, C. (27 octobre 2023). *La pédopornographie et les délits informatiques commis par des mineurs.* Diritto.net. https://www.diritto.net/pedopornografia/

Carcelén-García, S., Narros-González, M. J., & Galmes-Cerezo, M. (2023). *Vulnérabilité numérique chez les jeunes : genre, âge et modes de participation en ligne.* International Journal of Adolescence and Youth, 28(1). https://doi.org/10.1080/02673843.2023.2287115

Cyber Security Challenge Greece. (n.d.). https://cybersecuritychallenge.gr/2025/

Cyberviolence contre les femmes dans l'UE. (2024). *Parlement européen.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI(2024)767146_EN.pdf

Digiturvalisuse mängud. (n.d.). *Digiturvalisuse Mängud.* https://www.lasteaeg.ee/

En 2023, un tiers des internautes ressentent au moins un effet néfaste des écrans – *Insee Focus – 329.* https://www.insee.fr/fr/statistiques/8199393

FAQ : Violence numérique… (10 février 2025). *ONU Femmes.* https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women

Fournari, J. (9 avril 2025). *Chiffres sur le cyberharcèlement en 2025.* Jedha. https://www.jedha.co/formation-cybersecurite/chiffres-sur-le-cyberharcelement-en-2025

Objectif 5 | Département des affaires économiques et sociales. (s.d.). https://sdgs.un.org/goals/goal5

Centre grec pour un Internet plus sûr. (s.d.). https://better-internet-for-kids.europa.eu/en/sic/greece

Note d'orientation sur la violence sexiste au Guyana – *PANCAP.* https://pancap.org/pancap-documents/guyana-gender-based-violence-policy-brief/

Le Guyana dispose d'un modèle… (22 septembre 2024). *DPI Guyana.* https://dpi.gov.gy/guyana-has-comprehensive-holistic-model-to-address-gender-based-violence/

Comment la violence sexiste facilitée par la technologie… (Novembre 2023). *ONU – UNRIC.* https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/

Commission économique pour l'Amérique latine et les Caraïbes. (s.d.). http://www.cepal.org/

Inspiratsioonikogumik 2023 – *Targalt Internetis.* (16 janvier 2024). https://www.targaltinternetis.ee/inspiratsioonikogumik-2023/

Komal. (27 mars 2025). *L'impact des réseaux sociaux dans la lutte contre la violence sexiste.* IJLSSS. https://ijlsss.com/the-impact-of-social-media-in-combating-gender-based-violence/

L'Hoiry, X., Moretti, A., & Antonopoulos, G. A. (2024). *Traite des êtres humains, exploitation sexuelle et technologies numériques.* https://doi.org/10.1007/s12117-024-09526-4

Marasco, T. (11 mars 2019). *È legale vedere video pornografici su internet ?* La Legge per Tutti. https://www.laleggepertutti.it/104726_e-legale-vedere-video-pornografici-su-internet

Ministère de la Gouvernance numérique. (s.d.). *THE GREEK NATIONAL DIGITAL DECADE STRATEGIC ROADMAP.* https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digital_decade_national_roadmap.pdf

Texila International Journal – Revues en libre accès. (s.d.). http://www.texilajournal.com/

Ourania. (11 octobre 2022). *European SafeOnline Initiative (ESOI).* https://athenslifelonglearning.gr/el/european-safeonline-initiative/

Quayle, E. (2020). *Prévention, perturbation et dissuasion de l'exploitation sexuelle des enfants en ligne.* ERA Forum, 21(3), 429–447. https://doi.org/10.1007/s12027-020-00625-7

Research ICT Africa. (17 février 2025). *L'impact des réseaux sociaux et de l'IA générative sur la violence sexiste.*
https://researchictafrica.net/research/the-impact-of-social-media-and-generative-ai-on-gender-based-violence/

Activités SID 2024 en Estonie. *Better Internet for Kids.*
https://better-internet-for-kids.europa.eu/en/news/safer-internet-day-2024-activities-estonia

SaferInternet4kids. (n.d.).
https://saferinternet4kids.gr/

Santi, P. (1er mai 2024). *Enfants et écrans…* Le Monde.
https://www.lemonde.fr/societe/article/2024/05/01/enfants-et-ecrans-les-constats-qui-ont-nourri-les-preconisations-de-la-commission-nommee-par-macron_6231003_3224.html

Sanusi, T. (17 novembre 2021). *Violence sexiste en ligne.* Global Citizen.
http://globalcitizen.org/en/content/what-is-online-gender-based-violence-2/

ISS Africa. (s.d.). *Social media can change actions that drive gender-based violence.*
https://issafrica.org/iss-today/social-media-can-change-actions-that-drive-gender-based-violence

EIGE. (9 décembre 2024). *Tackling cyber-violence against women and girls.*
https://eige.europa.eu/publications-resources/publications/tackling-cyber-violence-against-women-and-girls-role-digital-platforms

Targalt Internetis. (s.d.).
https://www.targaltinternetis.ee/

UNFPA. (s.d.). *Technology-facilitated gender-based violence.*
https://www.unfpa.org/TFGBV

Commission européenne. (27 octobre 2022). *Digital Services Act.*
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

UNODC. (s.d.). *The role of technology in human trafficking.*
https://www.unodc.org/unodc/en/human-trafficking/Webstories2021/the-role-of-technology-in-human-trafficking.html

Tomczyk, Ł. (2019). *Les compétences en matière de sécurité numérique…*
https://doi.org/10.1007/s10639-019-09980-6

ONU Femmes. (2024). *Référentiel des travaux…*
https://www.unwomen.org/sites/default/files/2024-10/repository-of-un-womens-work-on-technology-facilitated-gender-based-violence-en.pdf

Université de Rhode Island & Hughes, D. (2002). *L'utilisation des nouvelles technologies…* https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1000&context=wms_facpubs

Point de vue sur la culture numérique. (s.d.). https://engagement.fkdp.or.id/index.php/engagement/article/view/1534/217

Westphal, V. (12 avril 2024). *12 % des adolescents déclarent se livrer à du cyberharcèlement.* Santé Mentale. https://www.santementale.fr/2024/04/un-jeune-sur-6-victime-de-cyberharcelement

UNICEF. (2023). *What we know about the gender digital divide.* https://www.unicef.org/eap/media/8311/file/What%20we%20know%20about%20the%20gender%20digital%20divide

Women's Media Center. (n.d.). *Why online anonymity is critical for women.* https://womensmediacenter.com/speech-project/why-online-anonymity-is-critical-for-women

Better Internet for Kids. (s.d.). *Back to School Greece – Digital Citizenship.* https://better-internet-for-kids.europa.eu/en/news/back-school-greece-focus-digital-citizenshi

End Exploitation https://endexploits.com/statistics.html

Statista https://www.statista.com/statistics/1339631/onlyfans-reports-to-national-center-missing-exploitedchildren-csam-material/

New York Post (13/03/2024) The https://nypost.com/2024/03/13/us-news/behind-the-onlyfans-porn-boom-insideallegations-of-rape-abuse-and-betrayal/

The Guardian (30/08/2025) https://www.theguardian.com/society/2025/aug/30/uk-anti-slaverycommissioner-launches-investigation-into-pimping-websites

Wired (18/08/2025) https://www.wired.com/story/is-roblox-getting-worse/

Visitez la Bibliothéque de Mémoire

sur YouTube @WeLensProject

Welens

MADRES VICTIMAS DE TRATA
desaparecidas para ser prostituidas

KEMEA

élan interculturel

D'AILLEURS & D'ANTILLES

NOGAP
WHAT'S NORMAL?

cesie
the world is only one creature

beecom

femLENS

Cofinancé par l'Union européenne

Financé par l'Union européenne. Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables.