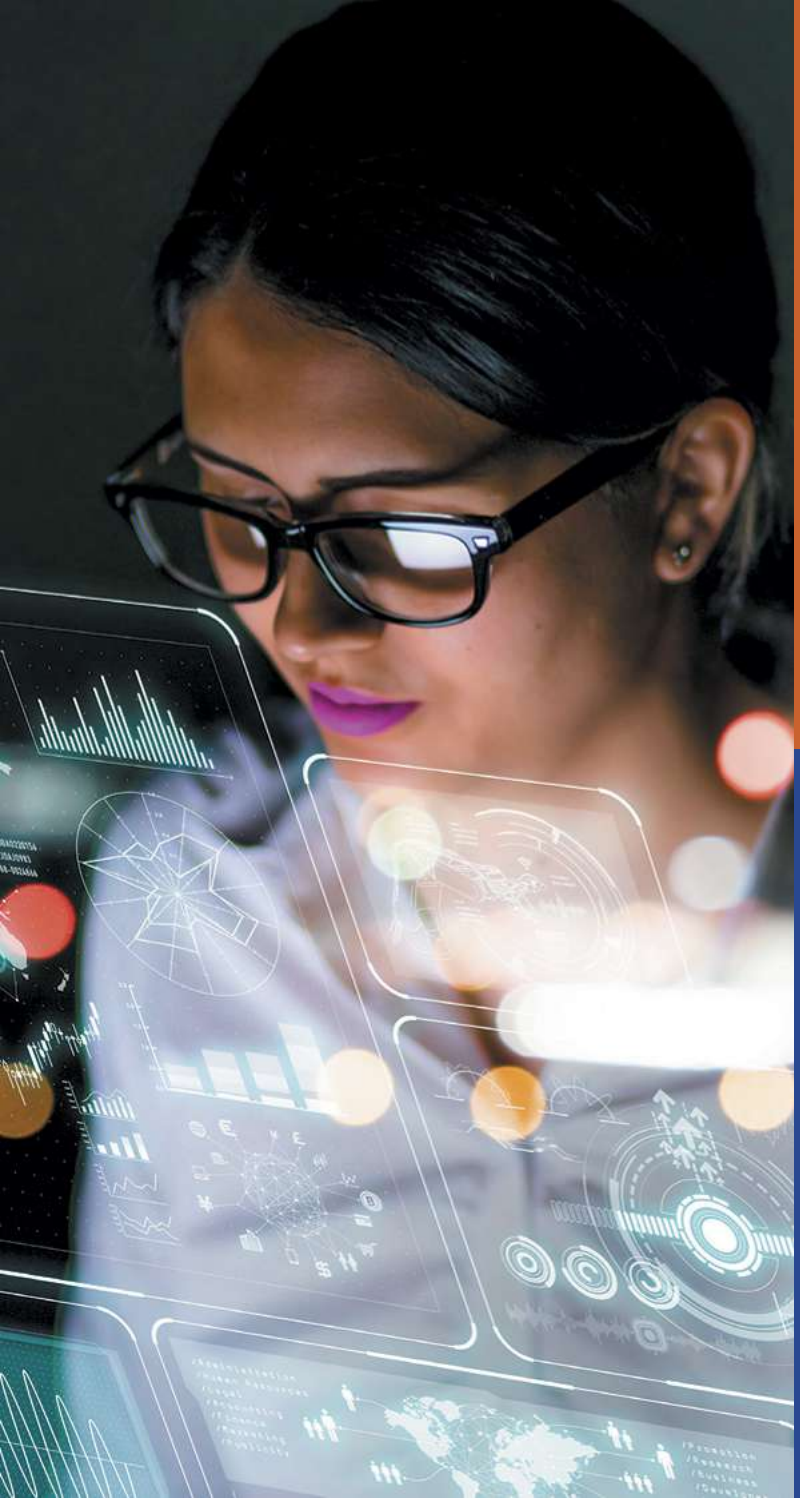


PROTÉGER LES FEMMES ET LES FILLES CONTRE LA VIOLENCE À L'ÈRE DU NUMÉRIQUE

La pertinence de la Convention d'Istanbul et de la Convention de Budapest sur la cybercriminalité pour la lutte contre la violence à l'égard des femmes en ligne et facilitée par la technologie

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PROTÉGER LES FEMMES ET LES FILLES CONTRE LA VIOLENCE À L'ÈRE DU NUMÉRIQUE

La pertinence de la Convention d'Istanbul et de la Convention de Budapest sur la cybercriminalité pour la lutte contre la violence à l'égard des femmes en ligne et facilitée par la technologie

Décembre 2021

Adriane van der Wilk

Conseil de l'Europe

Conception de la couverture et mise en page : Division de la production des documents et des publications (DPDP), Conseil de l'Europe
Photo: Shutterstock

Cette publication n'a pas fait l'objet d'une relecture typographique et grammaticale de l'Unité éditoriale du SPDP.

Imprimé aux ateliers du Conseil de l'Europe

TABLE DES MATIÈRES

RÉSUMÉ

La présente étude examine dans quelle mesure deux traités internationaux, la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (Convention d'Istanbul) et la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), peuvent contribuer à la lutte contre la violence à l'égard des femmes en ligne et facilitée par la technologie grâce à des politiques coordonnées, à la prévention, à la protection, aux poursuites et à la coopération internationale.

La violence à l'égard des femmes en ligne et facilitée par la technologie s'inscrit dans le continuum des multiples formes de violence à l'égard des femmes qui ont lieu hors ligne. La plupart des formes de violence à l'égard des femmes en ligne et facilitée par la technologie correspondent à des comportements qui constituent déjà des infractions mais qui se répandent, s'amplifient ou se généralisent du fait de l'utilisation d'internet. Malgré leur grave incidence sur les victimes et sur la société au sens large, l'impunité demeure la règle plutôt que l'exception.

La Convention d'Istanbul, qui englobe toutes les formes de violence à l'égard des femmes et de violence domestique, est, en la matière, le plus ambitieux des traités juridiquement contraignants relatifs aux droits humains. Elle peut donc être un instrument particulièrement utile pour lutter contre la violence à l'égard des femmes en ligne et facilitée par la technologie. La Convention de Budapest, quant à elle, est le traité international juridiquement contraignant le plus pertinent dans le domaine de la cybercriminalité et de preuves électroniques. Elle prévoit la possibilité de mener des poursuites contre la violence à l'égard des femmes en ligne et facilitée par la technologie.

La présente étude classe et définit les différentes formes de violence à l'égard des femmes en ligne et facilitée par la technologie. Elle s'intéresse plus particulièrement aux articles 33, 34 et 40 de la Convention d'Istanbul, ainsi qu'aux dispositions pertinentes de la Convention de Budapest. Elle analyse aussi les dispositions de la Convention d'Istanbul sur les politiques intégrées, la prévention, la protection et les poursuites et fournit des commentaires sur leur application en ce qui concerne les divers aspects du phénomène de la violence à l'égard des femmes en ligne et facilitée par la technologie.

Cette étude avance que la Convention d'Istanbul et la Convention de Budapest peuvent se complémenter de manière dynamique : la Convention d'Istanbul puise sa force dans le fait qu'elle reconnaît la violence à l'égard des femmes comme étant une violence qui affecte les femmes parce qu'elles sont des femmes. La Convention de Budapest met à disposition un large éventail de moyens en matière d'enquête et d'obtention des preuves électroniques relatives aux infractions commises en ligne et par le biais des nouvelles technologies ainsi que pour toute autre infraction impliquant des preuves électroniques.

Néanmoins, le domaine de la cybercriminalité est, à ce jour, encore largement neutre du point de vue du genre, dans la mesure où les infractions commises contre les femmes en ligne ne sont pas conceptualisées dans les cadres de la cybercriminalité. Bien que certains efforts soient déployés pour accorder une place centrale à la notion d'égalité entre les femmes et les hommes, le vaste champ d'application et l'approche globale de la Convention d'Istanbul peuvent ainsi constituer à la fois un outil essentiel pour démultiplier ces efforts et la base d'une reconnaissance plus systématique de l'exposition des femmes à la violence dans le domaine de la cybercriminalité.

INTRODUCTION

Avec l'augmentation constante des taux d'accès à internet dans le monde et l'utilisation accrue des technologies numériques, la violence à l'égard des femmes revêt de nouvelles formes. Les actes de violence physique, sexuelle et psychologique commis hors ligne, y compris dans la rue, à la maison ou sur le lieu de travail, sont répétés, amplifiés, propagés et aggravés par les technologies de l'information et de la communication (TIC). De nouvelles formes de violence font également leur apparition. La violence à l'égard des femmes affecte les femmes à cause de leur genre et de leurs identités croisées. Elle fait partie d'un continuum qui se déploie, se reflète et prend de l'ampleur en ligne (Kelly 1988).

La violence à l'égard des femmes en ligne et facilitée par la technologie est exercée sur différentes plateformes et au moyen d'une multitude d'outils, à la fois publiquement accessibles et privés, tels que les réseaux sociaux, les applications de messagerie privée, les courriers électroniques, les applications de rencontre, les forums, les rubriques commentaires des médias , les jeux vidéo ou les plateformes de visioconférence. La violence étant souvent visible de tous et partagée sans limites par différents moyens, les victimes se trouvent constamment revictimisées. Ces formes de violence sont souvent déployées dans plusieurs pays, sans que se pose la question de la responsabilité des intermédiaires et des auteurs. Par conséquent, le phénomène et ses effets sont difficiles à saisir, et les auteurs bénéficient d'une impunité apparente, tandis que les victimes se sentent impuissantes et seules à chaque étape de leur victimisation. La cyberviolence a de graves répercussions sur la vie des femmes et des personnes qu'elles ont à leur charge, ainsi que sur leur santé physique et psychologique, leurs moyens de subsistance, leur réputation, leur participation à la vie politique et leur présence en ligne.

Bien que de plus en plus d'ouvrages documentent ces répercussions, la grande majorité des infractions restent impunies. La présente étude a pour objectif d'examiner dans quelle mesure deux traités du Conseil de l'Europe, la Convention d'Istanbul et la Convention de Budapest, peuvent contribuer à la lutte contre la violence à l'égard des femmes en ligne et facilitée par la technologie grâce à des politiques intégrées, à la prévention, à la protection, aux poursuites et à la coopération internationale.

La Convention d'Istanbul est le premier instrument juridiquement contraignant en Europe à établir un cadre complet pour mettre fin à la violence à l'égard des femmes et à la violence domestique, et représente le traité le plus ambitieux en matière de lutte contre les violences faites aux femmes. C'est un texte historique en matière de droits humains, qui couvre toutes les formes de violence à l'égard des femmes. La convention reconnaît la nature structurelle de la violence à l'égard des femmes en tant que violence fondée sur le genre et réaffirme que les femmes sont exposées à un risque plus élevé de violence fondée sur le genre que ne le sont les hommes. Elle s'applique donc à toutes les formes de violence à l'égard des femmes et de violence domestique et vise à protéger les femmes, à prévenir la violence à leur égard et la violence domestique, à poursuivre les auteurs de violences et à éliminer ce fléau.

Les Parties à la convention sont tenues d'intégrer la convention dans leur législation nationale afin de protéger les femmes, de prévenir la violence dirigée contre elles et de poursuivre comme il se doit les auteurs de ce type de violence. GREVIO – le Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique, organe spécialisé indépendant chargé de contrôler la mise en œuvre de la Convention d'Istanbul – et le Comité des Parties garantissent tous deux l'application effective de la convention, grâce à des rapports d'évaluation, des recommandations aux États parties et une action de suivi.

La Convention du Conseil de l'Europe sur la cybercriminalité (la Convention de Budapest ; Conseil de l'Europe 2011a) est un traité juridiquement contraignant axé sur la cybercriminalité et les preuves électroniques. Elle fait obligation aux Parties d'ériger en infraction pénale des comportements qui portent préjudice à des données ou à des systèmes informatiques ou qui impliquent l'utilisation de tels systèmes, y compris des comportements relatifs à la production, à la diffusion ou à la possession de pornographie enfantine[1], ainsi que des atteintes à la propriété intellectuelle et aux droits connexes. Les Parties à la convention sont également tenues d'instaurer des pouvoirs et des procédures liés à l'obtention de preuves électroniques aux fins d'enquêtes pénales spécifiques, non seulement pour les infractions précitées mais aussi pour toute infraction dont il existe des preuves sous forme électronique, et de faciliter effectivement la coopération internationale et l'entraide judiciaire dans le cadre des enquêtes ou des procédures pénales concernant ces infractions. La Convention de Budapest est complétée par un protocole additionel relatif aux actes racistes et xénophobes commis par le biais de systèmes

1. Un glossaire est disponible à la fin du document.

informatiques (Conseil de l'Europe 2003). Le Comité de la Convention sur la cybercriminalité (T-CY) assure la mise en œuvre effective de la convention et de son protocole additionnel.

Les Conventions d'Istanbul et de Budapest peuvent se compléter pour lutter de manière plus effective et plus efficiente contre la violence à l'égard des femmes en ligne et facilitée par la technologie dans les États parties. La présente étude vise à analyser et évaluer les protections offertes aux victimes par les deux instruments et à déterminer leur portée et leur possible complémentarité dans le cas de certaines formes de violence à l'égard des femmes en ligne et facilitée par la technologie[2].

Dans la première partie, cette étude définit le phénomène de la violence à l'égard des femmes en ligne et facilitée par la technologie, examine les différentes formes de violence et les caractéristiques de la victimisation et met en avant les nombreuses difficultés auxquelles les victimes font face sur le chemin de la réparation. La deuxième partie de l'étude présente la Convention d'Istanbul, son champ d'application et son fonctionnement. Dans la troisième partie, la Convention de Budapest sur la cybercriminalité sera présentée, ainsi que les normes qui s'y rapportent et le fonctionnement de son comité de suivi. La quatrième partie présente le cadre normatif général des instruments régionaux et internationaux qui couvrent – partiellement – certaines de ces formes de violence spécifiques. La cinquième partie s'attache à classer et à définir les différentes formes de violence à l'égard des femmes en ligne et facilitée par la technologie, en se référant aux articles 33, 34 et 40 de la Convention d'Istanbul, complétés, le cas échéant, par des dispositions de la Convention de Budapest. La sixième partie de cette étude vise à déterminer si, et comment, les normes juridiques existantes de la Convention d'Istanbul sur les politiques intégrées, la prévention, la protection et les poursuites peuvent être utilisées pour lutter contre la violence à l'égard des femmes en ligne et facilitée par la technologie. Les dispositions complémentaires de la Convention de Budapest sont analysées en parallèle. En conclusion, une série de recommandations sont formulées. Dans les annexes figurent deux discussions sur des formes de violence spécifiques, ainsi qu'un glossaire.

En ce qui concerne la violence contre les enfants en ligne et facilitée par les nouvelles technologies, et la traite des êtres humains aux fins d'exploitation sexuelle facilitée par la technologie, la présente étude adopte la même approche que la Convention d'Istanbul :

> Les rédacteurs ont décidé que cette convention devrait éviter de couvrir les mêmes comportements que d'autres conventions du Conseil de l'Europe couvrent déjà, en particulier la Convention sur la lutte contre la traite des êtres humains (STCE n° 197) et la Convention sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201).

Ainsi, nous ne nous intéresserons pas ici à ces formes de violence, qui mériteraient à elles seules déjà une étude. Il serait cependant nécessaire d'approfondir les recherches sur les liens entre la violence à l'égard des femmes, l'exploitation et les abus en ligne contre des enfants, et la traite des êtres humains aux fins d'exploitation sexuelle, trois phénomènes qui sont amplifiés par les nouvelles technologies, qui relèvent à de nombreux égards du même continuum de violences contre les femmes et les filles et qui sont tous trois imputables aux structures patriarcales (European Women's Lobby 2017). Parmi les ressources du Conseil de l'Europe relatives à ces sujets figurent une déclaration récente du président du Comité de Lanzarote, « Le renforcement de la protection des enfants contre l'exploitation et les abus sexuels en temps de pandémie de Covid-19 » (Conseil de l'Europe 2020d), le projet « Mettre fin à l'exploitation et aux abus sexuels des enfants en ligne EndOCSEA@ Europe », mis en œuvre par la Division des droits des enfants du Conseil de l'Europe, en coopération avec le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC), et des ressources sur la dimension numérique de la traite des êtres humains (Conseil de l'Europe 2007) ainsi que l'étude à venir sur la traite des êtres humains en ligne et facilitée par les technologies.

En outre, il convient de noter que cette étude suit une approche centrée sur les victimes et que, bien que soient abordées des questions cruciales comme la protection des données, le respect de la vie privée, la surveillance, le modèle économique axé sur la publicité et la responsabilité des sociétés internet, ces aspects interdépendants ne sont pas au cœur de l'étude.

L'objectif de la présente étude est en définitive de montrer comment les victimes de la violence à l'égard des femmes en ligne et facilitée par la technologie pourraient bénéficier des protections juridiques existantes que les Parties aux deux conventions sont tenues de garantir aux personnes qui relèvent de leur juridiction.

2. Voir également Conseil de l'Europe 2018c ; l'Étude cartographique sur la cyberviolence du T-CY qui examine les réponses internationales au titre de la Convention de Budapest et d'autres traités, notamment la Convention d'Istanbul.

CHAPITRE I

DÉFINIR LA VIOLENCE À L'ÉGARD DES FEMMES EN LIGNE ET FACILITÉE PAR LA TECHNOLOGIE

Le phénomène : quoi, comment et où ?

Pour mieux comprendre comment prévenir chaque forme de violence à l'égard des femmes et des filles, comment mieux protéger les victimes et comment poursuivre les auteurs, il est essentiel de définir le phénomène. Dans cette première partie, nous examinerons comment et pourquoi la violence à l'égard des femmes en ligne et facilitée par la technologie constitue un ensemble de formes de violence très spécifiques dont l'impact sur les victimes est important.

La violence à l'égard des femmes en ligne et facilitée par la technologie fait partie de l'éventail des formes de violence à l'égard des femmes exercées hors ligne. La plupart des formes de violence à l'égard des femmes en ligne et facilitée par la technologie correspondent à des comportements qui constituent déjà des infractions mais qui se répandent, s'amplifient ou se généralisent du fait de l'utilisation d'internet et des technologies numériques, par exemple dans le cas de la violence domestique :

> Le (t)rolling, les insultes, la sextorsion, le partage non consenti d'images intimes, la manipulation de photos, le cyberharcèlement, le doxing, le piratage, les atteintes à la propriété intellectuelle et les attaques DDOS se produisent exclusivement en ligne ; ces formes de violence peuvent également être exercées en lien avec des événements hors ligne, et elles ont presque toujours des répercussions à la fois en ligne et hors ligne (Ging and Siapera 2018).

Certains types de violence, toutefois, sont aussi spécifiques aux plateformes et outils numériques, en particulier du fait de leur impact et de leur permanence et en raison du nombre d'auteurs impliqués ; ils sont « liés aux possibilités technologiques des nouveaux médias, à la politique algorithmique de certaines plateformes, aux cultures professionnelles qui créent ces technologies, et aux personnes et communautés qui les utilisent » (ibid.).

La violence à l'égard des femmes en ligne et facilitée par la technologie existe sur une multitude de plateformes : principalement les médias sociaux et leurs innombrables fonctionnalités et espaces, mais aussi les pages web et les forums, les moteurs de recherche, les applications de messagerie, les blogs, les applications et les sites de rencontre, les rubriques commentaires des médias, les groupes de discussion des jeux vidéo en ligne, les plateformes de streaming, les applications de jeux vidéo, les outils de réalité augmentée et virtuelle, les applications de discussion, les outils de visioconférence, les applications et les sites internet professionnels, etc.

> La violence facilitée par la technologie est invasive et omniprésente. Elle ne se limite pas à une seule sphère (...) En tout état de cause, la division public/privé, si elle existe, peut être rendue encore plus floue par la technologie. L'« effondrement du contexte » entre ces zones (professionnelle/personnelle) (...) fait qu'il est difficile, voire impossible, de faire la distinction entre le type de violence et le domaine dans lequel cette violence est exercée (Harris 2020b).

Formes de violence à l'égard des femmes facilitée par la technologie

Les formes de violence à l'égard des femmes facilitée par la technologie comprennent, entre autres :

1. Le harcèlement sexuel en ligne (y compris le cyber flashing – ou l'envoi de photos à caractère sexuel non sollicitées – les commentaires à caractère sexuel, la diffamation à caractère sexuel, la calomnie à caractère sexuel, l'usurpation d'identité à des fins sexuelles, le doxing, mais aussi le trolling, le flaming et les agressions de masse à caractère sexuel et fondées sur le genre), le harcèlement sexuel sur la base d'images comme les creepshots (des images sexuellement suggestives ou intimes prises sans consentement et partagées en ligne), l'upskirting (des photos sexuelles ou intimes prises sous la jupe ou la robe d'une femme à son insu et partagées en ligne), les abus sexuels basés sur des images (le partage non consenti de vidéos ou de photos, ou le partage non consenti d'images intimes ou « revenge porn »), les deepfakes, les viols et les agressions sexuelles enregistrés, y compris le « vidéolynchage » (diffusion en direct ou sur des sites pornographiques), les menaces et la contrainte comme le sexting forcé, la sextorsion, les menaces de viol ou l'incitation à commettre un viol.
2. Les formes de traque en ligne, la surveillance ou l'espionnage sur les réseaux sociaux ou les boîtes de messagerie, le vol de mots de passe, les dispositifs de craquage ou de piratage, l'installation de logiciels espions, l'usurpation d'identité à des fins de traque, la surveillance par GPS ou géolocalisation, la peur, les menaces et le contrôle grâce à des systèmes de verrouillage intelligent ou à la domotique.
3. Les formes de violence psychologique comme le discours de haine sexiste en ligne et l'incitation à l'automutilation ou au suicide, les agressions verbales, les insultes, les menaces de mort, les pressions, le chantage ou le morinommage (le fait de révéler le prénom de naissance d'une personne contre sa volonté pour la blesser).

Plan International a récemment publié un rapport sur la violence à l'égard des filles en ligne qui révèle que « les propos injurieux et insultants constituent la forme d'agression la plus fréquente, signalée par 59 % des filles qui ont été harcelées, suivie par le fait de créer volontairement une gêne (41 %), le « body shaming » et les menaces de violence sexuelle (39 % dans les deux cas) (Plan International 2020) ».

Caractéristiques de la victimisation

Les filles constituent un groupe vulnérable. Elles sont touchées par les formes spécifiques de la violence en ligne et facilitée par la technologie visant les mineurs et ayant des particularités liées au genre. Il est important de préciser que les femmes qui présentent des identités intersectionnelles, telles que les lesbiennes, les femmes bi, queer et trans, les femmes de couleur, les migrantes, les femmes en situation de handicap ou atteintes d'une maladie chronique, les femmes dans des contextes spécifiques comme les femmes en situation de violence domestique ou de pauvreté, mais aussi les femmes ayant une image publique, comme les femmes politiques, les journalistes, les défenseuses des droits des femmes ou les militantes, sont davantage exposées au risque de ce type de violence : selon une étude menée par le Conseil de l'Europe en 2017 (Conseil de l'Europe 2017a), 53 % des journalistes européennes ont fait l'objet de cyberharcèlement. Au sein de l'UE, au moins 58,2 % des députées ont été la cible d'attaques sexistes en ligne sur les réseaux sociaux (IPU 2018).

Selon le rapport de Plan International cité dans le paragraphe précédent :

> Plus d'un tiers (37 %) des filles issues d'une minorité ethnique et ayant fait l'objet d'abus déclarent avoir été ciblées en raison de leur race ou de leur origine ethnique, tandis que plus de la moitié (56 %) de celles qui s'identifient comme LBTQI déclarent avoir été harcelées en raison de leur identité de genre ou de leur orientation sexuelle.

La victimisation par ces types de violence fondée sur le genre en ligne et facilitée par la technologie présente plusieurs caractéristiques.

1. La première caractéristique est l'existence ou l'inexistence d'une relation, et le type de relation, entre la victime et l'auteur. À titre d'exemple, une étude britannique de 2011 a montré que plus de la moitié (54 %)

des personnes interrogées avaient rencontré leur agresseur (en ligne) pour la première fois dans la vie réelle (Maple, Shart and Brown 2011). Depuis le début de la pandémie de Covid-19, il semblerait que les abus contre les femmes soient plus souvent commis par des inconnus parce que les femmes interagissent davantage en ligne : une étude menée pendant la pandémie par Glitch UK et End Violence Against Women indique que « 84 % des personnes interrogées ont fait l'objet d'abus par des personnes qu'elles ne connaissaient pas avant le ou les incidents, 16 % ont fait l'objet d'abus par une connaissance et 10 % par un partenaire ou un ancien partenaire… 9 % des personnes ont fait l'objet d'abus par un collègue ou un supérieur (Glitch and End Violence against Women 2020) ».

2. La deuxième caractéristique est le nombre de plateformes et d'outils utilisés pour commettre les abus. La plupart des formes de violence sont exercées sur plusieurs plateformes, à la fois publiques et privées, et ont lieu simultanément sur toutes ces plateformes ou sont commises grâce à différents outils. Une victime peut faire l'objet d'abus sur l'ensemble de ses médias sociaux et plateformes de messagerie en même temps, mais aussi par courriel, puis hors ligne, par téléphone ou par de vrais agresseurs à son domicile, au travail, etc. La récente loi française contre les violences sexuelles et sexistes énonce, par exemple, que les « agressions de masse » (en réunion) sont un comportement typique. Elle tient compte également de l'aspect répétitif du harcèlement, de la multiplicité des lieux où il peut se produire et du fait que plusieurs auteurs peuvent harceler la même victime en même temps (Legifrance 2018).

3. En effet, la troisième caractéristique de ces types de violence est le nombre et le profil des auteurs. Certains types de violence à l'égard des femmes en ligne et facilitée par la technologie sont perpétrés par plusieurs auteurs en même temps, comme les agressions de masse, l'intimidation en ligne (dans le cas des enfants) ou le harcèlement sexuel par tout un groupe ou toute une communauté[3]. Le partage non consenti d'images est également facilité par des dizaines, des centaines ou parfois des milliers de personnes. Le comportement de « l'effet de meute » est une particularité des médias sociaux, étant donné que les auteurs se cachent derrière des profils anonymes, ont un sentiment d'impunité et se sentent soutenus par leur communauté ou, s'ils postent sous leur vrai nom, ne font pas le lien entre la personne qu'ils agressent et une vraie personne. En favorisant l'engagement et la croissance avant tout, les conceptions algorithmiques permettent la formation de meutes. Malgré les efforts déployés pour identifier les propos et contenus visuels injurieux, des contenus extrêmes, voire violents, sont mis en avant par les algorithmes, ce qui permet la polarisation. En outre, « cet effet peut être amplifié grâce à des fonctionnalités qui associent les abus, comme les hashtags qui regroupent des cas disparates de misogynie et les transforment ainsi en une véritable campagne (Harris and Megarry 2014) ». Zarizana Abdul Aziz, directrice du Due Diligence Project, fait une distinction entre les auteurs primaires et les auteurs secondaires. Les auteurs primaires mettent en ligne les contenus injurieux et les auteurs secondaires diffusent les contenus (Abdul Aziz 2017).

4. La quatrième caractéristique de la violence à l'égard des femmes en ligne et facilitée par la technologie est l'incidence de la violence en ligne. Combien de temps ont duré les abus, quelle était leur fréquence, quelle est la permanence des données préjudiciables ? La plupart des abus basés sur des images présentent un risque de revictimisation sans fin, étant donné que les images sont partagées par des milliers de comptes, partout en ligne. En effet, les formes de violence en ligne les plus courantes se caractérisent par un aspect répétitif et la permanence des contenus préjudiciables.

5. De plus, en raison de l'incidence et de la permanence, l'impact sur la vie des victimes est considérable. Elles peuvent être effrayées à vie par l'ampleur de la violence. Ces formes de violence ont des répercussions sur leur famille, leurs enfants, leur emploi, leurs relations, leur santé mentale et physique et, enfin, sur leur espérance de vie. Selon une récente étude de l'UE sur le phénomène, le coût global du cyberharcèlement et de la cyberintimidation à l'égard des femmes représenterait chaque année entre 49 milliards et 89,3 milliards d'euros de frais en matière de santé, de justice et d'emploi et coût lié à une qualité de vie réduite (European Parliamentary Research Service 2021).

Difficultés pour les victimes

En outre, les victimes font face à plusieurs niveaux de difficultés dans leur quête de réparation.

1. Il est souvent difficile d'identifier la forme de violence, dans la mesure où la plupart des formes de violence en ligne ne sont pas clairement définies sur le plan juridique et que de nombreuses formes comportent des éléments communs. La plupart des plateformes de réseaux sociaux mettent à la disposition de leurs

3. Voir, par exemple, le GamerGate, une campagne de harcèlement en ligne contre une conceptrice de jeux vidéo, incluant le doxing, la diffusion non consensuelle d'images privées, des menaces de viol et de mort.

utilisateurs des définitions très limitées. Elles mentionnent rarement les lois, et les informations relatives au signalement d'abus sont rares et incomplètes. De plus, les pages concernant le signalement manquent très souvent d'une perspective croisée sur les types de violence.

2. Il est essentiel de documenter les violences. Cependant, la majorité des victimes ne savent pas qu'elles ont la possibilité et, dans la plupart des cas, l'obligation, de garder trace des contenus injurieux (si elles y ont accès) dans le but d'engager des poursuites. De plus, les preuves peuvent disparaître, être effacées par les auteurs ou ne pas être connues des victimes. Elles peuvent également être stockées par les auteurs sur le cloud, dans d'autres pays ou sur des dispositifs déconnectés privés. Le fait de garder une trace du plus grand nombre de preuves possible peut permettre de poursuivre les auteurs des abus.

3. En général, les victimes de violence à l'égard des femmes fondée sur le genre ont beaucoup de difficulté à déposer plainte. Dans des cas de la violence à l'égard des femmes en ligne et facilitée par la technologie, il leur est difficile d'être entendues et crues par les agents des services répressifs dans de nombreux pays. Au sein d'un même pays, si les femmes ont effectivement la possibilité de porter plainte dans certaines régions, cela peut en revanche être plus aléatoire en zone rurale. La plupart des agents des services répressifs ne sont pas formés à identifier les différents types de violence affectant les femmes en ligne et beaucoup d'entre eux ne savent pas comment gérer ces procédures. Ce manque de formation a un effet sur la capacité des femmes à déposer plainte correctement. De plus, lors du traitement de la plainte, la victime se voit souvent reprocher les faits. Un avocat explique que « ce n'est pas le rôle du policier d'un commissariat de quartier de prendre une plainte pour abus sexuel basé sur des images, le soir à 23 heures[4] ». Par ailleurs, seules certaines forces de police peuvent avoir le droit d'enquêter sur ces infractions, et les victimes ne savent donc tout simplement pas auprès de quelles unités elles doivent porter plainte (Conseil de l'Europe 2018c).

4. Le travail d'enquête relatif à ce type d'affaire est colossal. Le même avocat souligne que « les signalements et les messages sont très nombreux, que l'identification des personnes demande du temps et que l'obtention d'informations auprès des fournisseurs de services exige beaucoup de ressources. Lorsqu'il n'y a qu'un seul auteur, c'est gérable, mais cela devient impossible s'il y en a 500, voire 3 000. Il faut en effet demander des informations sur chacun d'entre eux aux fournisseurs de services. Faute d'enquêteur spécialement chargé de cette tâche, et particulièrement motivé, personne ne fera le travail ; or, ces affaires requièrent une enquête préliminaire solide[5] ». De plus, alors que les preuves des infractions sont de plus en plus stockées sur des serveurs hébergés dans des juridictions étrangères, multiples, fluctuantes ou inconnues, autrement dit dans le cloud, les pouvoirs des services répressifs sont, quant à eux, limités par les frontières territoriales. La coopération internationale est par conséquent primordiale.

5. À ce jour, rares sont les lois qui englobent toutes les formes d'abus subis par les femmes en ligne, et les sanctions, lorsqu'elles sont appliquées, risquent de ne pas prendre en compte ni l'impact de la violence sur la vie des victimes ni la composante de genre d'une infraction commise en ligne ou par le biais de la technologie. Le Secrétariat de la Convention de Budapest va jusqu'à affirmer que seuls 1 % des cas de cybercriminalité sont signalés aux services répressifs, et que, parmi les signalements, moins de 1 % aboutissent réellement à une réponse de la justice pénale. Une très faible part des actes de cybercriminalité est donc en réalité sanctionnée[6].

6. La tendance à culpabiliser les victimes et la normalisation de la violence dans les médias et dans l'ensemble de la société, qui nuisent à la compréhension et à l'incrimination de toutes les formes de violence à l'égard des femmes fondée sur le genre, se manifestent également dans le cas de la violence à l'égard des femmes en ligne et facilitée par la technologie : « Faute de programmes de soutien et de mises en garde contre la culpabilisation de la victime, les victimes de revenge porn risquent d'éprouver des niveaux élevés de détresse émotionnelle lorsqu'elles essaient de faire face à la situation. Certaines victimes de revenge porn déclarent même avoir été blâmées par des policiers et s'être vu refuser leur aide parce qu'ils considéraient que l'incident était de la faute de la victime (Citron et Franks 2014 ; Wolak et Finkelhor 2016). Il en va de même pour les victimes de viol, à qui l'on reproche parfois leur victimisation malgré une formation spécialisée au sein de la police (Sleath et Bull 2012). Il est donc important de tenir compte de l'influence des reproches faits aux victimes pour les victimes de cette nouvelle infraction qu'est le revenge porn (Tegan, Starr and Lavis 2018) ».

4. Entretien avec Maître Frety, avocat, septembre 2020, disponible sur : https://www.frety-avocats.fr/
5. Entretien avec Maître Frety, avocat, septembre 2020, https://www.frety-avocats.fr/
6. Entretien avec Alexander Seger, chef de la division Cybercriminalité et Secrétaire exécutif du Comité de la Convention sur la cybercriminalité, septembre 2020.

CHAPITRE II

LA CONVENTION D'ISTANBUL ET LA VIOLENCE À L'ÉGARD DES FEMMES EN LIGNE ET FACILITÉE PAR LA TECHNOLOGIE

La Convention d'Istanbul et son rapport explicatif ont été adoptés par le Comité des Ministres du Conseil de l'Europe le 7 avril 2011. Elle a été ouverte à la signature le 11 mai 2011 à l'occasion de la 121e session du Comité des ministres à Istanbul. Elle est entrée en vigueur le 1er août 2014 et, au mois d'octobre 2021, trente-quatre États sont Parties à la convention. La convention est ouverte à l'adhésion de tout pays prêt à mettre en œuvre ses dispositions.

Traité historique pour les droits des femmes, la Convention d'Istanbul offre aux gouvernements l'ensemble de mesures le plus complet pour prévenir et combattre toutes les formes de violence à l'égard des femmes et la violence domestique. Elle définit ce type de violence comme une violation des droits humains et une forme de discrimination contre les femmes, et associe clairement son élimination à la réalisation de l'égalité entre les femmes et les hommes. Dans son préambule (Conseil de l'Europe 2011a) , la convention rappelle la Convention européenne des droits de l'homme et des libertés fondamentales, la Charte sociale européenne et la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains, ainsi que la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.

La Convention d'Istanbul rappelle également la Convention des Nations Unies sur l'élimination de toutes les formes de discrimination à l'égard des femmes (CEDAW) et ses recommandations générales ultérieures, la Convention des Nations Unies relative aux droits de l'enfant et la Convention des Nations Unies relative aux droits des personnes handicapées.

Le texte réaffirme la nature structurelle et fondée sur le genre de la violence à l'égard des femmes et établit un cadre global pour mettre fin à la violence à l'égard des femmes et la violence domestique. La convention s'articule autour des « 4 P » : Prévention, Protection et soutien des victimes, Poursuite des auteurs et Politiques coordonnées (Conseil de l'Europe 2020c).

Champ d'application

En ce qui concerne son champ d'application (article 2) (Conseil de l'Europe 2011a) , la Convention d'Istanbul « s'applique à toutes les formes de violence à l'égard des femmes, y compris la violence domestique » et « s'applique en temps de paix et en situation de conflit armé », couvrant chaque situation où les femmes sont la cible de violences.

La convention établit un certain nombre de définitions et de concepts et définit la violence à l'égard des femmes comme étant « une violation des droits humains et une forme de discrimination à l'égard des femmes »

et une forme de violence fondée sur le genre qui entraîne « pour les femmes, des dommages ou souffrances de nature physique, sexuelle, psychologique ou économique » (article 3a), ciblant ainsi les femmes en raison de leur genre et de leurs « rôles, comportements, activités et attributions socialement construits » (article 3c).

De plus, l'article 3a énonce que « la menace de se livrer à de tels actes, la contrainte ou la privation arbitraire de liberté, que ce soit dans la vie publique ou privée » sont considérées comme des formes de violence à l'égard des femmes. « Le terme « femmes » inclut les filles de moins de 18 ans » (article 3f).

Dans son article 4, la convention rappelle aux Parties qu'il faut qu'elles « prennent les mesures législatives et autres nécessaires pour promouvoir et protéger le droit de chacun, en particulier des femmes, à vivre à l'abri de la violence aussi bien dans la sphère publique que dans la sphère privée ». L'article 5 définit les obligations en matière de diligence voulue imposées aux Parties : « les Parties prennent les mesures législatives et autres nécessaires pour agir avec la diligence voulue afin de prévenir, enquêter, punir, et accorder une réparation pour les actes de violence couverts par le champ d'application de la présente Convention commis par des acteurs non étatiques » ; il leur est ainsi rappelé qu'elles ont l'obligation d'élaborer des politiques intégrées visant à prévenir toutes les formes de violence à l'égard des femmes et des filles, tant dans la sphère publique et que dans la sphère privée, à protéger les femmes et les filles contre ces violences et à poursuivre leurs auteurs.

> Ce principe n'impose pas une obligation de résultat, mais une obligation de moyens. Il est demandé aux Parties d'organiser leur réponse à toutes les formes de violence couvertes par cette convention de sorte que les autorités compétentes puissent prévenir de tels actes de violence ou mener des enquêtes, sanctionner les auteurs et accorder une réparation pour de tels actes de violence. Le non-respect de cette obligation engage la responsabilité de l'État pour un acte qui, dans le cas contraire, n'est imputable qu'à un auteur non étatique (Conseil de l'Europe 2011b).

En énonçant des obligations détaillées visant à faire avancer la prévention de toutes les formes de violence à l'égard des femmes grâce à la sensibilisation et à l'éducation, notamment la formation des professionnels et le travail avec les auteurs, la convention a pour objectif de réduire les comportements qui tolèrent ou contribuent à perpétuer la violence à l'égard des femmes. Il s'agit de protéger et de soutenir les victimes et les personnes à risque d'une manière centrée sur la victime et responsabilisante, et ces services doivent être accessibles à tous. Des enquêtes et des procédures pénales doivent être menées pour traduire les auteurs en justice et faire en sorte qu'ils répondent de leurs actes. Tout ce qui précède doit s'inscrire dans le cadre d'une réponse globale aux différentes formes de violence à l'égard des femmes, une particularité qui donne à ce traité juridique important un caractère unique.

Si la Convention d'Istanbul ne fait pas expressément référence à la dimension numérique de la violence à l'égard des femmes, il est cependant conforme à l'intention de ses rédacteurs que son champ d'application, défini à l'article 2, s'étende aux violences commises dans l'espace numérique. En effet, plusieurs articles de la Convention d'Istanbul sont applicables au contexte numérique et sont examinés en détail dans la présente étude. Par exemple, l'article 40 s'applique au harcèlement sexuel en ligne ou facilité par la technologie aux termes de sa définition : « toute forme de comportement non désiré, verbal, non verbal ou physique, à caractère sexuel, ayant pour objet ou pour effet de violer la dignité d'une personne, en particulier lorsque ce comportement crée un environnement intimidant, hostile, dégradant, humiliant ou offensant. »

La disposition de la convention relative au harcèlement (article 34) s'applique également au harcèlement en ligne ou facilité par la technologie, étant donné que le harcèlement y est défini comme « le fait, lorsqu'il est commis intentionnellement, d'adopter, à plusieurs reprises, un comportement menaçant dirigé envers une autre personne, conduisant celle-ci à craindre pour sa sécurité ». L'extension du champ d'application de l'article 34 à la sphère numérique est confirmée dans le rapport explicatif de la convention (ibid.), qui qualifie expressément de « communication non désirée », au sens de l'article 34, « la poursuite d'un contact actif quel qu'il soit avec la victime par n'importe quel moyen de communication disponible, notamment les outils de communication modernes et les TIC ». Compte tenu des conséquences psychologiques graves que de nombreuses formes de violence en ligne et facilitée par la technologie peuvent avoir sur les femmes, l'exigence de la Convention d'Istanbul d'ériger en infraction pénale la violence psychologique (article 33) prend tout son sens.

Mécanismes de suivi

Deux organes distincts mais interdépendants assurent le suivi de la Convention d'Istanbul.

Le GREVIO, Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique, un organe spécialisé indépendant, veille à la mise en œuvre de la convention. Il est actuellement composé de

15 membres, forts d'une expertise multidisciplinaire en matière de droits humains, d'égalité entre les femmes et les hommes, de lutte contre la violence à l'égard des femmes et la violence domestique, ou d'assistance et de protection des victimes. Le GREVIO mène des procédures d'évaluation pays par pays, pour vérifier que la Convention d'Istanbul soit effectivement implémentée dans les États parties[7]. Ces procédures d'évaluation des pays donnent lieu à des orientations spécifiques, adaptées à chaque pays, qui visent à renforcer le niveau de mise en œuvre. Elles comprennent également une évaluation de référence des mesures prises pour concrétiser toutes les obligations de la convention. Les rapports d'évaluation de référence du GREVIO sont rendus publics, avec les commentaires de la Partie concernée[8]. Le GREVIO joue un rôle unique

> dans le suivi de la mise en œuvre d'un instrument aussi détaillé (…) Le GREVIO est considéré comme une plateforme unique ; il devrait générer des données inestimables à partir de son analyse approfondie des dispositions juridiques nationales et internationales en matière de violence à l'égard des femmes. Il devrait également permettre un échange de bonnes pratiques entre les États dans la lutte contre la violence à l'égard des femmes (Guney 2020).

Le Comité des Parties est l'organe politique chargé de suivre la mise en œuvre de la convention. Son rôle est décrit à l'article 67 de la convention. Il se compose des représentants des Parties à la convention.

Sur la base des rapports élaborés par le GREVIO, le Comité des Parties adopte des recommandations portant sur les mesures à prendre « pour mettre en œuvre les conclusions du GREVIO et (...) ayant pour objectif de promouvoir la coopération avec cette Partie afin de mettre en œuvre la présente convention de manière satisfaisante (Conseil de l'Europe 2015a) ». Il contrôle la mise en œuvre de ces recommandations après une période de trois ans.

Dans le cadre de sa procédure d'évaluation de référence, le GREVIO applique les articles précités de la Convention d'Istanbul au contexte numérique et contrôle leur mise en œuvre en ce qui concerne certains aspects de la violence en ligne et facilitée par la technologie, notamment le cyberharcèlement et le harcèlement sexuel en ligne. Dans ses rapports d'évaluation de référence, le GREVIO a souligné les bonnes pratiques des États parties. Ainsi, dans son rapport sur la France, il a salué l'introduction de nouvelles infractions pénales dans le système juridique français, dont l'infraction de cyberharcèlement à l'égard des femmes et des filles. Par ailleurs, le GREVIO a salué les modifications apportées aux codes pénaux de la Slovénie et de la Pologne, qui ont élargi le champ d'application des infractions de harcèlement pour y inclure ses manifestations en ligne. Dans le cadre de sa procédure d'évaluation de base, le GREVIO a également examiné les pratiques éducatives des États parties à la Convention d'Istanbul. Au Portugal, le GREVIO s'est félicité de l'adoption d'une série complète de guides sur le genre et la citoyenneté, qui comprennent des lignes directrices consacrées à la sécurité sur internet, pour tous les niveaux d'enseignement, de la maternelle au secondaire. De la même manière, il a pris note avec satisfaction des efforts déployés par Monaco pour prévenir le cyberharcèlement auprès de tous les élèves âgés de 6 à 10 ans tandis que les efforts de la Slovénie ont été salués du fait qu'ils visaient à sensibiliser les jeunes à la violence lors de rencontres, y compris dans sa dimension en ligne, et à améliorer les connaissances et la sensibilité des professionnels concernés, y compris les enseignants et les travailleurs sociaux, pour une prévention et une protection efficaces contre la violence et le harcèlement en ligne des filles et des femmes.

En plus de mettre en avant les bonnes pratiques, les rapports d'évaluation de référence du GREVIO attirent l'attention sur les domaines qui nécessitent une attention accrue de la part des États membres. Par exemple, le rapport sur la France appelle à mener des actions de sensibilisation et de plaidoyer en ce qui concerne la cyberviolence verbale et sexuelle à l'égard des filles, tandis que le rapport sur les Pays-Bas pointe le fait que les professionnels manquent de connaissances sur la dimension numérique de la violence à l'égard des femmes. De manière analogue, les autorités espagnoles ont été encouragées à intensifier les efforts consacrés à la formation de groupes professionnels comme les forces de l'ordre, le personnel infirmier et les autres professions médicales, ainsi que les enseignants, sur les différentes formes de violence à l'égard des femmes, y compris leur dimension numérique.

Bien que le GREVIO ait salué l'adoption de lois nationales traitant de la dimension numérique de la violence à l'égard des femmes, il a également identifié des lacunes communes à la plupart de ces lois. À titre d'exemple, les sanctions tendent à assurer la sécurité d'une personne et la protection de sa réputation et de ses biens, sans prendre suffisamment en considération les autres conséquences des violences, notamment les préjudices sociaux, économiques et psychologiques et les entraves à la participation. Mais surtout, la majorité des lois

7. Les rapports sont disponibles sur : www.coe.int/fr/web/istanbul-convention/country-monitoring-work.
8. Plus d'information sur le mécanisme de suivi de la Convention d'Istanbul disponible sur : www.coe.int/fr/web/istanbul-convention/about-monitoring1

nationales n'inscrivent pas les violences à l'égard des femmes commises par des moyens numériques dans le contexte d'un éventail de violences affectant les femmes et les filles dans tous les domaines de leur vie.

La Recommandation générale n° 1 du GREVIO, adoptée en octobre 2021 conformément à l'article 69 de la Convention d'Istanbul, précise les modalités d'application de la convention en ce qui concerne les expressions numériques de la violence à l'égard des femmes. Elle donne une interprétation détaillée de la convention dans le cadre de la violence en ligne et facilitée par la technologie et explique, en des termes pratiques, les obligations des États membres à cet égard en formulant des recommandations concrètes. À l'instar de la violence à l'égard des femmes exercée hors ligne, la dimension numérique de la violence à l'égard des femmes est très complexe et multidimensionnelle par nature. La recommandation générale propose une approche globale et multisectorielle permettant d'aborder le problème sous l'angle des quatre piliers (« les 4P ») de la Convention d'Istanbul.

Relations avec d'autres instruments

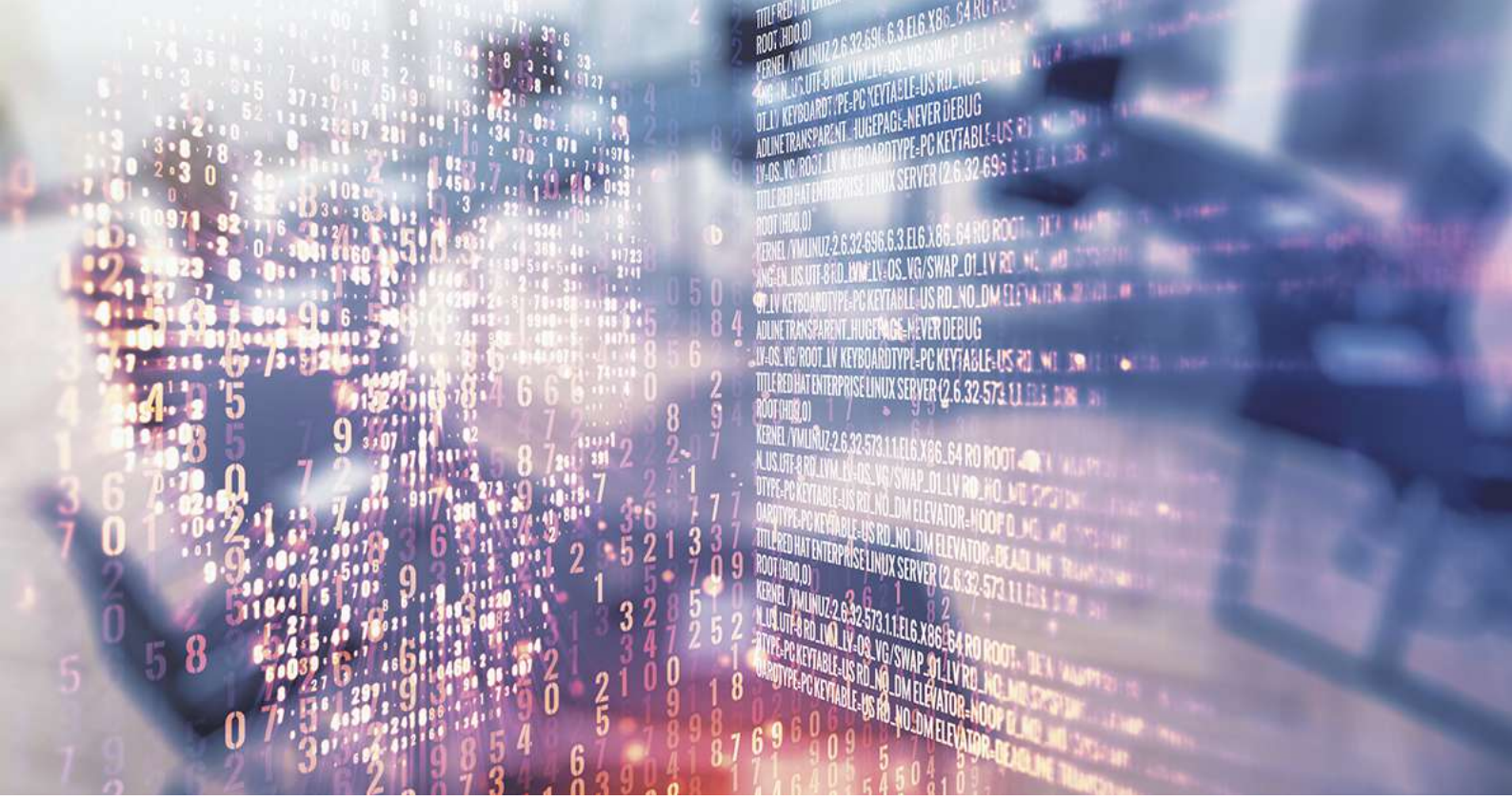
Dans son chapitre X intitulé Relations avec d'autres instruments internationaux, la Convention d'Istanbul prend également en considération des instruments existants ou futurs, qu'ils soient nationaux ou internationaux, et explique le lien de la convention avec ces instruments (Conseil de l'Europe 2011b).

> Le rapport explicatif de la convention souligne que la convention coexiste harmonieusement avec d'autres traités, multilatéraux ou bilatéraux… (L)e principal objectif de la convention est de renforcer la protection des victimes en leur assurant le niveau de protection le plus élevé (...) L'expression « plus élevé » est importante. Il peut être avancé que n'importe quelle approche garantissant le niveau de protection le plus élevé, qu'il s'agisse de la Convention d'Istanbul ou de tout autre instrument, devrait prévaloir. Cela est conforme à l'approche centrée sur la victime de la Convention d'Istanbul, selon laquelle il convient de privilégier l'intérêt supérieur de la victime (Guney 2020).

En effet, l'article 71 souligne que la convention ne porte pas atteinte aux « obligations découlant d'autres instruments internationaux » qui ont été, ou seront, ratifiés par les arties et « qui contiennent des dispositions relatives aux matières régies par la présente Convention ». Il rappelle ainsi aux Parties la validité de leurs obligations au titre des autres traités relatifs aux droits des femmes qu'elles ont ratifiés ou qu'elles ratifieront dans l'avenir.

L'article 73 ajoute que les dispositions de la convention « ne portent pas atteinte aux dispositions du droit interne et d'autres instruments internationaux contraignants déjà en vigueur ou pouvant entrer en vigueur, et en application desquels des droits plus favorables sont ou seraient reconnus aux personnes en matière de prévention et de lutte contre la violence à l'égard des femmes et la violence domestique », reconnaissant ainsi que d'autres instruments sont susceptibles de garantir une meilleure protection aux victimes de violence fondée sur le genre et donc de compléter la Convention d'Istanbul. En outre, le paragraphe 2 de l'article 71 énonce que les Parties peuvent conclure d'autres accords, bilatéraux ou multilatéraux, relatifs à la question de la protection contre la violence à l'égard des femmes, aux fins de compléter ou de renforcer la Convention d'Istanbul.

La partie suivante de cette étude présentera la Convention de Budapest et ses particularités. Ensuite seront examinés précisément les instruments qui existent en dehors de la Convention d'Istanbul et la façon dont ils couvrent certains types de violence à l'égard des femmes en ligne et facilitée par la technologie.



CHAPITRE III

LA CONVENTION DE BUDAPEST

Le texte et son champ d'application

La Convention du Conseil de l'Europe sur la cybercriminalité (la Convention de Budapest) est le premier et le plus pertinent des traités internationaux juridiquement contraignants en matière de cybercriminalité et de preuves électroniques.

La convention et son rapport explicatif ont été adoptés par le Comité des Ministres du Conseil de l'Europe en novembre 2001. La convention a été ouverte à la signature à Budapest et est entrée en vigueur le 1er juillet 2004. En juin 2021, elle comptait 66 États parties. Tous les pays disposés à appliquer ses dispositions et à s'engager dans la voie de la coopération internationale en matière de cybercriminalité peuvent y adhérer. Plus important encore, la Convention de Budapest peut servir de ligne directrice à tout pays qui souhaite se doter d'une législation nationale complète pour lutter contre la cybercriminalité et contre toute infraction impliquant des preuves électroniques ; un grand nombre d'États l'ont d'ailleurs déjà utilisée à cette fin[9].

La convention exige des Parties qu'elles érigent en infraction pénale des comportements qui portent préjudice à des données ou à des systèmes informatiques ou qui impliquent l'utilisation de tels systèmes, y compris des comportements relatifs à la production, à la diffusion ou à la possession de pornographie enfantine, ainsi que des atteintes à la propriété intellectuelle et aux droits connexes. Les Parties à la convention sont également tenues de renforcer les pouvoirs et procédures prévus dans leur législation pénale nationale et de doter leur système judiciaire des moyens nécessaires pour sécuriser les preuves électroniques des infractions et pour permettre une coopération internationale et une entraide judiciaire efficaces dans le cadre des enquêtes et des poursuites relatives à des infractions de cybercriminalité et à d'autres infractions impliquant des preuves électroniques. La convention vise principalement 1) à harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité ; 2) à fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique ; 3) à mettre en place un dispositif rapide et efficace de coopération internationale (Conseil de l'Europe 2001a).

9. Conseil de l'Europe, *The global state of cybercrime legislation 2013 – 2020 : A cursory overview*, disponible sur : https://rm.coe.int/3148-1-3-4-cyberleg -global-state-feb2020-v1-public/16809cf9a9

Le succès et la légitimité de la Convention de Budapest résident à bien des égards dans le fait que les mesures prévues allient une réponse efficace de la justice pénale et des garanties concernant le respect de la prééminence du droit.

Protocoles additionnels à la Convention de Budapest

Le premier protocole additionnel

Le protocole additionnel à la Convention sur la cybercriminalité porte sur l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Adopté par le Comité des Ministres du Conseil de l'Europe en novembre 2002, il est entré en vigueur le 1er mars 2006. En juin 2021, 33 États étaient Parties au protocole additionnel.

Le protocole reconnaît que les systèmes informatiques facilitent la communication et l'exercice de la liberté d'expression, mais aussi la diffusion de contenus et de discours racistes et xénophobes. Il exige donc que les Parties érigent en infraction pénale la diffusion de ce type de contenus.

Il se concentre sur la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques, sur les menaces et insultes ayant une motivation raciste et xénophobe, et sur la négation, la minimisation grossière, l'approbation ou la justification du génocide ou des crimes contre l'humanité.

Le protocole élargit le champ d'application de la convention, y compris ses dispositions en matière de droit matériel, de procédure pénale et de coopération internationale, de manière à couvrir également les infractions de propagande raciste ou xénophobe. Ainsi, outre l'harmonisation des éléments de droit matériel de tels comportements, le protocole facilite l'utilisation par les Parties des moyens et voies de coopération internationale établis dans ce domaine par la convention (Conseil de l'Europe 2003).

Le futur deuxième protocole additionnel

L'élaboration du deuxième protocole additionnel à la Convention de Budapest a commencé en septembre 2017, en vue de répondre aux défis que représente, pour la justice pénale, le développement des activités dans le cyberespace, et en vue de garantir une coopération plus efficace en matière de cybercriminalité et de preuves électroniques. Les preuves électroniques sont indispensables pour enquêter non seulement sur les affaires de cybercriminalité mais aussi sur tout type d'infraction. Si les pouvoirs des autorités judiciaires pénales sont limités par les frontières territoriales, il n'en va pas de même pour les auteurs, les victimes et les preuves électroniques, qui peuvent se situer dans plusieurs États. Il est donc souvent difficile de connaître les lois applicables et de savoir comment et auprès de qui obtenir les preuves.

Cela a des effets négatifs sur l'état de droit et sur le respect, par les gouvernements, de leur obligation de protéger les individus dans le cyberespace. Comme dans le cas de la Convention de Budapest, les mesures définies dans le protocole ne sont conçues que pour des enquêtes pénales spécifiques et sont assorties de garanties relatives à l'état de droit et à la protection des données.

Le deuxième protocole additionnel devrait être adopté et ouvert à la signature d'ici à la fin de l'année 2021.

Cet instrument vise à renforcer la coopération sur la cybercriminalité et l'obtention de preuves électroniques grâce à des outils supplémentaires permettant une entraide plus efficace et d'autres formes de coopération entre les autorités compétentes ; la coopération dans les situations d'urgence, à savoir lorsque la vie ou la sécurité d'une personne physique est exposée à un risque important et imminent ; et la coopération directe entre les autorités compétentes et les prestataires de services et autres entités qui possèdent ou contrôlent les informations nécessaires à l'identification des auteurs d'infractions[10].

Par conséquent, ce protocole a pour objectif de compléter la convention et le premier protocole additionnel. Ses dispositions seront utiles sur le plan opérationnel et politique et permettront de maintenir la pertinence de la Convention de Budapest.

10. Comité de la Convention sur la cybercriminalité (T-CY) (2020), *Préparation du 2e protocole additionnel à la Convention sur la cybercriminalité, État des lieux, disponible sur* : https://rm.coe.int/t-cy-2020-32-fr-protocol-tor-chair-state-of-play/1680a06a82

Comité de suivi et Bureau de programme sur la cybercriminalité

Le Comité de la Convention sur la cybercriminalité (T-CY) garantit la mise en œuvre effective de la Convention de Budapest et représente les États parties à la convention.

L'article 46 de la Convention de Budapest définit le rôle du Comité. Le T-CY facilite l'utilisation et l'application de la convention. Le rôle du comité consiste également à faciliter l'échange d'informations pertinentes entre les Parties sur la cybercriminalité et les preuves électroniques. Enfin, le T-CY est chargé de rédiger les éventuels amendements à la convention[11].

Le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC), situé à Bucarest (Roumanie), complète le travail du T-CY. Le C-PROC est chargé de donner aux pays du monde entier les moyens de renforcer leur système judiciaire et leur système juridique afin de lutter de manière efficace contre la cybercriminalité et contre les infractions dont il existe des preuves électroniques, au niveau national et au niveau international. En particulier, le C-PROC aide les États à élaborer de nouvelles lois ou à mettre à jour leurs lois en s'inspirant de la Convention de Budapest et des normes connexes, mais aussi à renforcer leurs capacités en matière de justice pénale afin de relever les défis posés par la cybercriminalité et les preuves électroniques, et à améliorer la coopération internationale, interinstitutionnelle et public/privé. Si le Conseil de l'Europe peut aider n'importe quel pays à renforcer sa législation nationale sur la cybercriminalité, le fait qu'un gouvernement s'engage politiquement à adhérer à la Convention de Budapest et à la mettre en œuvre permet cependant d'utiliser tous les dispositifs de soutien pour renforcer les capacités en matière de justice pénale. Le C-PROC œuvre également en faveur de la protection des enfants contre la violence sexuelle en ligne et, grâce à une série d'activités sur la cyberviolence, étudie les synergies entre la Convention d'Istanbul et la Convention de Budapest ainsi que d'autres instruments[12]. Le développement des capacités reste une approche efficace pour aider les sociétés à faire face au défi croissant de la cybercriminalité et des preuves électroniques, notamment en ce qui concerne l'instruction des affaires de violence à l'égard des femmes en ligne et facilitée par la technologie, les poursuites et les sanctions.

La Convention de Budapest, son premier protocole et son futur deuxième protocole offrent ainsi un cadre de réflexion très intéressant sur le phénomène de la violence à l'égard des femmes en ligne et facilitée par la technologie, en relation avec la Convention d'Istanbul. Grâce à plusieurs dispositions de droit pénal matériel, elle aborde de manière directe et indirecte certains types de violence à l'égard des femmes en ligne et facilitée par la technologie. D'autres dispositions s'intéressent aux actes facilitant ces types de violence. Les pouvoirs procéduraux et les dispositions sur la coopération internationale de la Convention sur la cybercriminalité présentent un intérêt dans le cadre des enquêtes sur les actes de cyberviolence à l'égard des femmes, notamment pour l'obtention de preuves électroniques.

Dans les deux chapitres précédents, nous avons montré que le champ d'application de la Convention d'Istanbul couvre toutes les formes de violence à l'égard des femmes, que la convention réaffirme la nature structurelle et fondée sur le genre de la violence à l'égard des femmes et qu'elle s'articule autour de la révention, de la protection et du soutien des victimes, de la oursuite des auteurs et de l'élaboration de politiques coordonnées. Nous avons également vu que les Parties ont, à l'égard de leurs citoyens, l'obligation d'agir avec la diligence voulue en ce qui concerne ces quatre piliers.

Nous venons d'examiner dans quelle mesure la Convention du Conseil de l'Europe sur la cybercriminalité couvre les infractions pénales commises contre des systèmes informatiques ou au moyen de tels systèmes, tandis que ses dispositions en matière de procédure et de coopération internationale s'appliquent à toute infraction dont il existe des preuves électroniques. Nous avons constaté que la Convention de Budapest complète les dispositions de la Convention d'Istanbul sur la question spécifique de la violence à l'égard des femmes en ligne et facilitée par la technologie, en permettant de mieux enquêter sur ce type de violence.

De nombreux autres instruments internationaux traitent de certains aspects du phénomène de la violence à l'égard des femmes en ligne et facilitée par la technologie. La Convention d'Istanbul reconnaît que, sur certains points spécifiques, d'autres instruments juridiques peuvent offrir une protection plus complète et elle affirme clairement qu'ils doivent prévaloir. Toutefois, ces instruments ne sont pas toujours suffisamment coordonnés pour faire face au phénomène croissant de la violence à l'égard des femmes en ligne et facilitée par la technologie.

---

11. Information sur le Comité de la Convention sur la cybercriminalité (T-CY), disponible sur : https://www.coe.int/fr/web/cybercrime/tcy
12. Information sur le Bureau de programme sur la cybercriminalité (C-PROC), disponible sur : https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

CHAPITRE IV

INSTRUMENTS RÉGIONAUX ET INTERNATIONAUX TRAITANT DE LA QUESTION DE LA VIOLENCE À L'ÉGARD DES FEMMES EN LIGNE ET FACILITÉE PAR LA TECHNOLOGIE

Ainsi que cela est indiqué dans son préambule, la Convention d'Istanbul s'appuie sur les instruments existants et futurs couvrant les questions relatives à la violence à l'égard des femmes fondée sur le genre, notamment la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (CEDAW), la Convention européenne des droits de l'homme et des libertés fondamentales, la Charte sociale européenne, la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains et la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.

D'autres instruments, accords et politiques, de portée régionale ou internationale, couvrent plus précisément la question de la violence à l'égard des femmes en ligne et facilitée par la technologie (Simonovic 2020).

Récemment, certains instruments, textes et déclarations ont élargi la définition de la violence à l'égard des femmes fondée sur le genre ou du sexisme pour en reconnaître les formes spécifiques commises en ligne et par le biais des nouvelles technologies.

Recommandation générale n° 35 du Comité CEDAW

La Recommandation générale n° 35 adoptée par le Comité pour l'élimination de la discrimination à l'égard des femmes (Comité CEDAW) au sujet de la violence à l'égard des femmes fondée sur le genre, actualisant la Recommandation générale n° 19 (Comité pour l'élimination de la discrimination à l'égard des femmes 2017), définit la violence à l'égard des femmes fondée sur le genre comme se manifestant « sous des formes multiples, interdépendantes et récurrentes, dans des contextes divers, publics ou privés, y compris dans les cadres créés par la technologie et, à l'ère de la mondialisation, en se moquant des frontières », et ajoute que

> la violence à l'égard des femmes fondée sur le genre s'exerce dans toutes les sphères de l'interaction humaine, qu'elles soient publiques ou privées. Il peut s'agir de la famille, de la communauté, des espaces publics, du lieu de travail, des loisirs, du monde politique, du sport, des services de santé, de l'éducation ou d'environnements créés par la technologie qui ont généré de nouvelles formes de violence en ligne et dans les autres espaces numériques.

Dans son rapport concernant la violence en ligne à l'égard des femmes, la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences définit le phénomène comme

> tout acte de violence fondée sur le genre qui est commis, facilité ou aggravé pleinement ou partiellement par l'utilisation des TIC, par exemple les téléphones portables et les smartphones, Internet, les plateformes de réseaux sociaux ou les courriers électroniques, et qui vise une femme parce qu'elle est une femme ou touche spécialement les femmes.

Recommandation du Conseil de l'Europe sur la prévention et la lutte contre le sexisme

En mars 2019, le Comité des Ministres du Conseil de l'Europe a adopté une nouvelle recommandation sur la prévention et la lutte contre le sexisme, qui énonce la première définition internationalement reconnue du sexisme, y compris le sexisme en ligne et facilité par les nouvelles technologies, et réaffirme l'existence d'un éventail de violences dirigées contre les femmes et les filles (Conseil de l'Europe 2019). Le sexisme est défini comme :

> Tout acte, geste, représentation visuelle, propos oral ou écrit, pratique ou comportement fondés sur l'idée qu'une personne ou un groupe de personnes est inférieur du fait de leur sexe, commis dans la sphère publique ou privée, en ligne ou hors ligne, avec pour objet ou effet :
>
> I. de porter atteinte à la dignité ou aux droits inhérents d'une personne ou d'un groupe de personnes ; ou
> II. d'entraîner pour une personne ou un groupe de personnes des dommages ou des souffrances de nature physique, sexuelle, psychologique ou socio-économique ; ou
> III. de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant ; ou
> IV. de faire obstacle à l'émancipation et à la réalisation pleine et entière des droits humains d'une personne ou d'un groupe de personnes ; ou
> V. de maintenir et de renforcer les stéréotypes fondés sur genre.

Elle ajoute que « les comportements sexistes, en particulier le discours de haine sexiste, peuvent dégénérer en ou inciter à des agissements ouvertement offensants et menaçants, y compris des abus ou de la violence sexuels, des viols ou des actes potentiellement mortels. Le sexisme peut aussi résulter en perte de ressources, automutilation ou suicide ». Elle souligne que ces comportements « sont présents dans toutes les activités humaines, y compris dans le cyberespace (internet et réseaux sociaux). L'expérience du sexisme peut être individuelle ou collective, même si ni la personne ni le groupe ne sont directement visés ». La recommandation contient aussi l'observation suivante : « Internet a donné une nouvelle dimension à l'expression et à la diffusion du sexisme, en particulier du discours de haine sexiste, auprès d'un large public, même si les origines du sexisme ne sont pas à chercher du côté des technologies mais dans la persistance des inégalités entre les femmes et les hommes ». Enfin, la recommandation réaffirme la dimension intersectionnelle du sexisme et met en avant les circonstances aggravantes, telles que les relations de pouvoir et la portée et la récurrence des abus. Cette définition du sexisme dans le contexte de la communication numérique est unique à ce jour.

Stratégie du Conseil de l'Europe pour l'égalité entre les femmes et les hommes

La stratégie du Conseil de l'Europe pour l'égalité entre les femmes et les hommes 2018-2023 réaffirme l'existence des formes de discrimination et de violence affectant les droits, la sûreté et la sécurité des femmes en ligne et hors ligne.

> Les contenus violents et dégradants en ligne, y compris dans la pornographie, la normalisation de la violence sexuelle, notamment le viol, renforcent l'idée d'un rôle de soumission des femmes et contribuent à traiter les femmes comme des membres subordonnés de la famille et de la société. Ils alimentent la violence contre les femmes, le discours de haine sexiste ciblant les femmes, particulièrement les féministes, et contribuent au maintien et au renforcement des stéréotypes de genre et au sexisme (Conseil de l'Europe 2018b).

La stratégie insiste en effet sur l'idée que les violences contre les femmes forment un continuum et que ces violences se nourrissent de stéréotypes dégradants et de comportements normalisés qui s'expriment à la fois en ligne et hors ligne :

> il est également établi que les réseaux sociaux font, en particulier, l'objet d'utilisations abusives, et que les femmes et les filles sont souvent confrontées à des menaces violentes et à caractère sexuel en ligne. Des plateformes en particulier sont utilisées pour véhiculer un discours de haine sexiste, dont les réseaux sociaux et les jeux vidéo. La liberté d'expression sert souvent d'excuse pour justifier des comportements inacceptables et offensants. À l'instar d'autres formes de violence contre les femmes, le discours de haine sexiste reste insuffisamment signalé, mais ses effets sur les femmes, en particulier les plus jeunes d'entre elles, peuvent être dévastateurs, que ce soit sur le plan émotionnel, psychologique et/ou physique. Il en va de même pour le sexisme.

L'Union européenne s'intéresse également à la question de la violence à l'égard des femmes en ligne et facilitée par la technologie. Dans plusieurs de ses stratégies, elle reconnaît le problème et propose des feuilles de route pour y répondre.

Stratégie de l'UE en faveur de l'égalité entre les hommes et les femmes

La stratégie de l'UE en faveur de l'égalité entre les hommes et les femmes reconnaît la violence à l'égard des femmes en ligne et facilitée par la technologie comme suit :

> La violence en ligne ciblant les femmes est devenue très courante et a des conséquences spécifiques particulièrement néfastes ; cette situation est inacceptable. Elle fait obstacle à la participation des femmes à la vie publique. L'intimidation, le harcèlement et les insultes sur les réseaux sociaux ont des incidences considérables sur la vie quotidienne des femmes et des filles. La Commission proposera une législation sur les services numériques pour clarifier les responsabilités des plateformes en ligne en ce qui concerne les contenus diffusés par les utilisateurs. Cette législation précisera quelles mesures les plateformes doivent prendre pour lutter contre les activités illégales en ligne, tout en protégeant les droits fondamentaux. Les utilisateurs doivent également être à même de contrer d'autres types de contenus préjudiciables et insultants, qui ne sont pas toujours considérés comme illégaux, mais qui peuvent avoir des effets désastreux. Afin de protéger la sécurité des femmes en ligne, la Commission facilitera l'élaboration d'un nouveau cadre de coopération entre les plateformes internet (Commission européenne 2020a).

Le 13 août 2020, dans sa réponse à une question parlementaire, Helena Dalli, Commissaire européenne à l'Égalité, ajoute que « conformément à la stratégie en faveur de l'égalité entre les hommes et les femmes, la Commission facilitera la mise en place d'un cadre de coopération entre les plateformes et les autres parties prenantes pour lutter contre les violences sexistes en ligne » (Parlement européen 2020).

Stratégie de l'UE relative au droit des victimes

La stratégie de l'UE relative au droit des victimes définit la cybercriminalité comme « tout type d'infraction commise en ligne ou au moyen d'un ordinateur ou d'outils en ligne ». De plus, elle ajoute que :

> La cybercriminalité peut inclure des infractions graves contre les personnes, telles que les infractions à caractère sexuel en ligne (y compris contre des enfants), l'usurpation d'identité, les crimes de haine en ligne. (...) Les victimes de cybercriminalité ne trouvent pas toujours l'aide nécessaire pour remédier au préjudice qu'elles ont subi et, souvent, ne dénoncent pas l'infraction. (...) Il y a lieu de faciliter davantage la dénonciation des infractions relevant de la cybercriminalité et d'apporter aux victimes l'aide dont elles ont besoin (Commission européenne 2020b).

Cette définition est intéressante car elle considère la cybercriminalité comme un problème susceptible de toucher toute personne en ligne, par n'importe quel moyen.

En ce qui concerne la cybercriminalité de manière générale et la cybercriminalité contre les femmes en particulier, ainsi que les questions connexes relatives aux éventuels recours contre la violence à l'égard des femmes en ligne et facilitée par la technologie, telles que la protection de la vie privée, la responsabilité des intermédiaires et l'obtention de preuves numériques, il existe un grand nombre d'instruments. Certains instruments et réglementations de l'UE, tels que le règlement général sur la protection des données (RGPD), la législation sur les services numériques ou le règlement sur les preuves électroniques, sont ou seront juridiquement contraignants pour les États membres. En revanche, d'autres instruments détaillant la coopération avec le secteur privé par exemple, tels que le Code de conduite visant à combattre les discours de haine illégaux en ligne,

sont considérés comme des autoréglementations mais ont toutefois été efficaces en pratique pour endiguer le phénomène (la dernière pour les discours de haine illégaux sur les réseaux sociaux).

La Convention du Conseil de l'Europe 108 + et le RGPD

Le but de la Convention 108 du Conseil de l'Europe sur la protection des données est de « garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ». Modernisé en 2018 devenant ainsi la « Convention 108+, la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel », le texte prévoit que la protection de la convention s'applique à toute personne, sans tenir compte de de sa nationalité, dès lors qu'elle relève de la juridiction de l'une des Parties ayant ratifié la convention (Conseil de l'Europe 2018a). Les personnes sont protégées à l'égard du traitement, automatisé ou non automatisé, des informations les concernant, y compris des données sensibles comme les données génétiques et biométriques. Le texte prévoit aussi un « droit d'effacement ».

Entré en vigueur le 25 mai 2018, le Règlement (UE) 2016/679, c'est-à-dire le Règlement général de l'Union européenne sur la protection des données (RGPD), régit la collecte des données à caractère personnel des résidents de l'UE et leur traitement par des personnes, des sociétés ou des organisations. Il renforce les droits individuels en matière de contrôle, d'effacement, de rectification, de limitation ou d'opposition concernant le traitement des données à caractère personnel. Il facilite également l'accès aux données personnelles, y compris les images (dont les images intimes non consenties), et leur transfert. Enfin, le règlement oblige les sociétés et entités qui traitent les données à obtenir le consentement explicite de l'utilisateur. Par « consentement », on entend une manifestation de volonté « libre, spécifique, éclairée et univoque » de la personne concernée.

Le règlement s'applique si le responsable du traitement des données (un organisme qui collecte les données de résidents de l'UE), le sous-traitant (un organisme qui traite les données pour le compte du responsable du traitement et qui peut donc être un prestataire de services de cloud, par exemple), ou la personne concernée (la personne à laquelle se rapportent les données), est basé dans l'UE.

Ainsi, le règlement ouvre des possibilités de mettre un frein à certains aspects de la violence à l'égard des femmes en ligne et facilitée par la technologie, en exigeant, par exemple, que les entreprises tiennent compte du respect de la vie privée dans la conception de leurs produits (sur la question du «stalkerware», voir Citizen Lab 2020), ou que les personnes chargées de mettre en ligne des contenus à caractère sexuel basés sur des images, ainsi que les diffuseurs de ces contenus, soient considérés comme coresponsables du traitement des données, et soient donc soumis aux obligations et sanctions imposées par le RGPD (Van der Wilk 2018) . De plus, le RGPD prévoit un « droit à l'effacement », plus connu sous le nom de droit à l'oubli :

> Le règlement accorde aux personnes concernées qui ne veulent plus que leurs données soient traitées un nouveau droit : elles peuvent demander la suppression définitive des données, s'il n'existe pas de motifs légitimes de les conserver (...) Ce droit à l'effacement s'applique à tous les niveaux, pas uniquement aux moteurs de recherche, ce qui signifie que les nouvelles dispositions de la législation de l'UE sur la protection des données offrent aux victimes de revenge porn non seulement un moyen de supprimer les liens vers les images diffusées, mais aussi la possibilité de retirer les images des sites internet sources, au moins dans les pays de l'UE (Setterfield 2019).

La législation de l'UE sur les services numériques

La directive sur le commerce électronique est entrée en vigueur le 8 juin 2000. Elle établit des règles harmonisées relatives au commerce électronique, y compris la responsabilité des prestataires de services comme les plateformes de commerce en ligne et les réseaux sociaux. Elle prévoit des exonérations de responsabilité pour les prestataires de services numériques considérés comme ayant joué un rôle neutre en ce qui concerne les contenus transmis ou hébergés. Les prestataires de services sont tenus de retirer les contenus illicites hébergés sur leurs plateformes ou d'en interdire l'accès dès qu'ils sont avertis du caractère illicite des contenus. Le texte permet également aux États membres d'exiger le retrait des contenus illicites par les prestataires de services. Il offre ainsi une fondement juridique pour le signalement et la suppression des contenus en ligne illicites (Van der Wilk 2018).

En 2019, les dispositions principales de la directive sur le commerce électronique ont été ouvertes à la révision et la Commission européenne a proposé la nouvelle législation sur les services numériques afin de moderniser le cadre juridique de ces services.

La proposition de législation sur les services numériques a été publiée en décembre 2020 et devrait être adoptée dans un an et demi environ. « En énonçant des obligations claires de diligence raisonnable pour certains services intermédiaires, notamment des procédures de notification et d'action pour les contenus illicites et la possibilité de contester les décisions relatives à la modération de contenu des plateformes, la proposition vise à améliorer la sécurité des utilisateurs en ligne dans toute l'Union et à renforcer la protection de leurs droits fondamentaux » (Commission européenne 2020d).

Le texte définit des règles pour les très grandes plateformes, telles que les géants des médias sociaux, et prévoit que « les prestataires de services numériques sont tenus de réduire les risques auxquels leurs utilisateurs sont exposés et de protéger leurs droits ». Elle conserve le régime de responsabilité hérité de la directive sur le commerce électronique, en vertu duquel les sociétés hébergeant des contenus ne sont pas responsables de ces contenus à moins qu'elles n'aient connaissance de leur caractère illicite. Si un contenu est signalé, la proposition actuelle exige des prestataires qu'ils le retirent rapidement. De plus, la législation sur les services numériques inclut la proposition faite par des groupes de défense des droits humains de désigner dans chaque État membre un « coordinateur pour les services numériques », c'est-à-dire une autorité chargée de contrôler la mise en œuvre du règlement, de mettre en place un mécanisme de réclamation et de réparation et de régler les litiges à l'amiable dans les cas où du contenu a été injustement retiré.

> La proposition exigera uniquement le retrait des contenus illicites et prévoira des garanties obligatoires lorsque les informations des utilisateurs sont supprimées, notamment la fourniture d'informations explicatives à l'utilisateur, des mécanismes de réclamation pris en charge par les fournisseurs de services ainsi qu'un mécanisme externe de règlement extrajudiciaire des litiges. En outre, elle garantira que les citoyens de l'UE sont également protégés lorsqu'ils utilisent des services fournis par des fournisseurs non établis dans l'Union, mais actifs sur le marché intérieur, puisque ces fournisseurs sont également compris dans le champ d'application (Commission européenne 2020d).

Enfin, la proposition mentionne l'obligation, pour les très grandes plateformes en ligne, de permettre aux chercheurs agréés d'accéder aux données, sous le contrôle du coordinateur pour les services numériques.

La proposition relative aux preuves électroniques

Selon la Commission européenne, « aujourd'hui, plus de la moitié des enquêtes pénales incluent une demande d'accès transfrontière à des preuves électroniques telles que des textes, des courriers électroniques ou des applications de messagerie » (Commission européenne 2019).

En 2019, la Commission européenne a proposé d'engager des négociations internes sur l'accès transfrontière aux preuves électroniques et publié une « Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale » ainsi qu'une « Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale ». Les deux propositions législatives visent à apporter plus de clarté sur le plan juridique et à accélérer le processus d'obtention de preuves électroniques, grâce à « l'obligation, pour les prestataires de services, de réagir dans un délai maximum de 10 jours, voire 6 heures en cas d'urgence (contre 10 mois en moyenne dans le cadre de la procédure d'entraide judiciaire) ». Ces instruments permettraient aux forces de l'ordre des États membres de l'UE d'accéder plus rapidement aux données électroniques, en les demandant directement ou en demandant leur conservation aux prestataires de services en ligne dans d'autres pays de l'UE dans les cas où l'enquête sur un crime est couverte par l'instrument. Les données ou les informations électroniques peuvent être des textes, des messages, des courriels ou des informations permettant d'identifier un auteur, comme son adresse IP. En outre, ces instruments obligeraient les fournisseurs de services à « désigner un représentant légal dans l'Union, afin de garantir que tous les prestataires offrant des services dans l'Union sont soumis aux mêmes obligations, même s'ils sont basés dans un pays tiers » (Commission européenne 2019).

La réglementation proposée permettra de traiter les cas les plus urgents et d'accélérer les processus d'accès aux preuves dans d'autres États membres de l'UE.

Comme le futur deuxième protocole additionnel à la Convention de Budapest, la proposition de règlement sur les preuves électroniques apporte une valeur ajoutée dans la mesure où elle tient compte du fait que la majorité des infractions présentent aujourd'hui une dimension numérique, avec des preuves et des informations parfois stockées en dehors du pays de résidence de la victime.

L'équivalent américain de la proposition sur les preuves électroniques, le « CLOUD Act », est une loi qui permet aux partenaires étrangers des États-Unis d'obtenir directement la coopération des prestataires de services dans un pays partenaire. À ce jour, seul le Royaume-Uni est considéré comme un partenaire étranger dans ce cadre.

Outre les instruments précités, le Plan d'action pour la démocratie européenne et la Stratégie de l'UE pour l'union de la sécurité sont également des textes de l'UE qui font référence aux contenus en ligne préjudiciables ou illicites.

Un autre instrument, qui existe depuis quelques années maintenant, a produit des résultats dans la lutte contre les discours de haine illégaux en ligne.

Le Code de conduite de l'UE visant à combattre les discours de haine illégaux en ligne

En mai 2016, Facebook, Microsoft, Twitter et YouTube ont signé un « Code de conduite visant à combattre les discours de haine illégaux en ligne » avec la Commission européenne. Instagram, Snapchat et Dailymotion ont adhéré au Code de conduite en 2018, Jeuxvideo.com en 2019 et TikTok en septembre 2020.

Les signataires du Code de conduite se sont engagés à examiner les signalements de discours de haine sur leurs plateformes et à réagir aux contenus illicites dans un délai de 24 heures. Les Parties définissent le discours de haine illégal sur la base de la « Décision-cadre du Conseil sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal » (Union européenne 2008). La définition couvre l'incitation publique à la violence ou à la haine contre un groupe de personnes ou un membre de ce groupe défini par référence à la race, à la couleur, à la religion, à l'ascendance ou à l'origine nationale ou ethnique. Le cinquième cycle de suivi du Code de conduite (2019-2020) a montré que 90 % des notifications étaient examinées dans un délai de 24 heures et que 71 % des contenus étaient supprimés. En 2020, le motif le plus courant des discours de haine en ligne était l'orientation sexuelle, qui représentait 33 % des signalements. Cela s'explique en partie par le fait que « les organisations de défense des droits des personnes LGBTQI ont signalé les contenus de manière plus active » (Commission européenne 2020c).

Cette activité de suivi présente deux lacunes principales : l'absence de ventilation des données et le manque de transparence globale sur les signalements et les retraits. En outre, les agressions fondées sur plusieurs motifs ne sont pas prises en considération. Par conséquent, il est difficile de bien comprendre le phénomène des discours de haine en ligne comportant une forte dimension intersectionnelle et l'expérience de nombreuses utilisatrices est donc ignorée[13]. Dans l'étude du Conseil de l'Europe intitulée *Models of Governance of Online Hate Speech*, Alexander Brown identifie deux autres problèmes majeurs dans cet exercice de suivi :

> Les plateformes internet sont informées de la période de suivi. En conséquence, il est difficile de déterminer si ces évolutions de pourcentages illustrent de véritables améliorations du taux de retrait des discours de haine en ligne sur l'année ou si elles reflètent en réalité l'amélioration de la capacité des plateformes internet à manipuler le processus de suivi en augmentant les taux de retrait durant la période de suivi uniquement (Conseil de l'Europe 2020a).

De plus, selon l'auteur : les organisations participant en tant que « signaleurs de confiance » aux sessions de formations et réunions de suivi se voient accorder des « subventions publicitaires » par les plateformes internet (ces organisations peuvent ainsi mener gratuitement des campagnes sur les plateformes, par exemple). Cela fait douter de l'indépendance, de la neutralité et de la transparence des « signaleurs de confiance » dans ce contexte précis.

À l'échelle mondiale, la dimension numérique de la violence est de plus en plus prise en compte. L'Observation générale n° 25 sur les droits de l'enfant en relation avec l'environnement numérique est un exemple récent

13. Amnesty International rapporte, par exemple, que les femmes politiques et les femmes journalistes noires ont 84 % plus de risques que les femmes blanches de faire l'objet de commentaires injurieux sur Twitter, « UK : online abuse against black women MPs 'chilling », disponible sur : https://www.amnesty.org.uk/press-releases/uk-online-abuse-against-black-women-mps-chilling.

de la façon dont les traités en matière de droits humains font face à un nouvel ensemble de menaces[14]. À l'échelle de l'UE, la priorité est actuellement donnée à la ratification de la Convention d'Istanbul. Cependant, la Présidente de la Commission européenne, Mme Von der Leyen, a également annoncé pour 2021 plusieurs grandes initiatives susceptibles de contribuer à la lutte contre les formes de violence à l'égard des femmes en ligne et facilitée par la technologie : une proposition législative visant à prévenir et combattre des formes spécifiques de violence sexiste est actuellement à l'étude, ainsi que des propositions visant à étendre la liste des infractions pénales de l'UE à toutes les formes de crimes et de discours haineux[15]. Certains groupes de défense des droits des femmes plaident aussi pour un cadre juridique complet et une directive sur la prévention et la lutte contre la violence à l'égard des femmes, qui permettraient d'instaurer un lien entre les instruments existants, reconnaîtraient la violence en ligne et définiraient expressément les types de violence à l'égard des femmes en ligne et facilitée par la technologie[16].

Nous allons à présent examiner dans quelle mesure les deux traités du Conseil de l'Europe, la Convention d'Istanbul et la Convention de Budapest, peuvent contribuer à la lutte contre la violence à l'égard des femmes en ligne et facilitée par la technologie, grâce à des politiques intégrées, à la prévention, à la protection, aux poursuites et à la coopération internationale.

En effet, au niveau du Conseil de l'Europe, les synergies entre les traités offrent la possibilité d'élaborer des réponses coordonnées face au phénomène. Dans la prochaine partie, nous étudierons cette complémentarité en définissant les formes de la violence en ligne et en les mettant en relation avec les dispositions de la Convention d'Istanbul et, le cas échéant, les dispositions de fond de la Convention de Budapest. En nous référant aux comportements visés à l'article 40 (Harcèlement sexuel), à l'article 34 (Harcèlement) et à l'article 33 (Violence psychologique) de la Convention d'Istanbul, nous examinerons trois grandes catégories de violence en ligne : 1) le harcèlement sexuel et fondé sur le genre en ligne, 2) le harcèlement en ligne et facilité par la technologie, et 3) les formes de violence psychologique en ligne et facilitée par la technologie, y compris les discours de haine sexistes.

14. Convention des Nations Unies relative aux droits de l'enfant (2021), Comité des droits de l'enfant, « Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique », disponible sur : : https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFsdFXGQsWU46nx%2b-5vAg3QbGXlnOwo3Oquj8nN7ltX6yUYoRpe7N%2b7Q6mEUIz2mfWi
15. Von der Leyen, U., Šefčovič, M., Commission européenne (2020), État de l'Union 2020, « Lettre d'intention adressée au Président David Maria Sassoli et à la Chancelière Angela Merkel », disponible sur : https://ec.europa.eu/info/sites/info/files/state_of_the_union_2020_letter_of_intent_fr.pdf
16. Entretien avec Asha Allen, European Women's Lobby, septembre 2020, disponible sur : https://womenlobby.org/?lang=en

CHAPITRE V

GROS PLAN SUR LES ARTICLES 33, 34 ET 40 DE LA CONVENTION D'ISTANBUL

Le présent chapitre offre une classification des types de violence à l'égard des femmes en ligne et facilitée par la technologie, compte tenu des recherches menées récemment dans ce domaine. Il existe plusieurs types de classification qui sont tout autant valables pour comprendre ce phénomène[17]. Certaines formes de violence à l'égard des femmes en ligne et facilitées par la technologie ont été classées et présentées selon la relation entre la victime et son agresseur, d'autres selon les modalités comportementales de l'abus et d'autres encore selon les moyens employés pour commettre les actes de violence. Certaines classifications juridiques se concentrent sur la dimension technologique des abus et n'intègrent pas la dimension de genre ou présentent ces types de violence comme des atteintes aux droits, notamment le droit à la vie privée ou le droit d'auteur. La classification proposée ci-dessous définit chaque type de violence dans le cadre de la Convention d'Istanbul et des dispositions applicables de la Convention de Budapest.

En effet, les articles 33, 34 et 40 de la Convention d'Istanbul couvrent un grand nombre de formes de violence perpétrées en ligne et par le biais des nouvelles technologies. Les chapitres qui suivent présentent une définition de chaque catégorie, les correspondances avec les définitions contenues dans la Convention d'Istanbul, et d'autres définitions le cas échéant. Ensuite, chaque forme de violence est définie de manière détaillée, illustrée par des exemples et considérée sous l'angle des articles applicables de la Convention de Budapest.

Harcèlement sexuel et fondé sur le genre en ligne

Note sur le cyberharcèlement

Le cyberharcèlement touche le plus souvent des mineurs, quel que soit leur sexe. Il consiste à adopter un comportement agressif et répété en ligne, dans le but d'effrayer une personne et d'ébranler son amour-propre ou de porter atteinte à sa réputation, et peut conduire des personnes vulnérables à la dépression et au suicide.

Le harcèlement sexuel est défini à l'article 40 de la Convention d'Istanbul de la manière suivante : « toute forme de comportement non désiré, verbal, non verbal ou physique, à caractère sexuel, ayant pour objet ou pour effet de violer la dignité d'une personne, en particulier lorsque ce comportement crée un environnement

17. Voir, par exemple, Conseil de l'Europe 2018c ; Harris 2020b ; Hinson et al.2018.

intimidant, hostile, dégradant, humiliant ou offensant ». La convention énonce le principe selon lequel le harcèlement sexuel doit être soumis à des sanctions pénales ou autres sanctions légales. En outre, l'article 46 de la convention prévoit des circonstances aggravantes lorsque (46.a) « l'infraction a été commise à l'encontre d'un ancien ou actuel conjoint ou partenaire, conformément au droit interne, par un membre de la famille, une personne cohabitant avec la victime, ou une personne ayant abusé de son autorité », (46.a) « l'infraction, ou les infractions apparentées, ont été commises de manière répétée », (46.b) « l'infraction a été commise à l'encontre d'une personne rendue vulnérable du fait de circonstances particulières », (46.c) « l'infraction a été commise par deux ou plusieurs personnes agissant ensemble », (46.e) et « l'infraction a entraîné de graves dommages physiques ou psychologiques pour la victime » (46.h).

S'agissant des autres définitions, l'Agence des droits fondamentaux de l'Union européenne, dans son enquête la plus récente sur la violence à l'égard des femmes (2014) définit le harcèlement sexuel en ligne comme « des e-mails ou SMS sexuellement explicites non sollicités qui vous ont offensée, des avances déplacées qui vous ont offensée sur des sites Internet de réseaux sociaux comme Facebook, ou sur des forums de discussion en ligne ». Il ressort des résultats de l'enquête qu'en 2014, 20 % des jeunes femmes dans l'Union européenne avaient été victimes de harcèlement sexuel en ligne. Le projet de recherche intitulé DeShame (axé sur les mineurs), qui est financé par l'Union européenne, propose une définition exhaustive du harcèlement sexuel en ligne : « un comportement non désiré, à caractère sexuel, qui se déroule sur toute plateforme numérique » (Childnet/Save the Children/UCLan 2019). Il est reconnu comme une forme de violence sexuelle et englobe un « large éventail de comportements ayant recours à du contenu numérique (images, vidéos, publications, messages, pages) sur différentes plateformes (privées ou publiques), pouvant amener une personne à se sentir menacée, exploitée, contrainte, humiliée, contrariée, sexualisée ou visée par des discriminations ». Cette définition reflète en soi celle de la Convention d'Istanbul, et ne fait qu'ajouter les lieux dans lesquels ces types de comportements peuvent être observés. Le groupe de chercheurs participant au projet propose une catégorisation intéressante du harcèlement sexuel en ligne : 1) le partage non consenti de vidéos ou d'images ; 2) l'exploitation, la contrainte et les menaces ; 3) le harcèlement sexualisé. Ces trois catégories englobent une grande majorité des formes de violence auxquelles les femmes sont confrontées en ligne. Cette catégorisation servira de base pour regrouper ci-dessous les différentes formes de harcèlement sexuel et fondé sur le genre en ligne.

Partage non consenti d'images ou de vidéos

Le partage non consenti d'images ou de vidéos ou la diffusion non consentie de matériel explicite se manifeste sous différentes formes et constitue une forme croissante et répandue de violence en ligne et facilitée par le biais de nouvelles technologies.

Dans une étude internationale sur les victimes et les auteurs d'abus sexuel basé sur des images, l'ensemble des infractions est défini comme « la prise, le partage non consentis ou la menace de partager des images (photos ou vidéos) d'une personne, à caractère sexuel ou représentant cette personne nue (qui) comprend aussi la production d'images retouchées par des moyens numériques : le visage ou le corps d'une personne peut être inséré, en surimpression, dans une photo ou une vidéo à caractère pornographique, ce qui constitue de la « fausse pornographie » (fake pornography). On parle de deepfake lorsque ces images de synthèse sont créées en utilisant l'intelligence artificielle ». Il ressort de l'étude que : « une personne interrogée sur trois a indiqué que quelqu'un avait pris une image à caractère sexuel ou la représentant nue sans son consentement, une sur cinq a signalé que quelqu'un avait partagé une image à caractère sexuel ou la représentant nue sans son consentement (20,9 %), et presque une personne sur cinq a signalé que quelqu'un avait menacé de partager une image à caractère sexuel ou la représentant nue (18,7 %) ». Les auteurs concluent également que cette forme de violence « englobe une variété de contextes relationnels, de préjudices, ainsi que tout un éventail de répercussions différentes pour les victimes, et que les femmes vivent différemment les abus basés sur des images dans le contexte d'expériences multiples de préjudices et de victimisation interpersonnels, y compris le harcèlement, la violence sexuelle et/ou les situations de violence entre partenaires intimes (Powell et al. 2020) ».

Images/vidéos à caractère sexuel prises sans consentement et diffusées en ligne ou voyeurisme numérique

Cette forme de comportement violent comprend les creepshots (images à caractère sexuel ou privé prises dans un cadre public ou privé sans le consentement de la personne et à son insu et partagées en ligne) et l'upskirting (images à caractère sexuel ou privé prises sous la jupe ou la robe de la victime, sans son consentement et partagées en ligne). L'upskirting est parfois illustré par l'expérience de Gina Martin, une jeune femme britannique qui participait à un festival ; des photos ont été prises sous sa jupe alors qu'elle faisait la queue pour

aller aux toilettes. Elle a ensuite saisi le parlement de l'affaire et l'upskirting est désormais considéré comme une infraction pénale au Royaume-Uni ; les auteurs risquent jusqu'à deux ans de prison[18].

Images/vidéos à caractère sexuel prises avec le consentement de la personne mais partagées sans son consentement[19]

Le partage d'images et de vidéos à caractère sexuel de victimes sans leur consentement constitue un abus sexuel basé sur des images(McGlynn, Rackley et Houghton 2017). L'abus sexuel basé sur des images est également appelé exploitation sexuelle basée sur des images (Powell et Henry 2016), partage non consenti d'images ou de vidéos, ou encore partage non consenti d'images intimes[20], pornographie non consentie (Citron et Franks 2014) ou « revenge porn ». De nombreux universitaires insistent sur la nécessité de redéfinir le terme « revenge porn » employé par les médias étant donné qu'il décrit l'expérience de l'auteur plutôt que la violence interminable que cela engendre pour la victime.

L'auteur (ancien partenaire ou partenaire actuel, ami, proche, connaissance ou étranger) obtient des images ou des vidéos au cours d'une relation, ou pirate l'ordinateur de la victime, ses comptes de réseaux sociaux ou son téléphone. Les photos/vidéos sont ensuite partagées par l'auteur et diffusées en ligne, et de ce fait par de nombreux auteurs secondaires, parfois des milliers, parfois avec l'adresse et les coordonnées de la victime, ainsi que celles de sa famille ou de son employeur, une pratique également connue sous le nom de « doxing ».

Deepfakes

Les « deepfakes » sont le résultat d'un processus utilisant des algorithmes et les techniques de l'apprentissage profond pour remplacer numériquement un visage par un autre dans une vidéo, et modifier le son, de sorte à créer l'illusion qu'une autre personne est représentée (Langlais-Fontaine 2020). Les deepfakes n'entrent pas dans le cadre de classification proposé par le projet DeShame mais Powell et al. (2020) classent les deepfakes dans la catégorie du harcèlement sexuel en ligne dans leur enquête transnationale sur l'abus sexuel basé sur des images.

Selon un rapport établi par la société néerlandaise Sensity (Ajder et al. 2019), 96 % des vidéos deepfakes analysées étaient des vidéos pornographiques :

> La pornographie deepfake est un phénomène qui cible exclusivement les femmes et leur porte préjudice. En revanche, les vidéos deepfake non pornographiques [qu'ils ont] analysées sur YouTube contenaient une majorité de protagonistes de sexe masculin. ... L'écosystème de la pornographie deepfake est presque entièrement soutenu par des sites web dédiés à la pornographie deepfake, qui hébergent 13 254 vidéos parmi le nombre total de vidéos [qu'ils ont] découvertes. En revanche, les principaux sites web pornographiques n'hébergeaient que 802 vidéos.

La majorité des femmes ciblées sont des célébrités, essentiellement des actrices et des musiciennes qui représentent 81 % des victimes, tandis que les autres victimes de deepfakes pornographiques sont victimisées dans ce que la chercheuse Claire Langlais-Fontaine décrit comme de l'abus sexuel basé sur des images dans le contexte d'(anciennes) relations (Langlais-Fontaine 2020).

Cyber flashing

Le cyber flashing consiste à envoyer des photos à caractère sexuel non sollicitées, en utilisant des applications de rencontre ou de messagerie ou via Airdrop (un mélange de Bluetooth et de Wi-Fi, créant une communication à double sens entre des téléphones qui se situent à moins de 10 mètres) ou Bluetooth. Ce comportement est observé sur les réseaux sociaux, les applications de messagerie, les applications de rencontre et, dans le cas des systèmes Airdrop/Bluetooth, dans les transports publics par exemple. Cette forme spécifique de harcèlement sexuel, exercé à la fois par des étrangers et des connaissances, peut relever du harcèlement qui se déroule dans des contextes de violence domestique, du harcèlement de rue, de l'exhibitionnisme (et du flashing) et du harcèlement sexuel perpétré par des étrangers ou des pairs (BBC 2019a).

---

18. Ministère de la Justice du Royaume-Uni (2019) , « Upskirting : know your rights » disponible en anglais sur : www.gov.uk/government/news/upskirting-know-your-rights
19. L'abus sexuel basé sur des images fait l'objet de la première discussion sur des aspects spécifiques (voir annexe 1).
20. Définie comme telle par Facebook (n.d.).

Harcèlement sexuel en ligne contenant de l'exploitation, de la contrainte et des menaces

La deuxième catégorie de harcèlement sexuel en ligne ajoute au harcèlement des femmes et des filles le recours à l'exploitation, à la contrainte et aux menaces. Ce deuxième groupe de harcèlement sexuel en ligne contient les différentes formes de violence énumérées ci-dessous.

Sexting forcé

On entend par sexting forcé le fait de harceler ou de faire pression sur une victime, en ligne, pour qu'elle partage des images d'elle la représentant nue ou qu'elle adopte un comportement sexuel en ligne (ou hors ligne).

Il ressort d'une étude récente que :

> les jeunes s'adonnent au sexting car ils subissent la pression de partenaires ou de partenaires potentiels (Döring, 2012 ; Lippman & Campbell, 2014). Dans le cadre d'une relation amoureuse, une pression est souvent exercée lorsqu'un des partenaires exige d'une personne avec laquelle il entretient une relation intime de lui envoyer du contenu sexuellement explicite, voire de participer à des échanges mutuels de tels contenus (Döring, 2012 ; Lippman & Campbell, 2014).
>
> Certaines filles consentent à s'adonner à du sexting « non désiré » car elles pensent qu'il s'agit d'un type de « conformité sexuelle » ou du « prix indésirable » à payer pour maintenir une bonne relation (Drouin & Tobin, 2014 ; Lippman & Campbell, 2014 ; Renfrow & Rollo, 2014). Généralement, les filles subissent une plus grande pression que les garçons pour s'adonner au sexting (Lippman & Campbell, 2014 ; Ringrose et al., 2012 ; Walker et al., 2013 ; Walgrave et al., 2013) (Dodaj et Sesar 2020).

Le sexting forcé peut devenir du sexting violent dans le contexte de la violence domestique, et aussi de l'abus sexuel basé sur des images ou de la sextortion.

Sextortion

La sextortion, et/ ou chantage à la webcam, est une forme croissante de violence en ligne qui consiste à menacer une personne de publier du contenu sexuel (images, vidéos, deepfakes, rumeurs sexuelles) à des fins d'intimidation, de contrainte ou de chantage pour obtenir de nouveaux contenus sexuels ou de l'argent, parfois les deux.

Roberta Liggett O'Malley et Karen M. Holt établissent différentes catégories d'auteurs de sextortion, et décrivent donc quatre différents types de sextortion : la cyber sextortion axée sur les mineurs ; la cyber sextortion usant de moyens illégaux ; la cyber sextortion violente entre partenaires intimes et la cyber sextortion criminelle transnationale (Liggett O'Malley 2020). Lorsque des enfants sont concernés, Europol conseille d'employer l'expression « contrainte et extorsion en ligne d'enfants à des fins sexuelles » étant donné que le terme sextortion « ne véhicule pas le message selon lequel l'acte en question implique l'abus et l'exploitation sexuels d'un enfant, entraînant des conséquences extrêmement graves pour la victime ».

En France par exemple, l'infraction est punissable depuis 2014 (2018) par l'article 11 de la loi n 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, qui punit le harcèlement sexuel en ligne, et par l'article 312-1 concernant l'extorsion. En Suisse en revanche, l'infraction n'existe pas, et les actes de sextortion peuvent être poursuivis en vertu de l'article 156 du CP (extorsion et chantage), de l'article 174 du CP (calomnie), de l'article 179^{quater} du CP (violation du domaine privé) ou de l'article 197 du CP (pornographie)[21], qui ne tiennent pas nécessairement compte de l'aspect genré de l'infraction.

Dans le cadre de la Convention d'Istanbul, la sextortion affectant les femmes et les filles peut être considérée comme une forme de harcèlement sexuel en ligne, tel qu'il est défini : « toute forme de comportement non désiré, verbal, non-verbal ou physique, à caractère sexuel, ayant pour objet ou pour effet de violer la dignité d'une personne, en particulier lorsque ce comportement crée un environnement intimidant, hostile, dégradant, humiliant ou offensant » avec les circonstances aggravantes potentielles suivantes : « l'infraction a été commise à l'encontre d'un ancien ou actuel conjoint ou partenaire, conformément au droit interne, par un membre de la famille, une personne cohabitant avec la victime, ou une personne ayant abusé de son autorité » et/ou « l'infraction a entraîné de graves dommages physiques ou psychologiques pour la victime ».

21. Code pénal suisse, disponible sur : www.admin.ch/opc/fr/classified-compilation/19370083/index.html#a156

Menaces de viol

Les menaces en ligne qui revêtent un caractère de violence sexuelle, comme les menaces de viol ciblant la victime ou ses proches, y compris ses enfants, les membres de sa famille, ses amis, etc., font partie des formes de violence que les femmes rencontrent le plus souvent en ligne. Selon le rapport intitulé « Toxic Twitter » publié par Amnesty International, « les menaces en ligne de violence à l'égard des femmes sont souvent sexualisées et comprennent des références spécifiques aux corps des femmes. Le but de la violence et de l'abus est de créer un environnement en ligne hostile pour les femmes dans l'intention de les stigmatiser, de les intimider, de les humilier, de les rabaisser ou de les réduire au silence » (Amnesty International 2018). Dans le rapport, Amnesty a constaté que 25 % des femmes interrogées, toutes actives sur Twitter, avaient reçu des menaces adressées à elles ou à leur famille, notamment des menaces de violence sexuelle, de souffrances physiques et de mort, ainsi que des incitations au suicide. Ces menaces cohabitent souvent avec d'autres formes de discours de haine basées sur l'identité perçue de la victime.

Doxing à caractère sexuel/genré

Comme pour les autres formes de doxing, des informations personnelles sont partagées en ligne sans le consentement de la victime pour inciter d'autres internautes à la harceler sexuellement. En France, les abus sexuels basés sur des images et associés au doxing se sont multipliés pendant les confinements liés à la pandémie de Covid-19, avec la production d'un nouveau type de comptes Snapchat ou Telegram appelés « *ficha* » (pour « afficher » : ridiculiser en public) (Khouiel/Vice 2020). Ces comptes locaux repostent des photos de jeunes femmes dénudées – parfois mineures – révélant à la fois leur identité et leurs coordonnées, et dirigent vers elles des meutes de prédateurs sexuels, dans leur communauté locale. Les *ficha*, qualifiés de partage non consenti d'images, sont érigés en infraction pénale, et les contrevenants encourent jusqu'à deux ans de prison et 60 000 euros d'amende.

Harcèlement à caractère sexuel

La troisième sous-catégorie de harcèlement sexuel en ligne consiste par exemple à diffuser des commérages ou des rumeurs sur le comportement sexuel allégué d'une victime, à afficher des commentaires à caractère sexuel sous les messages ou les photos de la victime, à usurper l'identité d'une victime et à diffuser des contenus à caractère sexuel ou à harceler sexuellement d'autres personnes, en portant ainsi atteinte à leur réputation et/ou à leurs moyens d'existence, ou à révéler l'orientation sexuelle ou l'identité de genre d'une personne sans son accord préalable ou à utiliser le deadnaming ou morinommage (utiliser le prénom de naissance d'une personne transgenre), dans l'intention de lui faire peur, de la menacer ou de l'amener à avoir honte de son corps (body-shaming).

Nous avons vu que le harcèlement sexuel en ligne revêt de nombreuses formes, certaines se confondant partiellement avec le discours de haine sexiste et genré et d'autres types de discours de haine et de harcèlement comme ceux basés sur l'orientation sexuelle et les identités de genre. Ces différents types de violence ne constituent pas tous des infractions pénales potentielles en soi. Mais la plupart d'entre eux sont banalisés et les victimes doivent les affronter seules.

Dispositions applicables de la Convention de Budapest

Les articles susmentionnés de la Convention d'Istanbul sur le harcèlement sexuel et les circonstances aggravantes peuvent être complétés et clarifiés par un ensemble de dispositions de la Convention de Budapest. La liste ci-dessous n'est pas exhaustive, et sert davantage d'exemple de dispositions matérielles de la Convention de Budapest potentiellement applicables à la facilitation du harcèlement sexuel en ligne.

Article 2 de la Convention de Budapest (Accès illégal)

> Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Un Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Cette disposition décrit l'action consistant à accéder illégalement au système de la victime, pratique courante dans le cadre de cybermenaces, de cyberharcèlement, de sextortion et d'autres formes d'atteintes à la vie privée relevant de la cyberviolence. Un contrevenant peut accéder illégalement au système d'un tiers et l'utiliser comme plateforme pour publier des messages, perpétrer des attaques ou voler des données intimes.

Article 3 de la Convention de Budapest (Interception illégale)

> Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Cette disposition décrit l'action consistant à intercepter des données sans en avoir le droit[22]. Elle concerne l'écoute, le contrôle ou la surveillance du contenu des communications, l'obtention ou l'enregistrement des données à caractère personnel (non publiques) d'une victime, par des moyens techniques. Le trafic entrant ou sortant peut être intercepté illégalement pour gêner la communication avec les forces de l'ordre ou pour montrer à la victime que l'agresseur sait tout ce qu'elle fait. Le trafic peut aussi être intercepté pour commettre des atteintes à la vie privée, notamment dans le cadre d'abus basés sur des images et de harcèlement.

Article 8 de la Convention de Budapest (Fraude informatique)

> Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui : a) par toute introduction, altération, effacement ou suppression de données informatiques, b) par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Certaines formes de sextortion peuvent être comprises comme une fraude informatique, étant donné que les auteurs peuvent extorquer des images privées ou menacer de le faire afin d'exiger une rançon de leurs victimes, parfois en utilisant des stratégies de piratage (CBC 2017).

Article 10 de la Convention de Budapest (Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes)

> 1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, (...) à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

Le rapport explicatif de la Convention précise également dans quels cas les atteintes à la propriété intellectuelle devraient être érigées en infraction pénale : « En vertu des instruments visés dans l'article, chaque Partie est tenue d'ériger en infraction pénale les atteintes délibérées à la propriété intellectuelle et aux droits connexes, parfois désignés sous le nom de droits voisins, lorsque ces atteintes ont été commises au moyen d'un système informatique et à une échelle commerciale. »

Dans les pays qui ne sont pas dotés d'une législation sur l'abus sexuel basé sur des images, la législation sur le droit d'auteur est sans doute le meilleur outil dont disposent les victimes (O'Connell et Bakina 2020).

22. « Sans droit » est défini de la manière suivante dans le rapport explicatif de la Convention de Budapest : « Comportement qui ne repose sur aucune compétence (législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou comportement qui n'est couvert ni par des exceptions légales, excuses et faits justificatifs établis ni par des principes de droit interne pertinents ». Voir Conseil de l'Europe (2001b).

Harcèlement en ligne et facilité par la technologie

L'article 34 de la Convention d'Istanbul définit le harcèlement comme « le fait, lorsqu'il est commis intentionnellement, d'adopter, à plusieurs reprises, un comportement menaçant dirigé envers une autre personne, conduisant celle-ci à craindre pour sa sécurité ». La convention appelle les Parties à ériger cet abus en infraction pénale. Le rapport explicatif de la convention affine la définition du harcèlement et inclut les technologies de l'information et de la communication (TIC) dans les moyens de commission de l'infraction :

> Le comportement menaçant peut consister dans le fait de suivre de manière répétée une personne, d'engager une communication non désirée avec une personne, ou de faire savoir à une autre personne qu'elle est épiée. Ceci inclut le fait de suivre physiquement une personne, d'apparaître sur son lieu de travail, son centre sportif ou son établissement scolaire, de même que la suivre dans le monde virtuel (espaces de discussion, sites de réseaux sociaux, etc.). Une « communication non désirée » désigne la poursuite d'un contact actif quel qu'il soit avec la victime par n'importe quel moyen de communication disponible, notamment les outils de communication modernes et les TIC (Conseil de l'Europe 2011b).

Les menaces en ligne (sexuelles, économiques, physiques ou psychologiques), les tentatives d'atteinte à la réputation de la victime, le suivi des activités en ligne de la victime afin de collecter des informations privées, l'usurpation d'identité, la sollicitation d'actes sexuels en se faisant passer pour la victime et la mise en place d'une campagne de harcèlement collectif visant à isoler la victime sont autant d'exemples de pratiques de harcèlement se déroulant dans la sphère numérique. La surveillance ou l'espionnage de la victime sur diverses plateformes en ligne ou par l'utilisation d'outils numériques est fréquemment utilisée comme stratégie par les auteurs pour mener à bien ces atteintes à la vie privée. Dans une étude allemande de grande échelle sur le cyberharcèlement, les auteurs ont observé que la majorité des victimes étaient des femmes, que la majorité des auteurs étaient des hommes, et que le cyberharcèlement se déroulait essentiellement dans le contexte de la violence domestique (Dreßing et al. 2014). Selon le sondage le plus récent de la FRA sur la violence à l'égard des femmes, dans l'UE, 14 % des femmes ont été harcelées sous la forme de messages ou d'appels insultants ou menaçants depuis l'âge de 15 ans (harcèlement au moyen de courriers électroniques, de textos ou d'Internet). Les jeunes femmes en particulier sont ciblées : dans l'UE, 4 % des femmes âgées de 18 à 29 ans avaient été harcelées au cours des 12 mois précédant l'entretien, contre 0,3 % des femmes de 60 ans ou plus (FRA 2014). Ces chiffres seront complétés par la prochaine étude de la FRA sur la violence à l'égard des femmes qui sera réalisée entre 2020 et 2022.

En outre, selon un récent rapport commandé par Women's Aid, 45 % des victimes de violences domestiques ont déclaré avoir subi des abus en ligne pendant la relation avec l'auteur des violences, et 48 % avoir fait l'objet de harcèlement ou d'abus en ligne de la part de l'ex-partenaire après avoir mis fin à la relation. Quelques 38 % ont signalé avoir subi une traque en ligne à l'issue de la relation et 75 % se sont dites préoccupées par le fait que la police ne savait pas comment répondre à l'abus ou au harcèlement en ligne. Parmi elles, 12 % avaient signalé des violences à la police et n'avaient pas été aidées (Laxton/Women's Aid 2014).

L'objectif principal du harcèlement en ligne et facilité par la technologie est de créer un sentiment de peur et de détresse chez la victime. C'est une question de pouvoir et de contrôle :

> Les femmes ayant survécu ont expliqué que des services de localisation avaient été installés sur leurs appareils et activés par leurs anciens partenaires ou partenaires actuels et que les enfants subissaient des pressions pour activer des fonctions vidéo pendant les appels téléphoniques avec leur père. En soi, cela peut être perçu comme des actes anodins. Toutefois, ces efforts étaient déployés pour exercer un contrôle : harceler et localiser une femme ou un refuge ou encore son nouveau domicile. Ainsi, Woodlock et moi-même proposons que le terme et le cadre de contrôle de contrainte numérique soient employés pour renvoyer à « l'utilisation et d'appareils et de médias numériques destinés à traquer, harceler, menacer et abuser de partenaires ou d'anciens partenaires et enfants » (Salter et al. 2018).

Dans ce qu'elle qualifie également de violence domestique et familiale facilitée par la technologie (Technology Domestic and Family violence – TDFV), le Dr Bridget Harris décrit le fait que les auteurs de violences utilisent des « dispositifs physiques (...) des comptes virtuels ou électroniques (...), et des logiciels ou des plateformes (...) » pour exercer de la violence et contraindre les victimes qui peuvent être des « partenaires intimes actuels ou anciens, leurs enfants, de futurs partenaires intimes, des amis ou des membres de la famille » (Harris 2020a). Pour l'auteure, « le terme TDFV est un terme générique, qui englobe tout un éventail de comportements, y

compris l'utilisation de la technologie pour commettre d'autres actes de violence (comme des abus sexuels et des abus financiers) et pour faciliter le traditionnel harcèlement (physique) ».

Certains auteurs ont recours à la surveillance ou à l'espionnage sur les réseaux sociaux ou aux services de messagerie en créant de faux comptes et en se liant d'amitié avec leur cible, ou en la suivant de manière anonyme, voire en demandant l'accès à des mots de passe. Dans une étude statistique sur le harcèlement perpétré par le biais des nouvelles technologies dans le contexte de la violence domestique, les chercheurs ont observé que 17 % des victimes avaient reçu une demande de mot de passe de leur agresseur (Woodlock 2017). D'autres ont recours à des solutions plus « high tech » pour effrayer, menacer et abuser de leurs victimes (voir la section suivante). Mais des solutions low tech comme le harcèlement sur les réseaux sociaux ou les applications de messagerie ne sont pas nécessairement moins nocives que les moyens high tech employés pour commettre l'infraction.

> Les contacts abusifs et obsessifs et le harcèlement via la technologie ont été identifiés comme une nouvelle tendance dans les affaires d'homicides et de filicides commis dans un contexte de violence domestique et familiale (...) Récemment, la NSW Death Review Team (2017, 134) a constaté que les agresseurs harcelaient les victimes dans 39 % des cas, avant l'agression finale, notant que dans plus de la moitié des cas 'l'agresseur avait recours à la technologie pour harceler la victime, comme l'envoi répété de textos, le fait de contrôler le téléphone de la victime de violence domestique, et de nouer des contacts avec la victime sur les réseaux sociaux / les sites de rencontre sous une fausse identité (ibid.).

En outre, les particularités des réseaux sociaux qui pourraient se révéler inoffensives dans des situations sans contrainte deviennent des moyens de commission de l'infraction :

> Les plateformes partent généralement du principe que les contacts potentiels sont amicaux, sinon neutres, et que la multiplication des contacts est quelque chose de positif. Facebook via une « personne que vous connaissez peut-être », Twitter via « qui suivre » et Instagram via une liste de « suggestions pour vous », encouragent les utilisateurs à sympathiser avec d'autres personnes ou à les suivre, sur la base d'associations mutuelles. Il peut s'agir d'une fonction utile de réseautage social, cependant, cela entraîne des implications et des facteurs déclenchants potentiels pour les femmes qui ont été exposées à des actes de violence commis par des personnes dans des cercles sociaux plus larges. Bivens (2015) a décrit comment ces outils, sans le savoir, ont mis en relation des femmes ayant survécu à des violences sexuelles avec leur agresseur, et le sentiment de détresse qu'ont ressenti certaines femmes. De même, des femmes ayant survécu à la violence domestique ont décrit des facteurs déclenchants qui ont conduit à ce qu'elles soient invitées à sympathiser avec des membres du réseau social de l'auteur, qui ont soutenu l'auteur ou se sont joints à lui pour commettre des abus (Harris and Woodlock, à paraître). Il ne fait aucun doute que la technologie peut contribuer à renforcer les réseaux de l'agresseur. DeKeseredy and Schwartz (1993 ; DeKeseredy, 1990), expliquent que, dans des sociétés patriarcales, ceux qui participent à la violence peuvent avoir des alliés qui pensent comme eux et développent, partagent et renforcent des idéologies et des valeurs qui soutiennent, justifient et banalisent la violence. Ces réseaux de soutien entre pairs étaient autrefois connectés au monde réel mais ils sont aujourd'hui encouragés par la technologie (ibid.).

Ci-dessous sont définis quelques moyens « high tech » utilisés par les auteurs pour harceler, surveiller et contrôler les femmes en ligne et par le biais des nouvelles technologies.

Logiciels espion/logiciels de harcèlement et traçage via GPS ou géolocalisation

Dans un sondage réalisé auprès de 70 foyers pour victimes de violence domestique basés aux Etats-Unis, la radio publique nationale (National Public Radio – NPR) a constaté que « 85 pourcent des foyers (ont déclaré) qu'ils (travaillaient) directement avec des victimes dont les agresseurs les avaient tracées à l'aide d'un GPS (...) Quelques foyers (ont déclaré) que les agresseurs offraient des iPhones à leurs enfants, pendant la séparation des parents, afin de suivre la maman (NPR 2014) ».

Dans une récente étude française sur la fréquence de la cyberviolence dans le contexte de la violence domestique, les chercheurs ont constaté que le « cyber-contrôle » et le « cyber harcèlement » étaient les formes les plus répandues de violence en ligne et facilitée par la technologie[23] : environ six ou sept personnes interrogées sur dix avaient subi ce type de violence. Parmi les personnes interrogées, 29 % avaient le sentiment que leur

23. Données recueillies auprès de 212 répondants.

(ancien) partenaire les avaient surveillés via un GPS ou un logiciel espion (Centre Hubertine Auclert 2018). En outre, 41 % des anciens partenaires des victimes avaient essayé de les contacter pour les humilier, les harceler ou les contrôler par le téléphone de leurs enfants (ibid.).

Un logiciel espion est un logiciel ou une application utilisé pour tracer « quelqu'un en connectant leur smartphone, leur tablette ou leur ordinateur à un espion » (NPR 2014). « Conçu pour être installé sur l'appareil portable d'une autre personne, ces applications espion, (...) sont considérées comme des « logiciels de harcèlement » dans le contexte de la violence entre partenaires intimes et fondée sur le genre. (...) Par ailleurs, plusieurs applications destinées à surveiller les enfants et les employés sont souvent détournées à des fins de surveillance d'un partenaire intime »[24]. Accessibles dans l'app store pour un coût inférieur à 200 dollars américains par an, ces applications peuvent être installées sur n'importe quel smartphone après quelques manipulations techniques (installation d'applications tierces). Grâce à ces applications, l'auteur peut directement contrôler ou harceler la victime ou pénétrer dans le téléphone de la victime pour la surveiller, lui donnant ainsi accès aux communications et aux lieux où se trouve la victime, y compris son historique de navigation, ses textos, e-mails, appels, réseaux sociaux, médias tels que photos et vidéos, mots de passe, y compris ses mots de passe de comptes bancaires et leur position GPS en temps réel.

D'un point de vue juridique, ces types d'abus sont compris dans différents cadres. Certains pays classent le cyber contrôle et la surveillance via des logiciels espion comme une violation des communications privées et de la vie privée en général. À titre d'exemple, la France a choisi de qualifier ainsi ces infractions, et des circonstances aggravantes ont été prises en considération dans le contexte de la violence domestique dans quelques affaires seulement. Le pays a récemment actualisé sa loi sur la violence domestique pour y inclure notamment la surveillance par GPS (Legifrance 2020). En Espagne, le fait d'accéder au téléphone portable d'un(e) partenaire ou d'un(e) ami(e) sans son consentement est décrit par l'article 197 du Code pénal comme un crime de découverte et divulgation de secrets.

Les sanctions infligées sont des peines de prison comprises entre trois et cinq ans. Les peines peuvent être plus lourdes dans le contexte d'une relation intime (jusqu'à cinq ans de prison)[25]. Le code pénal allemand contient une section sur le harcèlement (Section 238.2), qui tient compte de cet aspect :

> « Tenter d'entrer en contact avec l'autre personne au moyen des télécommunications ou d'autres moyens de communication ou par l'intermédiaire de tiers », 238.3. « Faire une utilisation inappropriée des données à caractère personnel de l'autre personne aux fins a) de commander des produits ou des services pour cette personne ou b) d'inciter des tiers à établir un contact avec cette personne » et 238.4. « menacer l'autre personne, un des membres de sa famille, ou un de ses proches de porter atteinte à sa vie, à son intégrité physique, à sa santé ou à sa liberté » (Code pénal allemand 1998/2019).

L'installation d'une application ou d'un logiciel sur le téléphone ou l'ordinateur de quelqu'un comme un virus, un logiciel malveillant ou un cheval de Troie est généralement perçu comme un cybercrime par le grand public. L'installation d'un logiciel de harcèlement sur l'appareil d'une victime est comprise dans le même cadre par Europol par exemple, mais ces cadres ne tiennent pas compte du contexte de la violence domestique en tant que circonstance aggravante (Europol n.d.).

Les dispositions de la Convention d'Istanbul sur le harcèlement s'appliquent au harcèlement en ligne et facilité par la technologie, le harcèlement en ligne y étant défini comme « le fait, lorsqu'il est commis intentionnellement, d'adopter, à plusieurs reprises, un comportement menaçant dirigé envers une autre personne, conduisant celle-ci à craindre pour sa sécurité », ainsi que la disposition sur la violence psychologique comme « le fait, lorsqu'il est commis intentionnellement, de porter gravement atteinte à l'intégrité psychologique d'une personne par la contrainte ou les menaces ». Les circonstances aggravantes énoncées à l'article 46, paragraphes a, b, c, d et h, pourraient également s'appliquer au harcèlement commis en ligne ou par l'utilisation de moyens numériques. En outre, dans des situations menaçantes pour la vie impliquant l'utilisation de ces outils technologiques, l'article 52 sur les ordonnances d'urgence d'interdiction pourrait également s'appliquer :

> Les Parties prennent les mesures législatives ou autres nécessaires pour que les autorités compétentes se voient reconnaître le pouvoir d'ordonner, dans des situations de danger immédiat, à l'auteur de violence

24. Guzmán, L., Responsible Data (2019), « Addressing stalkerware and gender-based abuse through data protection law » disponible en anglais sur : https://responsibledata.io/rd-reflection-stories/addressing-stalkerware-and-gender-based-abuse-through-data-protection-law/.
25. Code pénal espagnol, disponible sur : https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

domestique de quitter la résidence de la victime ou de la personne en danger pour une période de temps suffisante et d'interdire à l'auteur d'entrer dans le domicile de la victime ou de la personne en danger ou de la contacter. Les mesures prises conformément au présent article doivent donner la priorité à la sécurité des victimes ou des personnes en danger.

Effrayer, menacer et contrôler via l'internet des objets (IdO)

En 2020, 50 milliards d'objets connectés étaient utilisés dans le monde entier, comme la domotique et les appareils domestiques intelligents utilisés pour contrôler différents dispositifs dont des thermostats ou des ampoules, des télécommandes ou des enceintes sans fil. On peut citer parmi d'autres appareils connectés les voitures, caméras de sécurité, drones domestiques et babyphones, appareils de santé intelligents utilisés pour suivre l'activité physique d'une personne ou pour injecter des médicaments, comme des pompes à insuline, des appareils portables comme des appareils Fitbits, des casques connectés, des montres ou des lunettes de réalité virtuelle, etc. Tous ces outils et appareils ont en commun le fait qu'ils sont connectés à internet et peuvent donc être activés et contrôlés à distance.

L'analyse juridique met en évidence quatre différentes faiblesses juridiques dans le paysage de l'internet des objets : la discrimination ancrée, le respect de la vie privée, des failles de sécurité et des lacunes au niveau du consentement (Peppet 2014). Bien que les questions de discrimination, de respect de la vie privée et de consentement touchent les femmes de manière spécifique, notre étude se contentera d'examiner comment les questions de sécurité structurelle des appareils et outils de l'internet des objets mettent les femmes en danger, en les exposant au harcèlement dans le contexte de la violence domestique.

La recherche sur les répercussions du harcèlement, du contrôle et des abus facilités par l'internet des objets dans le contexte de la violence domestique se trouve encore à un stade embryonnaire, mais avec 125 milliards d'outils et d'appareils de l'internet des objets attendus en 2030 (Markit 2017), il est de plus en plus nécessaire de tenir compte de ces types de violence et de l'utilisation des outils et appareils de l'internet des objets dans le cadre de la collecte de données sur la violence domestique et de l'incrimination de cette infraction.

Il ressort d'une enquête menée par le *New York Times* auprès de 30 victimes de violence domestique, avocats, personnes travaillant dans des foyers et premiers intervenants ce qui suit :

> Une femme avait allumé son climatiseur, mais a déclaré qu'il s'était ensuite éteint sans qu'elle le touche. Une autre femme a indiqué que le code sur le clavier numérique de sa porte d'entrée changeait tous les jours, sans qu'elle comprenne pourquoi. Une autre femme a déclaré à une permanence téléphonique qu'elle entendait sonner à la porte d'entrée mais que personne n'était là (...) Les auteurs de violences – en utilisant des applications sur leurs smartphones, qui sont connectés à des dispositifs reliés à internet – contrôleraient à distance des objets du quotidien dans la maison, parfois pour observer et écouter, d'autres fois pour effrayer ou montrer leur pouvoir. Même lorsqu'un partenaire avait quitté le domicile, les appareils restaient souvent en place et continuaient d'être utilisés pour intimider et semer la confusion.

Un auteur n'a donc pas besoin d'être physiquement présent pour rester connecté à sa victime et exercer un contrôle, une contrainte et des abus. Pour la victime, la perspective d'être observée et surveillée en permanence et le fait de voir des objets participer à la privation de liberté et à des souffrances physiques et émotionnelles et à des difficultés économiques peuvent avoir un impact psychologique fort pouvant se traduire par de l'anxiété et de la dépression, voire de la psychose et conduire jusqu'au suicide. En effet,

> Les serrures connectées à internet peuvent restreindre les mouvements à certaines pièces ou même empêcher une personne de sortir de chez elle. Les assistants virtuels contrôlés par la voix peuvent donner un compte rendu détaillé des questions qui leur ont été posées et de l'historique des recherches (...) ces systèmes ont également tendance à exiger un compte administrateur, qui donne à une seule personne du foyer le moyen, protégé par un mot de passe, de contrôler le système (BBC 2020).

Il est donc indispensable, au niveau de ce secteur d'activité, de mettre en œuvre le principe de la sécurité et du respect de la vie privée dès la conception mais aussi de garantir que ces objets et outils sont conçus en ne

perdant pas de vue l'intérêt de l'utilisateur le plus vulnérable. Cependant, selon le Dr Leonie Tanczer, conférencière en sécurité internationale et technologies émergentes et cheffe du projet « Gender and IoT » (#GIoT)[26] :

> on ne pourra pas résoudre des problèmes sociaux seulement par des moyens techniques. En outre, les services réglementés tels que les services répressifs, les responsables de l'élaboration des politiques et les établissements d'enseignement, ainsi que les organisations de défense des droits des femmes et les refuges, doivent être intégrés dans la conception de ces systèmes et informés de ce risque (Morrow 2019).

Dispositions applicables de la Convention de Budapest

Les articles de la Convention d'Istanbul sur le harcèlement et les circonstances aggravantes énumérés ci-dessus peuvent être complétés par un ensemble de dispositions de la Convention de Budapest. Certaines des dispositions mentionnées ci-après présentent un lien direct avec la violence à l'égard des femmes en ligne et facilitée par la technologie, en particulier le cyberharcèlement, tandis que d'autres prévoient l'incrimination d'actes qui pourraient intervenir dans le cyberharcèlement, mais le lien est moins direct (Conseil de l'Europe 2018c). De tels actes pourraient faciliter la violence et à ce titre donner lieu à des poursuites, mais les dispositions qui suivent ne suffiraient pas en soi à incriminer la violence elle-même.

Article 2 de la Convention de Budapest (Accès illégal)

> Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Cette disposition peut donc être comprise comme le fait d'accéder aux outils numériques d'une victime (ordinateur, tablette ou téléphone ou outils connectés) via un logiciel de harcèlement ou le piratage. L'accès illégal est défini de la manière suivante dans le rapport explicatif de la convention :

> créer une menace ou [à] attenter à la sécurité (c'est-à-dire la confidentialité, l'intégrité et la disponibilité) des systèmes et données informatiques. (...) L' « accès » comprend la pénétration dans l'intégralité ou un partie quelconque d'un système informatique (matériel, composantes, données stockées du système installé, répertoires, données relatives au trafic et au contenu).

Article 3 de la Convention de Budapest (Interception illégale)

> Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. un Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Cette disposition décrit l'action qui consiste à intercepter les données personnelles (non publiques) d'une victime sans droit, soit en installant un logiciel sur ses appareils en vue d'intercepter ces données, soit en pénétrant dans ses appareils par des moyens techniques. En effet, le rapport explicatif de la Convention de Budapest précise que :

> L'interception effectuée par des « moyens techniques » concerne l'écoute, le contrôle ou la surveillance du contenu des communications, et l'obtention du contenu soit directement, au moyen de l'accès au système informatique et de son utilisation, soit indirectement, au moyen de l'emploi de dispositifs d'écoute. L'interception peut aussi consister en un enregistrement des données.

26. « Gender and IoT », disponible uniquement en anglais sur : https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot.

Cet article pourrait donc s'appliquer à la facilitation du cyberharcèlement, car il prévoit l'incrimination d'actes qui peuvent intervenir dans ce type de violence, mais il ne suffit pas en soi à ériger en infraction pénale le cyberharcèlement dans toutes ses dimensions.

Article 4 de la Convention de Budapest (Atteinte à l'intégrité des données)

> 1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2) Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Dans le contexte de la violence domestique, cette forme d'abus peut avoir lieu lorsqu'un partenaire ou ancien partenaire violent détruit ou supprime les outils, les appareils ou les contenus de la victime à des fins de contrôle ou de vengeance. La notion de « dommages sérieux » devrait être comprise dans le contexte plus large de la violence domestique et devrait toujours être considérée comme une circonstance aggravante. Cet article pourrait s'appliquer à la facilitation de la violence et à la violence elle-même, à l'instar de l'article 5 ci-dessous (l'atteinte à l'intégrité des données ou du système étant susceptible de causer la mort ou des dommages physiques et psychologiques).

L'article 5 de la Convention de Budapest (Atteinte à l'intégrité du système)

> Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Dans le cas des tactiques de harcèlement utilisées dans la violence domestique, l'atteinte à l'intégrité des données d'une victime et la destruction de ces données, sans droit, par un auteur, pourraient entrer dans le champ d'application de ces deux dispositions. Les « dommages sérieux » résultant de cette action et « l'entrave grave » devraient être appréciés en termes de répercussions sur la victime dans un contexte de violence domestique.

Article 6 de la Convention de Budapest (Abus de dispositifs)

> Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit : a) la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition : 1) d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ; 2) d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ; et b) la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

Cette disposition est particulièrement intéressante dans le contexte des logiciels de harcèlement, lorsqu'un auteur possède « un élément (...) dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions (Conseil de l'Europe 2001a) » décrites précédemment, comme l'accès illégal et l'atteinte à l'intégrité du système et des données.

Formes de violence psychologique en ligne et facilitées par la technologie

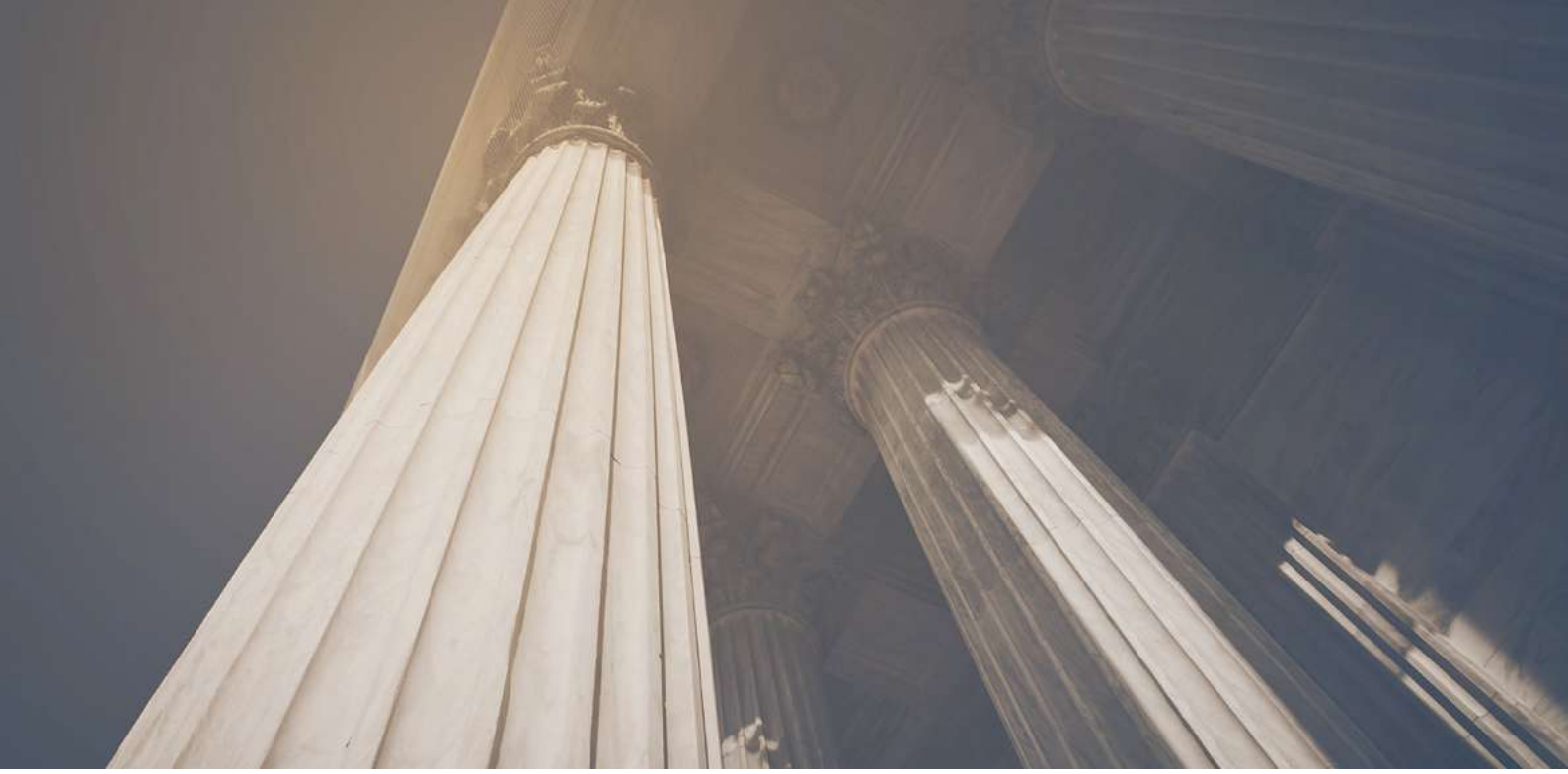
Les types de violence décrits ci-dessus peuvent aussi relever de la violence psychologique. La Convention d'Istanbul décrit la violence psychologique comme « *le fait, lorsqu'il est commis intentionnellement, de porter gravement atteinte à l'intégrité psychologique d'une personne par la contrainte ou les menaces* ». Le rapport explicatif de la convention complète la définition de la violence psychologique comme suit :

> L'étendue de l'infraction est limitée au comportement intentionnel qui, par des moyens et méthodes diverses, porte gravement atteinte et porte préjudice à l'intégrité psychologique d'une personne. La convention ne définit pas ce qui constitue une atteinte grave. Pour qu'un comportement relève de cette disposition, il doit être fait usage de la contrainte ou de menaces. (...) Cette disposition fait référence à un comportement et non à un événement ponctuel. Elle vise à saisir la nature pénale d'un comportement violent qui se produit dans le temps – à l'intérieur ou à l'extérieur de la famille (Conseil de l'Europe 2011b).

Toutes les formes de violence à l'égard des femmes en ligne et facilitées par la technologie ont des conséquences psychologiques et pourraient donc être considérées comme des violences psychologiques qui s'exercent en ligne ou qui supposent le recours à la technologie. En effet, les caractéristiques spécifiques de la violence à l'égard des femmes en ligne et facilitée par la technologie détaillées dans le premier chapitre amplifient leurs répercussions sur les victimes. De plus, les technologies numériques peuvent être utilisées à mauvais escient par les auteurs de violences domestiques afin d'intensifier la gravité de la violence psychologique exercée sur la victime (voir les sections sur le harcèlement moral et le harcèlement sexuel en ligne). Boukemidja (2018) ajoute :

> concernant la violence psychologique, elle consiste à dénigrer, humilier, dégrader la femme dans sa valeur humaine. Elle se manifeste par des agressions verbales, des insultes, des scènes de jalousie, des menaces, une pression, du chantage, le contrôle d'activités, le fait d'isoler la femme de ses proches, de ses amis et du monde extérieur. (...) la violence verbale est la répétition permanente de propos insultants ou d'insultes envers une femme. (...) la violence verbale peut entraîner toute une série de problèmes comportementaux, émotionnels et physiques. Dans ce contexte, la violence verbale se traduit par des propos blessants ou humiliants, comme le fait de donner un surnom ridicule à une femme, de l'insulter, de tenir des propos racistes ou de la taquiner sans cesse.

L'incitation au suicide ou à l'automutilation par le biais des communications numériques est un autre phénomène en expansion, dont les effets sont intensifiés par l'anonymat dont disposent les auteurs en ligne, la longévité des contenus et la facilité avec laquelle il est possible de réunir un grand nombre d'auteurs pour commettre une attaque de masse contre la victime. Les victimes sont poussées à se suicider ou à s'automutiler en ligne, parfois sur des sites web dédiés et sur les réseaux sociaux, et les filles ont davantage tendance à s'automutiler que les garçons (Morgan et al. 2017). Des hashtags dédiés sur les réseaux sociaux peuvent donc inciter les filles vulnérables à s'automutiler pour des questions de visibilité ou augmenter leur nombre de followers (BBC 2019b).



CHAPITRE VI

DISPOSITIONS PERTINENTES DE LA CONVENTION D'ISTANBUL ET DE LA CONVENTION DE BUDAPEST

Les quatre piliers de la Convention d'Istanbul sur les politiques intégrées, la prévention, la protection et les poursuites constituent la spécificité de l'approche complète et globale adoptée par la convention. Ces piliers permettent aux parties d'élaborer un ensemble exhaustif de mécanismes de réponse concernant tous les aspects de la violence à l'égard des femmes et de la violence domestique.

Lorsqu'elles présentent un intérêt pour bien comprendre le phénomène de la violence à l'égard des femmes en ligne et facilitée par la technologie, les dispositions de la Convention d'Istanbul seront commentées et analysées. Lorsque les dispositions de la Convention de Budapest peuvent compléter efficacement celles de la Convention d'Istanbul, elles seront incluses dans le commentaire. Cela s'applique essentiellement aux dispositions de la Convention de Budapest relatives au droit procédural et à la coopération internationale.

Politiques intégrées

Politiques globales et coordonnées (article 7)

Aux termes de l'article 7 :

> 1) Les Parties prennent les mesures législatives et autres nécessaires pour adopter et mettre en œuvre des politiques nationales effectives, globales et coordonnées, incluant toutes les mesures pertinentes pour prévenir et combattre toutes les formes de violence couvertes par le champ d'application de la présente Convention, et offrir une réponse globale à la violence à l'égard des femmes ;
>
> 2) Les Parties veillent à ce que les politiques mentionnées au paragraphe 1 placent les droits de la victime au centre de toutes les mesures et soient mises en œuvre par le biais d'une coopération effective entre toutes les agences, institutions et organisations pertinentes ;
>
> 3) Les mesures prises (...) doivent impliquer, le cas échéant, tous les acteurs pertinents tels que les agences gouvernementales, les parlements et les autorités nationales, régionales et locales, les institutions nationales des droits de l'homme et les organisations de la société civile.

Les politiques effectives, globales et coordonnées que les Parties sont tenues de prendre pour prévenir et combattre les formes de violence devraient aussi globalement tenir compte des formes de harcèlement et de violence psychologique en ligne et facilitées par la technologie.

Pour offrir une réponse globale à cette forme de violence, il faut que les initiatives de prévention et les cadres juridiques civils et pénaux soient régulièrement mis à jour pour tenir compte des types spécifiques et émergents de violence que les femmes rencontrent en ligne et via les nouvelles technologies, surtout dans le contexte de la violence domestique (dont les enfants victimes ou témoins de violence domestique) ou lorsque ces types de violence ciblent des groupes de femmes qui sont déjà visées par des menaces intersectionnelles.

Les organes de gouvernance locaux et nationaux, les institutions judiciaires, sociales et de santé devraient être dotés de ressources humaines et financières suffisantes pour lutter contre ces formes de violence, y compris pour nouer un dialogue interinstitutionnel et pour établir des mécanismes de contrôle et d'évaluation destinés à évaluer les progrès et les répercussions des politiques et des initiatives coordonnées entre les agences et les secteurs.

Ressources financières (article 8)

> Les Parties allouent des ressources financières et humaines appropriées pour la mise en œuvre adéquate des politiques intégrées, mesures et programmes visant à prévenir et combattre toutes les formes de violence couvertes par le champ d'application de la présente Convention, y compris ceux réalisés par les organisations non gouvernementales et la société civile.

Des ressources financières et humaines suffisantes sont nécessaires au niveau national et local pour prévenir, combattre et offrir une protection contre les formes de violence à l'égard des femmes en ligne et facilitées par la technologie. En outre, il faudrait veiller à ce que des ressources financières et humaines soient mises à disposition pour la coordination intersectorielle aux niveaux national et local.

Il faudrait encourager l'élaboration de budgets clairs, transparents, pertinents et sensibles au genre tenant compte des montants spécifiquement attribués à la prévention, à la protection et à la poursuite de toutes les formes de violence à l'égard des femmes. Par conséquent, ces budgets devraient aussi intégrer les ressources affectées à une réponse globale aux formes de harcèlement et de violence psychologique en ligne et facilitées par la technologie touchant les victimes et les personnes à leur charge. Des ressources financières et humaines devraient également être consacrées à la collecte de données et aux recherches concernant ces types de violence (voir aussi article 11 de la Convention d'Istanbul).

Organisations non gouvernementales et société civile (article 9)

> Les Parties reconnaissent, encouragent et soutiennent, à tous les niveaux, le travail des organisations non gouvernementales pertinentes et de la société civile qui sont actives dans la lutte contre la violence à l'égard des femmes et établissent une coopération effective avec ces organisations.

Les organisations de la société civile, les organisations de défense des droits des femmes et les organisations non gouvernementales ont toujours été à l'origine d'un grand nombre d'initiatives en faveur des victimes de violence à l'égard des femmes fondée sur le genre. Souvent, ces organisations sont encore chargées de ces initiatives, et si dans de nombreux pays elles bénéficient de fonds publics, leur sécurité financière et la qualité/volume des services consacrés aux victimes sont souvent remis en cause en raison d'une pénurie de ressources, de possibilités de financement insuffisantes sur le long terme ou de transformations du paysage politique, entre autres.

Les organisations qui exercent des responsabilités en matière de lutte contre la violence domestique et d'autres formes de violence touchant les femmes devraient donc recevoir un soutien financier suffisant pour leur permettre également d'inclure dans leurs cadres et programmes d'action une réponse aux formes de harcèlement et de violence psychologique en ligne et facilitées par la technologie. Une meilleure coopération, consultation et gouvernance entre les organes publics chargés de la protection des droits des femmes et ce secteur devraient être encouragées pour promouvoir la création et le maintien du plus grand nombre possible d'initiatives ainsi que la coopération dans ce cadre ; cela inclut des initiatives de prévention telles que des campagnes de sensibilisation, la collecte de preuves et des recherches ainsi que des mécanismes de protection pour les victimes de violence à l'égard des femmes en ligne et facilitée par la technologie, plus particulièrement dans les affaires de violence domestique, et en cas de menaces transversales.

Organe de coordination (article 10)

> 1) Les Parties désignent ou établissent un ou plusieurs organes officiels responsables pour la coordination, la mise en œuvre, le suivi et l'évaluation des politiques et des mesures prises afin de prévenir et combattre toutes les formes de violence couvertes par la présente Convention. Ces organes coordonnent la collecte des données mentionnées à l'article 11, analysent et en diffusent les résultats.
>
> 2) Les Parties veillent à ce que les organes désignés ou établis conformément au présent article reçoivent des informations de nature générale portant sur les mesures prises conformément au chapitre VIII.
>
> 3) Les Parties veillent à ce que les organes désignés ou établis conformément au présent article aient la capacité de communiquer directement et d'encourager des relations avec leurs homologues dans les autres Parties.

Des organes de coordination spécifiques sont établis pour examiner tous les aspects du phénomène de la violence à l'égard des femmes fondée sur le genre, dans tous les secteurs, et sont chargés d'examiner non seulement la dimension hors ligne de la violence à l'égard des femmes mais également l'importance de cette forme de violence lorsqu'elle est perpétrée en ligne et facilitée par la technologie. Ils peuvent être assistés dans leur mission par des observatoires nationaux ou d'autres mécanismes chargés de contrôler et de collecter des données sur la violence à l'égard des femmes ; le contrôle de toutes les données sur les formes de violence à l'égard des femmes en ligne et facilitées par la technologie devrait être intégré dans ces mécanismes. Les observations de chaque partie pourraient contribuer à mettre en place des outils de comparaison afin d'évaluer les progrès et de comparer la situation des droits des femmes et la sécurité des femmes en ligne avec l'utilisation de nouvelles technologies.

Collecte des données et recherche (article 11)

Aux termes de l'article 11, les Parties

> s'engagent à collecter les données statistiques désagrégées pertinentes, à intervalle régulier, sur les affaires relatives à toutes les formes de violence couvertes par le champ d'application de la présente Convention ; à soutenir la recherche dans les domaines relatifs à toutes les formes de violence couvertes par le champ d'application de la présente Convention, afin d'étudier leurs causes profondes et leurs effets, leur fréquence et les taux de condamnation, ainsi que l'efficacité des mesures prises pour mettre en œuvre la présente Convention (...) effectuer des enquêtes basées sur la population, à intervalle régulier, afin d'évaluer l'étendue et les tendances de toutes les formes de violence couvertes par le champ d'application de la présente Convention (...), fournissent les informations collectées, (...) au groupe d'experts (...) afin de stimuler la coopération internationale et de permettre une comparaison internationale (...) [et] veillent à ce que les informations collectées conformément au présent article soient mises à la disposition du public.

La collecte de données ventilées et la recherche revêtent une importance particulière s'agissant de ces nouvelles formes de violence se produisant en ligne ou facilitées par la technologie. En effet, ainsi que cela a été précisé lors de la classification des types de violence dans le cadre de la Convention d'Istanbul, certaines formes de harcèlement ou de persécution nécessitent des définitions spécifiques et une analyse approfondie pour les distinguer d'autres types de violence dépourvus d'une dimension de genre. La collecte de données est essentielle pour comprendre le contexte de la violence et servir de base à l'élaboration des décisions politiques et à la modification de la législation. À titre d'exemple, en ce qui concerne la violence domestique, il est particulièrement important de consigner la relation entre l'auteur et la ou les victimes ainsi que les circonstances aggravantes potentielles (le nombre d'auteurs, la durée des abus, la durée de vie des données, le chevauchement de plusieurs types de violence simultanément, l'implication des enfants de la victime ou l'impact sur ces enfants, etc.). En outre, la collecte de données concernant la fréquence et les taux de condamnation, y compris des données sur la justice civile (comme des ordonnances d'injonction), est particulièrement nécessaire pour évaluer l'impact de ces types de violence au niveau sociétal et pour fournir des éléments contribuant à l'élaboration de politiques efficaces. Les données sur les suicides ou les tentatives de suicide, les féminicides et les filicides pourraient inclure des informations sur les antécédents de harcèlement ou de violence psychologique exercés par le biais des nouvelles technologies – pour des questions d'incrimination et pour évaluer la fréquence et le rôle de ces formes de violence dans les infractions. Il faudrait vivement encourager la mise à disposition de ces données au grand public afin de le sensibiliser à ces formes de violence.

Il faudrait ventiler les données sur l'accès aux foyers, aux centres de santé, aux centres de ressources pour femmes et aux services sociaux et de santé pour tenir compte de ces formes de violence dans l'histoire de la victime et des femmes, et il faudrait pouvoir demander aux enfants demandeurs d'asile s'ils ont subi ces types de violence avant ou pendant leur voyage.

En outre, il faudrait encourager l'élaboration d'enquêtes, de méthodes de collecte des données et d'initiatives de recherche qui examinent les répercussions de ces types de violence dans l'objectif de les mesurer, y compris d'un point de vue financier, étant donné qu'il s'agit d'une étape importante pour inclure ces types de violence dans les cadres juridiques généraux, aux niveaux national et international. La collecte de données devrait toujours inclure une perspective intersectionnelle pour qu'elles soient aussi détaillées que possible.

Toutes ces données devraient être collectées et traitées conformément aux obligations qui incombent aux Parties en matière de protection des données. En outre, s'agissant des données spécifiques sur la violence commise sur les réseaux sociaux, les Parties devraient être encouragées à exiger une plus grande transparence et responsabilité des réseaux sociaux, ainsi que des gestionnaires de domaines et propriétaires/administrateurs de forums concernant la disponibilité de données détaillées sur la violence à laquelle les femmes sont confrontées sur ces plateformes (Algorithm Watch 2020 ; Amnesty International 2020).

Prévention

Obligations générales (article 12)

> 1) Les Parties prennent les mesures nécessaires pour promouvoir les changements dans les modes de comportement socioculturels des femmes et des hommes en vue d'éradiquer les préjugés, les coutumes, les traditions et toute autre pratique fondés sur l'idée de l'infériorité des femmes ou sur un rôle stéréotypé des femmes et des hommes.
>
> 2) Les Parties prennent les mesures législatives et autres nécessaires afin de prévenir toutes les formes de violence couvertes par le champ d'application de la présente Convention par toute personne physique ou morale.
>
> 3) Toutes les mesures prises conformément au présent chapitre tiennent compte et traitent des besoins spécifiques des personnes rendues vulnérables du fait de circonstances particulières, et placent les droits humains de toutes les victimes en leur centre.
>
> 4) Les Parties prennent les mesures nécessaires afin d'encourager tous les membres de la société, en particulier les hommes et les garçons, à contribuer activement à la prévention de toutes les formes de violence couvertes par le champ d'application de la présente Convention.
>
> 5) Les Parties veillent à ce que la culture, la coutume, la religion, la tradition ou le prétendu « honneur » ne soient pas considérés comme justifiant des actes de violence couverts par le champ d'application de la présente Convention.
>
> 6) Les Parties prennent les mesures nécessaires pour promouvoir des programmes et des activités visant l'autonomisation des femmes ».

Les stéréotypes et les préjugés, y compris les coutumes, la religion et la tradition ou le prétendu « honneur », constituent le cœur du continuum de la violence à l'égard des femmes qui se manifeste en ligne. En outre, les femmes qui ont plusieurs identités, telles que les lesbiennes, les bi, les femmes queer et les femmes transgenre, les femmes noires, les femmes appartenant à des minorités religieuses ou perçues comme telles, les femmes migrantes, les femmes en situation de handicap et de maladies chroniques, les femmes qui ont des difficultés économiques et les filles des moins de 18 ans, risquent tout particulièrement d'être la cible de préjugés néfastes qui se traduisent par des comportements violents en ligne et par le biais des nouvelles technologies. Les initiatives qui visent à modifier les stéréotypes préjudiciables et à promouvoir le changement au niveau sociétal pour une plus grande égalité entre les femmes et les hommes auront donc une incidence positive sur les comportements en ligne et hors ligne. Les initiatives et les programmes visant l'autonomisation et les représentations positives des femmes en ligne devraient également être plus répandues. Ces initiatives, lorsqu'elles sont nombreuses, contribuent à lutter contre les stéréotypes préjudiciables qui peuvent déferler sur les réseaux sociaux et affecter les femmes, en particulier celles qui présentent des vulnérabilités croisées.

Au-delà des changements socioculturels dans le domaine de l'égalité entre les femmes et les hommes, il est important que les cadres juridiques tiennent compte de toutes les formes de violence à l'égard des femmes, y

compris les types de harcèlement, de violence psychologique et de discours de haine que nous avons examinés plus haut. Sans modification de la législation et de la réglementation, les nouveaux cas de violence facilitée par les nouvelles technologies continueront de se traduire par l'impunité des auteurs. Au-delà de l'évolution juridique, le rôle du secteur de la justice est déterminant pour conférer une dimension de genre aux lois existantes au moyen de la jurisprudence.

En outre, il est essentiel qu'une perspective intersectionnelle soit appliquée dans les projets, les initiatives, les programmes et les lois qui visent à prévenir la violence en ligne et facilitée par la technologie et à répondre à ses différentes formes, afin d'accorder une place centrale aux victimes, et notamment de tenir compte des vulnérabilités croisées lors de la conception de ces mécanismes.

De plus, Les hommes et les garçons devraient être impliqués à la lutte contre les stéréotypes préjudiciables et être formés pour encourager des comportements sains en ligne, comme le fait d'être un « spectateur actif », surtout dans les sphères à dominante masculine comme les communautés de jeux vidéo (Active Bystander UK (n.d.) ; Glitch UK (n.d.)) ou lorsque des formes spécifiques de violence en ligne online sont observées, comme des agressions collectives et du harcèlement ciblé. En outre, l'éducation numérique généralisée pourrait contribuer à éradiquer le « recrutement » potentiel de jeunes hommes et de garçons dans des groupes extrémistes qui sévissent en ligne, qui font la promotion de stéréotypes négatifs sur les femmes et appellent même à la violence contre elles, comme la sous-culture « incel » (célibat involontaire), qui a donné lieu à des féminicides collectifs réels dans le passé et continue d'encourager les actes de violence quotidiens allant du harcèlement aux agressions.

Sensibilisation (article 13)

> 1) Les Parties promeuvent ou conduisent, régulièrement et à tous les niveaux, des campagnes ou des programmes de sensibilisation y compris en coopération avec les institutions nationales des droits de l'homme et les organes compétents en matière d'égalité, la société civile et les organisations non gouvernementales, notamment les organisations de femmes, le cas échéant, pour accroître la prise de conscience et la compréhension par le grand public des différentes manifestations de toutes les formes de violence couvertes par le champ d'application de la présente Convention et leurs conséquences sur les enfants, et de la nécessité de les prévenir.
>
> 2) Les Parties assurent une large diffusion parmi le grand public d'informations sur les mesures disponibles pour prévenir les actes de violence couverts par le champ d'application de la présente Convention.

Il faudrait encourager l'organisation de campagnes de sensibilisation sur les différents types de violence à l'égard des femmes en ligne et facilitée par la technologie, dans tous les secteurs de la société, y compris dans la filière où les produits sont conçus. En outre, le grand public devrait avoir connaissance des lois qui sanctionnent ces formes de violence, ainsi que la disponibilité des services dédiés et des lignes directrices sur les réponses à apporter à cette forme de violence au niveau des victimes. La coopération avec les acteurs du numérique devrait être priorisée, de sorte que les campagnes de sensibilisation trouvent également un écho en ligne.

Éducation (article 14)

> 1) Les Parties entreprennent, le cas échéant, les actions nécessaires pour inclure dans les programmes d'étude officiels et à tous les niveaux d'enseignement du matériel d'enseignement sur des sujets tels que l'égalité entre les femmes et les hommes, les rôles non stéréotypés des genres, le respect mutuel, la résolution non violente des conflits dans les relations interpersonnelles, la violence à l'égard des femmes fondée sur le genre, et le droit à l'intégrité personnelle, adapté au stade de développement des apprenants.
>
> 2) Les Parties entreprennent les actions nécessaires pour promouvoir les principes mentionnés au paragraphe 1 dans les structures éducatives informelles ainsi que dans les structures sportives, culturelles et de loisirs, et les médias.

L'éducation, y compris l'éducation numérique dispensée dès le plus jeune âge est de plus en plus indispensable dans nos démocraties pour lutter contre la désinformation et les fausses informations qui se traduisent par l'exploitation, la manipulation, la polarisation politique et la méfiance vis-à-vis des institutions démocratiques. En outre, ces efforts devraient inclure l'éducation aux réseaux sociaux et aux nouveaux médias, y compris en ce qui concerne leur structure et leurs caractéristiques qui permettent de donner de la visibilité à du contenu extrême et aux abus de se répandre. En outre, comme indiqué ci-dessus, le sexisme et la misogynie cohabitent souvent

avec un contenu politique extrême, des théories conspirationnistes et des positions racistes qui mènent à la diffusion de représentations et de comportements préjudiciables qui ciblent les femmes en ligne. Pour mieux comprendre comment les stéréotypes sur les femmes et les filles se répandent sur internet et pour éduquer les utilisateurs sur la source du contenu qu'ils consultent en ligne et sur la manière de déconstruire les stéréotypes et les comportements préjudiciables, l'inclusion de l'éducation numérique dans l'éducation à l'égalité entre les femmes et les hommes revêt tout autant d'importance que l'éducation juridique pour combattre la violence à l'égard des femmes en ligne et facilitée par la technologie.

Formation des professionnels (article 15)

> 1) Les Parties dispensent ou renforcent la formation adéquate des professionnels pertinents ayant affaire aux victimes ou aux auteurs de tous les actes de violence couverts par le champ d'application de la présente Convention, sur la prévention et la détection de cette violence, l'égalité entre les femmes et les hommes, les besoins et les droits des victimes, ainsi que sur la manière de prévenir la victimisation secondaire.
>
> 2) Les Parties encouragent l'inclusion dans la formation mentionnée au paragraphe 1, d'une formation sur la coopération coordonnée interinstitutionnelle afin de permettre une gestion globale et adéquate des orientations dans les affaires de violence couverte par le champ d'application de la présente Convention.

L'obligation de formation des professionnels revêt la plus haute importance lorsqu'il s'agit de prévenir les formes de harcèlement sexuel, de harcèlement moral et de violence psychologique en ligne et facilitées par la technologie. Comme nous l'avons vu ci-dessus à la section 1.4, les victimes se heurtent à plusieurs niveaux de difficultés lorsqu'elles tentent d'obtenir réparation pour les actes de violence subis. En effet, les victimes ne savent généralement pas vers qui se tourner et comment trouver de l'aide, un sentiment de désarroi qui contribue aux répercussions de cette violence sur les victimes. Elles ont également du mal à trouver des professionnels formés auprès desquels s'adresser pour obtenir des conseils et se heurtent à l'absence de formation des professionnels aux systèmes de la justice pénale et de la répression. Il est indispensable de s'appuyer sur les bonnes pratiques en matière de formation professionnelle dans les secteurs social, éducatif et de la santé et dans les secteurs de la justice pénale et de la répression. Plus précisément, les professionnels de la justice pénale et des services répressifs devraient bénéficier d'une formation initiale et continue tenant compte de la dimension de genre, sur les lois les plus récentes s'appliquant à ces formes de violence, sur la collecte et l'obtention de preuves, y compris des preuves électroniques, et sur les moyens de recueillir les témoignages et les récits des victimes sans qu'elles ne fassent l'objet d'une victimisation secondaire. En outre, les professionnels chargés de traiter les demandes d'asile déposées par des femmes devraient recevoir une formation tenant compte de la dimension de genre sur les formes de violence en ligne et facilitées par la technologie qui peuvent conduire à une migration forcée, surtout dans le contexte de la violence domestique.

Programmes préventifs d'intervention et de traitement (article 16)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour établir ou soutenir des programmes visant à apprendre aux auteurs de violence domestique à adopter un comportement non violent dans les relations interpersonnelles en vue de prévenir de nouvelles violences et de changer les schémas comportementaux violents.
>
> 2) Les Parties prennent les mesures législatives ou autres nécessaires pour établir ou soutenir des programmes de traitement destinés à prévenir la récidive des auteurs d'infractions, en particulier des auteurs d'infractions à caractère sexuel.
>
> 3) En prenant les mesures mentionnées aux paragraphes 1 et 2, les Parties veillent à ce que la sécurité, le soutien et les droits humains des victimes soient une priorité et que, le cas échéant, ces programmes soient établis et mis en œuvre en étroite coordination avec les services spécialisés dans le soutien aux victimes.

Lorsqu'il existe des mécanismes de prévention et de traitement à destination des auteurs de violence à l'égard des femmes, ils devraient être renforcés par des formations tenant compte de la dimension de genre sur les formes de violence numérique et les stéréotypes négatifs qui les exacerbent, ainsi que sur les structures et les aspects technologiques qui les facilitent. Lorsque ces mécanismes n'existent pas, leur conception devrait inclure des descriptions des formes de violence numérique, l'incidence spécifique de ce type de violence et des modules sur les moyens numériques et les spécificités de la commission d'une infraction en ligne.

Participation du secteur privé et des médias (article 17)

> 1) Les Parties encouragent le secteur privé, le secteur des technologies de l'information et de la communication et les médias, dans le respect de la liberté d'expression et de leur indépendance, à participer à l'élaboration et à la mise en œuvre des politiques, ainsi qu'à mettre en place des lignes directrices et des normes d'autorégulation pour prévenir la violence à l'égard des femmes et renforcer le respect de leur dignité.
>
> 2) Les Parties développent et promeuvent, en coopération avec les acteurs du secteur privé, les capacités des enfants, parents et éducateurs à faire face à un environnement des technologies de l'information et de la communication qui donne accès à des contenus dégradants à caractère sexuel ou violent qui peuvent être nuisibles.

Le document publié par le Conseil de l'Europe dans le cadre d'une série de documents expliquant les différentes dispositions de la Convention d'Istanbul, intitulé « Encourager la participation du secteur privé et des médias à la prévention de la violence à l'égard des femmes et de la violence domestique : article 17 de la Convention d'Istanbul », décrit quatre piliers qui doivent être mis en œuvre par les États avec le secteur privé et les médias, afin de prévenir la violence à l'égard des femmes : 1) améliorer la formation des professionnels des médias sur les questions d'égalité entre les femmes et les hommes et de violence à l'égard des femmes ; 2) promouvoir l'autorégulation et la régulation des contenus discriminatoires et violents dans les médias ; 3) mettre en place des partenariats pour accroître la couverture médiatique de la violence à l'égard des femmes et des questions d'égalité entre les femmes et les hommes ; et 4) promouvoir la coopération dans l'éducation aux médias (Conseil de l'Europe 2015b).

Le rôle du secteur privé, du secteur des technologies de l'information et de la communication et des médias est en effet fondamental pour s'assurer que les formes de violence à l'égard des femmes en ligne et facilitées par la technologie sont effectivement prises en considération sur toutes les plateformes et chaque outil de perpétration. Les Parties devraient mettre en place des mécanismes de suivi pour s'assurer que des perspectives axées sur la victime ont bien été incluses dans la conception de produits intelligents connectés à l'internet des objets afin d'atténuer les risques éventuels au niveau de la conception. En outre, les parties devraient accorder la priorité à une coopération effective avec le secteur des TIC, surtout grâce aux mécanismes de coopération existants tels que le Code de conduite de l'UE visant à combattre les discours de haine en ligne, le partenariat du Conseil de l'Europe avec les entreprises numériques dans le cadre du programme de coopération du Conseil de l'Europe avec les entreprises ou en établissant un code de conduite dédié sur la violence à l'égard des femmes en ligne et facilitée par la technologie et des observatoires nationaux sur la violence à l'égard des femmes qui incluraient des programmes et des initiatives dédiés (Conseil de l'Europe 2017b).

Les plateformes en ligne devraient être encouragées à adopter des cadres internationaux sur les droits humains, y compris des cadres et des normes sur les droits des femmes, et elles devraient être incitées à renforcer la responsabilité vis-à-vis des initiatives de prévention et de remédiation à disposition des utilisateurs et des victimes. Une bonne initiative à cet égard est la coopération avec les entreprises du Conseil de l'Europe, mentionnée plus haut, qui permet aux entreprises et aux gouvernements de se réunir pour élaborer des politiques fondées sur les droits de l'homme dans le domaine des technologies numériques. Les parties devraient surtout insister sur la transparence et la disponibilité de données détaillées concernant tous les types de violence à l'égard des femmes observés sur des plateformes en ligne.

En outre, les Parties devraient inciter le secteur des TIC à être plus inclusif, en particulier vis-à-vis des femmes avec des identités intersectionnelles, qui apportent une perspective à plusieurs niveaux dans la conception des produits et outils et dans la gouvernance de ces entreprises.

En ce qui concerne les médias, les parties devraient veiller à ce qu'ils respectent les principes de la dignité humaine et interdisent toute discrimination fondée sur le sexe, ainsi que l'incitation à la haine et toutes les formes de violence à l'égard des femmes fondée sur le genre. S'agissant des formes de violence en ligne, les médias devraient éviter de diffuser des perspectives de culpabilisation des victimes. Par ailleurs, les parties pourraient encourager l'émergence d'initiatives intersectorielles entre le secteur privé, les médias et le secteur des TIC pour combattre toutes les formes de violence à l'égard des femmes en ligne et facilitées par la technologie. Ces initiatives devraient essentiellement porter sur la lutte contre les stéréotypes et les comportements préjudiciables qui visent des femmes et des filles en ligne et par le biais des nouvelles technologies.

Protection

Afin d'atteindre l'objectif de la Convention d'Istanbul, à savoir une Europe exempte de toute forme de violence à l'égard des femmes et de violence domestique, les victimes doivent être en mesure d'accéder à un ensemble de mécanismes de protection que les Parties sont tenues de mettre à leur disposition. En ce qui concerne les victimes de violence en ligne et facilitée par la technologie, plusieurs solutions pourraient offrir une protection et un soutien aux victimes.

Obligations générales (article 18)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour protéger toutes les victimes contre tout nouvel acte de violence.
>
> 2) Les Parties prennent les mesures législatives ou autres nécessaires, conformément à leur droit interne, pour veiller à ce qu'il existe des mécanismes adéquats pour mettre en œuvre une coopération effective entre toutes les agences étatiques pertinentes, y compris les autorités judiciaires, les procureurs, les services répressifs, les autorités locales et régionales, ainsi que les organisations non gouvernementales et les autres organisations ou entités pertinentes pour la protection et le soutien des victimes et des témoins de toutes les formes de violence couvertes par le champ d'application de la présente Convention, y compris en se référant aux services de soutien généraux et spécialisés visés aux articles 20 et 22 de la présente Convention.
>
> 3) Les Parties veillent à ce que les mesures prises conformément à ce chapitre : soient fondées sur une compréhension fondée sur le genre de la violence à l'égard des femmes et de la violence domestique, et se concentrent sur les droits humains et la sécurité de la victime ; soient fondées sur une approche intégrée qui prenne en considération la relation entre les victimes, les auteurs des infractions, les enfants et leur environnement social plus large ; visent à éviter la victimisation secondaire ; visent l'autonomisation et l'indépendance économique des femmes victimes de violence ; permettent, le cas échéant, la mise en place d'un ensemble de services de protection et de soutien dans les mêmes locaux ; répondent aux besoins spécifiques des personnes vulnérables, y compris les enfants victimes, et leur soient accessibles.
>
> 4) La prestation de services ne doit pas dépendre de la volonté des victimes d'engager des poursuites ou de témoigner contre tout auteur d'infraction.
>
> 5) Les Parties prennent les mesures adéquates pour garantir une protection consulaire ou autre, et un soutien à leurs ressortissants et aux autres victimes ayant droit à cette protection conformément à leurs obligations découlant du droit international.

Cet article prévoit que les Parties élaborent et mettent en œuvre des lois et des politiques pour éviter une nouvelle victimisation. Cet aspect est particulièrement pertinent s'agissant de la violence en ligne et facilitée par la technologie. Les Parties devraient être incitées à introduire des lois ou à interpréter la législation existante d'une manière qui tienne compte des menaces auxquelles les femmes sont confrontées en ligne ; faire en sorte que la législation et la gouvernance nationales permettent d'instaurer le meilleur dialogue possible – formel et informel – entre les agences chargées d'apporter une réponse aux victimes de ces infractions en ligne et facilitées par la technologie. Cette réponse devrait tenir compte de la dimension de genre et des spécificités de ces formes de violence, y compris le fait qu'elles peuvent se produire dans le contexte de la violence domestique et après les abus, qu'elles peuvent se produire de manière répétée et continue, être commises par plusieurs auteurs et entraîner des répercussions sur les moyens de subsistance de la victime et des personnes à sa charge, sur leur santé mentale et parfois sur leur intégrité physique. Ces mécanismes de réponse coordonnée devraient également tenir compte du fait que les victimes de violence en ligne et facilitée par la technologie peuvent être revictimisées presque indéfiniment étant donné que le contenu criminel qui les concerne peut rester visible et accessible en ligne.

Information (article 19)

> Les Parties prennent les mesures législatives ou autres nécessaires pour que les victimes reçoivent une information adéquate et en temps opportun sur les services de soutien et les mesures légales disponibles, dans une langue qu'elles comprennent.

Dans le contexte de formes de violence nouvelles et émergentes, comme celles examinées ci-dessus, l'existence et l'accessibilité de l'information, tant juridique que concernant la protection et le soutien, est essentielle dans le parcours de nombreuses victimes. Sans cette information, facilement accessible du point de vue de la langue, de la présentation et des moyens tenant compte des besoins comme la langue des signes, le braille, etc., en ligne et hors ligne, les victimes sont souvent livrées à elles-mêmes, ne sachant pas quoi faire ni vers qui se tourner.

Services de soutien généraux (article 20)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour que les victimes aient accès à des services facilitant leur rétablissement. Ces mesures devraient inclure, si nécessaire, des services tels que le conseil juridique et psychologique, l'assistance financière, les services de logement, l'éducation, la formation et l'assistance en matière de recherche d'emploi.
>
> 2) Les Parties prennent les mesures législatives ou autres nécessaires pour que les victimes aient accès à des services de santé et des services sociaux, que les services disposent des ressources adéquates et que les professionnels soient formés afin de fournir une assistance aux victimes et de les orienter vers les services adéquats.

Les Parties sont tenues de mettre des services de soutien à la disposition des victimes de violence à l'égard des femmes, y compris de violence à l'égard des femmes en ligne et facilitée par la technologie. Le conseil juridique et psychologique revêt une importance particulière pour les victimes de ces formes de violence nouvelles et émergentes, pour prévenir la culpabilisation des victimes et leur proposer des outils pour pouvoir engager des poursuites si elles le souhaitent, pour sécuriser les preuves recueillies auprès de la victime et leur permettre de trouver un soutien et une protection en vue de leur rétablissement. En cas de harcèlement et de violence psychologique facilités par la technologie et survenant dans le contexte de la violence domestique, les victimes et les personnes à leur charge devraient bénéficier des mêmes services de soutien et de protection que les victimes de formes de violence domestique exemptes de dimension numérique. Plus particulièrement, elles devraient être en mesure de trouver des services de soutien et de protection tenant compte de la spécificité de ce type de victimisation, qui comprend parfois l'impossibilité de rester dans une maison où des appareils intelligents contribuent aux violences commises à leur encontre, ou elles devraient être en mesure de rencontrer des professionnels formés qui sont réceptifs aux répercussions que les logiciels espion/logiciels de harcèlement et le harcèlement en ligne peuvent avoir sur leur sécurité.

Soutien en matière de plaintes individuelles/collectives (article 21)

> Les Parties veillent à ce que les victimes bénéficient d'informations sur les mécanismes régionaux et internationaux de plaintes individuelles/collectives applicables et de l'accès à ces mécanismes. Les Parties promeuvent la mise à disposition d'un soutien sensible et avisé aux victimes dans la présentation de leurs plaintes.

Les victimes de violence à l'égard des femmes en ligne et facilitée par la technologie devraient bénéficier d'informations et d'orientations lorsqu'elles souhaitent accéder à des mécanismes régionaux ou internationaux de plaintes individuelles ou collectives si les recours au niveau national ont été épuisés.

Services de soutien spécialisés (article 22)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour fournir ou aménager, selon une répartition géographique adéquate, des services de soutien spécialisés immédiats, à court et à long terme, à toute victime ayant fait l'objet de tout acte de violence couvert par le champ d'application de la présente Convention.
>
> 2) Les Parties fournissent ou aménagent des services de soutien spécialisés pour toutes les femmes victimes de violence et leurs enfants.

Cet article complète l'article 20 en précisant que toutes les victimes doivent être en mesure de bénéficier d'une protection et d'un soutien immédiats, y compris de conseils tenant compte de leur expérience spécifique. En effet, une protection immédiate doit être accordée aux victimes de violence à l'égard des femmes en ligne et facilitée par la technologie, surtout lorsque ces infractions sont commises dans le contexte de la violence domestique et génèrent un sentiment d'insécurité pour la victime ou les personnes à sa charge. En raison de la géolocalisation, de la contrainte et du contrôle exercés en ligne par le biais des réseaux sociaux ou avec

l'aide de logiciels de harcèlement installés sur le téléphone, la tablette ou l'ordinateur de la victime, ou par le biais d'outils technologiques, comme des serrures intelligentes ou d'autres outils de l'internet des objets, la victime devrait pouvoir accéder à une protection et un soutien immédiats. Il faut veiller à mettre en place des services de conseil dotés des ressources humaines, financières et techniques nécessaires pour pouvoir offrir des conseils spécifiques et dédiés aux femmes et aux filles concernées. À cet égard, certaines organisations préconisent même « la possibilité pour les victimes de harcèlement et/ou de violence psychologique en ligne ou facilités par la technologie, dans le contexte de la violence domestique/violence fondée sur le genre, qui ne peuvent échapper au contrôle exercé par leur agresseur, de bénéficier d'une nouvelle identité (comme un changement de nom)[27] ».

Permanences téléphoniques (article 24)

> Les Parties prennent les mesures législatives ou autres nécessaires pour mettre en place à l'échelle nationale des permanences téléphoniques gratuites, accessibles vingt-quatre heures sur vingt-quatre, sept jours sur sept, pour fournir aux personnes qui appellent, de manière confidentielle ou dans le respect de leur anonymat, des conseils concernant toutes les formes de violence couvertes par le champ d'application de la présente Convention.

En ce qui concerne la violence à l'égard des femmes en ligne et facilitée par la technologie, il est primordial que les victimes puissent avoir accès à des permanences soit par téléphone, soit par chat ou messagerie instantanée, vingt-quatre heures sur vingt-quatre, sept jours sur sept, depuis leur propre pays mais aussi depuis l'étranger, de manière à pouvoir recevoir des conseils quant à la violence qu'elles ont subi, et être informées sur les premières mesures à prendre dans l'immédiat (comme le fait de conserver des preuves, via des captures d'écran ou des enregistrements) et sur la voie à suivre pour obtenir réparation.

Soutien aux victimes de violence sexuelle (article 25)

> Les Parties prennent les mesures législatives ou autres nécessaires pour permettre la mise en place de centres d'aide d'urgence pour les victimes de viols et de violences sexuelles, appropriés, facilement accessibles et en nombre suffisant, afin de leur dispenser un examen médical et médico-légal, un soutien lié au traumatisme et des conseils.

Dans le contexte des centres ou services d'aide d'urgence pour les victimes de violences sexuelles, des questions sur l'existence de formes antérieures de harcèlement ou de violence psychologique en ligne et facilitées par la technologie devraient être systématiquement posées à la victime, de manière à mettre en évidence le potentiel de facilitation des technologies numériques dans les affaires de viol et de violence sexuelle. Les services de soutien qui proposent des conseils immédiats ou sur le plus long terme devraient être équipés pour dispenser des conseils et un soutien dans le cadre d'expériences telles qu'un viol filmé, afin de tenir compte de la victimisation et du traumatisme supplémentaires que cela peut représenter.

Protection et soutien des enfants témoins (article 26)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour que, dans l'offre des services de protection et de soutien aux victimes, les droits et les besoins des enfants témoins de toutes les formes de violence couvertes par le champ d'application de la présente Convention soient dûment pris en compte.
>
> 2) Les mesures prises conformément au présent article incluent les conseils psychosociaux adaptés à l'âge des enfants témoins de toutes les formes de violence couvertes par le champ d'application de la présente Convention et tiennent dûment compte de l'intérêt supérieur de l'enfant.

Cet article peut être lu en parallèle avec l'**article 31** de la Convention d'Istanbul intitulé **Garde, droit de visite et sécurité (Chapitre V, Droit matériel)**.

Comme nous l'avons vu ci-dessus, les enfants sont souvent impliqués dans les formes de harcèlement en ligne visant leur mère en tant que parent victime de violence, par le biais de leur téléphone ou de leur tablette. En outre, pendant le confinement lié à la pandémie de Covid-19, les situations de visites virtuelles de parents

27. Entretien avec Floriane Volt et Louise Beriot de la Force Juridique de la Fondation des Femmes, 24 septembre 2020, disponible sur : https://fondationdesfemmes.org/.

n'ayant pas la garde de leurs enfants ont augmenté. Cette forme de rencontre entraîne un risque de revictimisation pour les victimes et leurs enfants, dès lors que l'ancien partenaire violent, en sa qualité de parent de l'enfant, est en mesure d'« (obtenir) des indices sur la vie de son ancien partenaire d'après ce qu'il voit lors des appels vidéo et de les utiliser pour poser aux enfants des questions qui pourraient compromettre la sécurité de leur parent (Klein 2020) ». Ces risques spécifiques de revictimisation devraient être pris en considération lorsque des conseils psychologiques sont dispensés aux enfants témoins et co-victimes. En effet, l'article 31 précise que « Les Parties prennent les mesures législatives ou autres nécessaires pour que, lors de la détermination des droits de garde et de visite concernant les enfants, les incidents de violence couverts par le champ d'application de la présente Convention soient pris en compte ».

Signalement et signalement par les professionnels (articles 27 et 28)

> Les Parties prennent les mesures nécessaires pour encourager toute personne témoin de la commission de tout acte de violence couvert par le champ d'application de la présente Convention, ou qui a de sérieuses raisons de croire qu'un tel acte pourrait être commis ou que des nouveaux actes de violence sont à craindre, à les signaler aux organisations ou autorités compétentes (article 27).
>
> Les Parties prennent les mesures nécessaires pour que les règles de confidentialité imposées par leur droit interne à certains professionnels ne constituent pas un obstacle à la possibilité, dans les conditions appropriées, d'adresser un signalement aux organisations ou autorités compétentes s'ils ont de sérieuses raisons de croire qu'un acte grave de violence couvert par le champ d'application de la présente Convention a été commis et que de nouveaux actes graves de violence sont à craindre (article 28).

En ce qui concerne les formes de harcèlement et de violence psychologique en ligne érigées en infractions pénales dans leur pays, les utilisateurs de plateformes internet devraient être en mesure d'accéder à des mécanismes de signalement immédiat, à la fois sur les plateformes des fournisseurs de services et sur les plateformes des services répressifs. Les professionnels qui découvrent des cas de violence en ligne et facilitée par la technologie via des sources accessibles au public devraient être en mesure de les signaler à une plateforme de services répressifs et/ou directement à des agents dans un commissariat de police.

Poursuites

C'est souvent dans le cadre des poursuites, ou des tentatives de poursuite de la violence en ligne et facilitée par la technologie que les victimes et leurs avocats sont confrontés à de nombreuses difficultés. Certaines trouvent leur origine dans l'absence de cadre juridique approprié pour tenir compte d'un nouveau type de violence. D'autres résident dans l'absence de formation du secteur de la justice pénale et dans le manque de volonté et d'incitation pour utiliser la jurisprudence et conférer une dimension de genre aux lois existantes couvrant la cybercriminalité ou les infractions liées au respect de la vie privée. Le nombre insuffisant d'enquêteurs spécialisés souvent nécessaires pour obtenir de nombreux éléments de preuve fait aussi obstacle à la poursuite effective de la violence à l'égard des femmes en ligne et facilitée par la technologie.

Certaines difficultés découlent aussi de la nature de l'espace en ligne, du fait qu'un grand nombre de preuves sont désormais électroniques et que ces éléments de preuve peuvent être copiés ou diffusés ou au contraire effacés ou modifiés d'un seul clic. Outre les problèmes de recevabilité des preuves électroniques devant un tribunal, il est souvent très difficile, voire impossible, pour les services répressifs d'obtenir des preuves d'un autre pays ou d'un fournisseur de services. Ces preuves peuvent également être stockées dans le cloud, causant des problèmes de juridiction.

> Étant donné que (…) la criminalité qui se déroule dans le monde physique implique de plus en plus des preuves électroniques, l'état de droit est menacé non seulement dans le cyberespace mais aussi dans le monde physique. Enfin, cette capacité décroissante à enquêter et à défendre la sécurité publique et les droits de l'homme se traduira par du (…) vigilantisme ou des victimes sans justice[28].

28. Comité de la Convention sur la cybercriminalité (T-CY), Accès de la justice pénale aux preuves électroniques dans le cloud : Recommandations pour examen par le T-CY, Rapport final du Groupe de travail du T-CY sur les preuves dans le cloud, disponible sur : http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b51cb.

De multiples cadres se font concurrence pour autoriser ou décourager l'accès à des preuves électroniques, y compris le « Cloud Act », le cadre nord-américain qui régit l'accès aux preuves électroniques stockées aux États-Unis. Mais en raison de la complexité des procédures entre les États eux-mêmes, entre les parties à des accords internationaux, entre les Parties et les non-Parties, et entre les États et les entreprises, il est extrêmement difficile pour la plupart des victimes d'entrevoir la fin de leur épreuve. Le deuxième protocole à la Convention de Budapest, qui sera bientôt adopté, propose d'examiner certaines de ces difficultés pour accéder aux preuves électroniques et à la coopération internationale conformément à l'État de droit et aux normes des droits humains, en s'assurant que les gouvernements satisfont à leur obligation de protéger les personnes et leurs droits dans le cyberespace.

La plus grande valeur de la Convention d'Istanbul réside dans la reconnaissance de la violence à l'égard des femmes fondée sur le genre, en tant que violence exercée sur une femme parce qu'elle est une femme. La Convention de Budapest complète cela en mettant à disposition des outils aux Parties aux deux conventions, et à la Convention de Budapest en cas de double incrimination, pour poursuivre efficacement ces infractions. Le deuxième protocole additionnel à la Convention de Budapest, qui sera adopté prochainement, propose d'accélérer les procédures d'entraide judiciaire (qui actuellement peuvent prendre jusqu'à 18 mois), en permettant un meilleur accès des services répressifs aux preuves électroniques stockées dans une autre partie, y compris des moyens de coopération dans des situations d'urgence, et une coopération directe entre un Partie et un fournisseur d'accès à internet situé dans une autre Partie. Le deuxième protocole faciliterait aussi la divulgation d'informations relatives à l'enregistrement d'un nom de domaine (parfois essentiel pour identifier les auteurs et clarifier la responsabilité) et résoudrait certains des problèmes posés par la juridiction et la territorialité[29].

Ces itérations faciliteraient un grand nombre de procédures, y compris pour les femmes victimes.

Nous allons maintenant évaluer un ensemble de dispositions de la Convention d'Istanbul relevant du domaine des poursuites, complétées par les dispositions de la Convention de Budapest (le cas échéant) renforçant les dispositions de la Convention d'Istanbul en ce qui concerne la violence à l'égard des femmes en ligne et facilitée par la technologie. Nous analyserons également d'autres dispositions de la Convention lorsqu'elles présentent un intérêt pour la cybercriminalité touchant les femmes parce qu'elles sont des femmes.

Enquêtes, poursuites, droit procédural et mesures de protection

Dans la section suivante nous évaluerons et commenterons sur la pertinence des dispositions de la Convention d'Istanbul s'agissant de la poursuite de la violence à l'égard des femmes en ligne et facilitée par la technologie complétées par les dispositions de la Convention de Budapest sur les enquêtes et le droit procédural. Nous analyserons ensuite les dispositions relatives à la coopération internationale.

Obligations générales (article 49)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour que les enquêtes et les procédures judiciaires relatives à toutes les formes de violence couvertes par le champ d'application de la présente Convention soient traitées sans retard injustifié tout en prenant en considération les droits de la victime à toutes les étapes des procédures pénales.
>
> 2) Les Parties prennent les mesures législatives ou autres nécessaires, conformément aux principes fondamentaux des droits de l'homme et en prenant en considération la compréhension de la violence fondée sur le genre, pour garantir une enquête et une poursuite effectives des infractions établies conformément à la présente Convention.

Cette disposition souligne l'importance de tenir compte de la nécessité urgente de poursuivre toutes les formes de violence à l'égard des femmes pour éviter d'accorder « une faible priorité sous l'angle des enquêtes et des procédures judiciaires, ce qui contribuerait significativement à faire naître un sentiment d'impunité chez les auteurs d'infractions et à perpétuer un niveau élevé d'acceptation de ces types de violences » (Conseil de l'Europe 2011b). Cela est également vrai dans le contexte des formes nouvelles et émergentes de violence comme la violence à l'égard des femmes en ligne et facilitée par la technologie. Cette disposition pourrait également servir à « conférer une dimension de genre » au texte de la Convention de Budapest en reconnaissant

29. Entretien avec Alexander Seger, Chef de la Division Cybercriminalité et Secrétaire exécutif du Comité de la Convention Cybercriminalité, septembre 2020, https://www.coe.int/en/web/cybercrime/tcy.

l'importance de mener des enquêtes et d'engager des poursuites dans les affaires de violence touchant les femmes en ligne.

Réponse immédiate, prévention et protection (article 50)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour que les services répressifs responsables répondent rapidement et de manière appropriée à toutes les formes de violence couvertes par le champ d'application de la présente Convention en offrant une protection adéquate et immédiate aux victimes.
>
> 2) Les Parties prennent les mesures législatives ou autres nécessaires pour que les services répressifs responsables engagent rapidement et de manière appropriée la prévention et la protection contre toutes les formes de violence couvertes par le champ d'application de la présente Convention, y compris l'emploi de mesures opérationnelles préventives et la collecte des preuves.

Les services répressifs devraient être en mesure de réagir rapidement et d'offrir aux victimes la bonne protection mais aussi de lancer des initiatives de prévention et de protection comme des mesures opérationnelles préventives et la collecte des preuves. Dans le cas des formes de violence en ligne et facilitées par la technologie, la reconnaissance précoce et rapide de cette forme de violence par les services répressifs contribue à l'établissement de processus optimum pour la collecte de preuves.

À cet égard, les articles 16 à 21 de la Convention de Budapest pourraient compléter l'article 50 de la Convention d'Istanbul dans le cadre de la poursuite des auteurs de violence à l'égard des femmes en ligne et facilitée par la technologie et donner aux parties des orientations plus précises sur les mesures à prendre pour obtenir des preuves électroniques dans le cadre de procédures pénales sur les territoires des Parties.

Article 16 de la Convention de Budapest (Conservation rapide de données informatiques stockées)

> 1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.
>
> 2) Lorsqu'un Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.
>
> 3) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

Le rapport explicatif de la Convention de Budapest souligne que :

> Les mesures mentionnées dans les articles 16 et 17 s'appliquent aux données stockées qui ont déjà été collectées et archivées par les détenteurs de données, tels que les fournisseurs de services. (...) en raison de leur volatilité, les données informatiques sont faciles à manipuler et à modifier. Ainsi, il est facile de perdre des éléments prouvant une infraction si les pratiques de traitement et de stockage manquent de rigueur, si les données sont intentionnellement manipulées ou effacées pour détruire tout élément de preuve ou si elles sont effacées dans le cadre d'opérations normales d'effacement de données qui n'ont plus à être conservées. L'un des moyens de préserver l'intégrité des données consiste pour les autorités compétentes à opérer des perquisitions ou à accéder d'une autre manière aux données et à saisir les données ou à se les procurer d'une autre manière. (...) les infractions informatiques et en relation avec l'ordinateur sont très souvent commises au moyen de la transmission de communications par le biais du système informatique. (...) L'identification de la source ou de la destination de ces communications antérieures peut aider à établir l'identité des auteurs de ces infractions (Conseil de l'Europe 2001b).

Article 17 de la Convention de Budapest (Conservation et divulgation partielle rapides de données relatives au trafic)

> 1) Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires : a) pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et b) pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.
>
> 2) Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

« L'obtention de données relatives au trafic stockées concernant des communications antérieures peut être indispensable pour déterminer la source ou la destination de ces communications » (ibid.). Cet accès est donc essentiel pour identifier les auteurs, même si

> aucun fournisseur ne possède à lui seul suffisamment de données relatives au trafic pour permettre de déterminer avec exactitude la source ou la destination de la communication. Chacun possède certaines parties du puzzle et chacune de ces parties doit être examinée afin d'identifier la source ou la destination (...) L'article 17 veille, lorsqu'un seul ou plusieurs fournisseurs de services ont participé à la transmission d'une communication, à ce qu'il soit procédé à la conservation rapide des données relatives au trafic parmi tous les fournisseurs (ibid.).

Article 18 de la Convention de Budapest (Injonction de produire)

> 1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner : a) à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et b) à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Cet article est important car il permet aux Parties, dans le cadre d'enquêtes judiciaires et de procédures pénales spécifiques, d'ordonner à une personne présente sur son territoire de communiquer les données informatiques spécifiées (article 18.1.a) ; et d'ordonner à un fournisseur de services de communiquer les données relatives aux abonnés, lorsque le fournisseur de services offre ses prestations sur le territoire de la partie sans nécessairement être établi sur le territoire (article 18.1.b)[30]. Les données relatives aux abonnés constituent souvent une information importante dans le cadre d'une enquête judiciaire dès lors qu'elles peuvent contenir, entre autres informations, l'adresse IP de l'auteur présumé (ou du ou des auteurs(s) secondaire(s))[31]. Le deuxième protocole additionnel prévoira des procédures visant à renforcer la coopération directe avec les fournisseurs et les entités d'autres parties, sous réserve de garanties appropriées pour tenir compte des exigences uniques découlant d'une coopération directe entre les autorités d'une partie avec les fournisseurs de services situés dans une autre partie.

Article 19 de la Convention de Budapest (Perquisition et saisie de données informatiques stockées)

> 1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire : a) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et b) à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

---

30. Conseil de l'Europe, (2017) T-CY Guidance Note #10 on « Production orders for subscriber information », disponible sur : https://rm.coe.int/16806f943e
31. « Dans le cadre d'une enquête pénale, les informations relatives aux abonnés peuvent être nécessaires dans deux situations spécifiques. Premièrement, elles sont nécessaires pour déterminer les services et mesures techniques connexes qui ont été utilisés ou sont utilisés par un abonné, tels que le type de service téléphonique utilisé (par exemple téléphonie mobile), le type de services connexes utilisé (renvoi automatique d'appel, messagerie téléphonique, etc.), le numéro de téléphone ou toute autre adresse technique (comme une adresse électronique). Deuxièmement, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé. D'autres informations relatives aux abonnés, telles que les informations commerciales figurant dans les dossiers de facturation et de paiement de l'abonné, peuvent également être utiles aux enquêtes pénales surtout lorsque l'infraction faisant l'objet de l'enquête concerne un cas de fraude informatique ou un autre délit économique » (Conseil de l'Europe 2001b). »

Cet article exige des parties qu'elles élaborent des lois habilitant les autorités compétentes à accéder à des systèmes informatiques et à des serveurs situés sur leur territoire. « Cet article vise à moderniser et harmoniser les législations internes concernant la perquisition et la saisie de données informatiques stockées aux fins de recueillir des preuves se rapportant à des enquêtes ou procédures pénales spécifiques » (Conseil de l'Europe 2001b).

Article 20 de la Convention de Budapest (Collecte en temps réel des données relatives au trafic)

> 1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes : a) à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et b) à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes : i) à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou ii) à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

Les données relatives au trafic revêtent de l'importance pour les enquêtes étant donné qu'elles indiquent le nombre de visiteurs sur un site web par exemple, à quel moment les suspects présumés se connectent ou communiquent et par l'intermédiaire de quel fournisseur de services (boîte de messagerie, date, heure, pseudo).

> « (C)es techniques sont souvent essentielles pour l'enquête ouverte sur certaines des infractions créées dans la Convention, telles que celles qui impliquent un accès illicite aux systèmes informatiques, la diffusion de virus ou la pornographie enfantine. Il arrive, par exemple, que la source de l'intrusion ou de la diffusion ne puisse pas être établie sans que l'on ait recours à la collecte en temps réel de données relatives au trafic. Dans certains cas, la nature de la communication ne peut être découverte sans interception en temps réel des données relatives au contenu » (ibid.).

Article 21 de la Convention de Budapest (Interception de données relatives au contenu)

> 1) Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne : a) à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et b) à obliger un fournisseur de services, dans le cadre de ses capacités techniques : i) à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou ii) à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

Les données relatives au contenu constituent les données les plus sensibles, dès lors qu'elles contiennent des informations telles que du texte, des images, des photos, des vidéos, du son, etc. Comparées à d'autres types de données, elles sont donc soumises à des règles plus strictes en matière de protection des données. Même dans le cadre d'une enquête pénale, « étant donné que les données relatives au contenu soulèvent davantage de questions au regard du droit au respect de la vie privée, la mesure d'enquête est limitée à 'de graves infractions à définir dans le droit interne » (ibid.).

Nous avons vu que les articles 16 à 21 de la Convention de Budapest sont complémentaires de l'article 50 de la Convention d'Istanbul.

D'autres dispositions de la Convention d'Istanbul relatives aux poursuites peuvent être analysées compte tenu de ces types de violence.

Article 51 de la Convention d'Istanbul (Appréciation et gestion des risques)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour qu'une appréciation du risque de létalité, de la gravité de la situation et du risque de réitération de la violence soit faite par toutes les autorités pertinentes afin de gérer le risque et garantir, si nécessaire, une sécurité et un soutien coordonnés.
>
> 2) Les Parties prennent les mesures législatives ou autres nécessaires pour que l'appréciation mentionnée au paragraphe 1 prenne dûment en compte, à tous les stades de l'enquête et de l'application des mesures de protection, le fait que l'auteur d'actes de violence couverts par le champ d'application de la présente Convention possède ou ait accès à des armes à feu.

En effet, de nombreuses formes de violence à l'égard des femmes en ligne et facilitées par la technologie peuvent prendre des proportions inquiétantes et aboutir à des situations mettant la vie des femmes en danger. Nous avons vu ci-dessus que la violence sexuelle peut être précédée de menaces et de comportements de harcèlement en ligne et facilités par la technologie. Dans le contexte de la violence domestique, c'est encore plus flagrant. Des mécanismes de sécurité et de soutien coordonnés devraient donc être mis à disposition des victimes de violence domestique, également lorsque celle-ci présente des formes d'abus commis en ligne ou par le biais des nouvelles technologies.

Article 52 de la Convention d'Istanbul (Ordonnances d'urgence d'interdiction) et article 53 (Ordonnances d'injonction ou de protection)

> Les Parties prennent les mesures législatives ou autres nécessaires pour que les autorités compétentes se voient reconnaître le pouvoir d'ordonner, dans des situations de danger immédiat, à l'auteur de violence domestique de quitter la résidence de la victime ou de la personne en danger pour une période de temps suffisante et d'interdire à l'auteur d'entrer dans le domicile de la victime ou de la personne en danger ou de la contacter. Les mesures prises conformément au présent article doivent donner la priorité à la sécurité des victimes ou des personnes en danger (article 52).
>
> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour que des ordonnances d'injonction ou de protection appropriées soient disponibles pour les victimes de toutes les formes de violence couvertes par le champ d'application de la présente Convention.
>
> 2) Les Parties prennent les mesures législatives ou autres nécessaires pour que les ordonnances d'injonction ou de protection mentionnées au paragraphe 1 soient : disponibles pour une protection immédiate et sans charge financière ou administrative excessive pesant sur la victime ; émises pour une période spécifiée, ou jusqu'à modification ou révocation ; le cas échéant, émises *ex parte* avec effet immédiat ; disponibles indépendamment ou cumulativement à d'autres procédures judiciaires ; autorisées à être introduites dans les procédures judiciaires subséquentes (article 53).

Les ordonnances d'urgence d'interdiction et les ordonnances de protection devraient être adaptées aux formes de violence domestique commises par le biais des nouvelles technologies et en ligne. En effet, il n'est pas rare que les ordonnances d'urgence d'interdiction/ordonnances de protection ne mentionnent pas les communications électroniques car les services répressifs ne comprennent pas toujours bien les nombreuses formes de violence commises par le biais des nouvelles technologies (Association for Progressive Communications/ OHCHR (n.d.)). Dans certains pays, des exceptions sont spécifiquement accordées en ce qui concerne la communication autour des enfants, y compris par téléphone portable ou communication numérique, ce qui prête encore plus à confusion. En outre, étant donné que les moyens de communications électroniques se sont étendus et sont désormais plus divers et moins clairs et directs, certains réseaux sociaux sont moins axés sur la communication (échange de messages ou de contenu) mais reposent sur l'observation (regarder le contenu de quelqu'un passivement sans échanger), voire même le harcèlement parfois, par exemple le fait de regarder les « stories » en ligne ou le comportement de l'« orbiting » qui consiste à ne pas répondre aux messages de quelqu'un mais à continuer de regarder son contenu de manière visible en ligne. C'est la raison pour laquelle il devient encore plus difficile d'apprécier ce qui peut être défini comme un contact entre un auteur et une victime (Fetters/The Atlantic 2018).

> « Je pense que ce que nous percevons et ce que nos clients perçoivent comme un comportement intimidant et menaçant n'est pas nécessairement traduit. (...) Si nos clients ont le sentiment de ne pas pouvoir faire face et d'être harcelés et s'il s'agit manifestement d'une violation de l'ordonnance de protection – pour ce qui est de l'intention de harceler, d'intimider, de contraindre – il est plus difficile de traduire cela en quelque chose qui doit être une violation d'un point de vue juridique » (ibid.).

Article 56 de la Convention d'Istanbul (Mesures de protection)

> 1) Les Parties prennent les mesures législatives ou autres nécessaires pour protéger les droits et les intérêts des victimes, y compris leurs besoins spécifiques en tant que témoins, à tous les stades des enquêtes et des procédures judiciaires, en particulier :
>
> a) en veillant à ce qu'elles soient, ainsi que leurs familles et les témoins à charge, à l'abri des risques d'intimidation, de représailles et de nouvelle victimisation ;

b) en veillant à ce que les victimes soient informées, au moins dans les cas où les victimes et la famille pourraient être en danger, lorsque l'auteur de l'infraction s'évade ou est libéré temporairement ou définitivement ;

c) en les tenant informées, selon les conditions prévues par leur droit interne, de leurs droits et des services à leur disposition, et des suites données à leur plainte, des chefs d'accusation retenus, du déroulement général de l'enquête ou de la procédure, et de leur rôle au sein de celle-ci ainsi que de la décision rendue ;

d) en donnant aux victimes, conformément aux règles de procédure de leur droit interne, la possibilité d'être entendues, de fournir des éléments de preuve et de présenter leurs vues, besoins et préoccupations, directement ou par le recours à un intermédiaire, et que ceux-ci soient examinés ;

e) en fournissant aux victimes une assistance appropriée pour que leurs droits et intérêts soient dûment présentés et pris en compte ;

f) en veillant à ce que des mesures pour protéger la vie privée et l'image de la victime puissent être prises ;

g) en veillant, lorsque cela est possible, à ce que les contacts entre les victimes et les auteurs d'infractions à l'intérieur des tribunaux et des locaux des services répressifs soient évités ;

h) en fournissant aux victimes des interprètes indépendants et compétents, lorsque les victimes sont parties aux procédures ou lorsqu'elles fournissent des éléments de preuve ;

i) en permettant aux victimes de témoigner en salle d'audience, conformément aux règles prévues par leur droit interne, sans être présentes, ou du moins sans que l'auteur présumé de l'infraction ne soit présent, notamment par le recours aux technologies de communication appropriées, si elles sont disponibles.

2) Un enfant victime et témoin de violence à l'égard des femmes et de violence domestique doit, le cas échéant, se voir accorder des mesures de protection spécifiques prenant en compte l'intérêt supérieur de l'enfant.

L'article 56 est essentiel en ce qu'il dresse la liste des besoins des victimes à tous les stades de la procédure de poursuites. Il est possible d'éviter qu'un grand nombre de menaces ne soient proférées par ces moyens en tenant compte des besoins spécifiques des victimes en tant que témoins et de la protection de leurs familles et témoins contre la revictimisation et les représailles en ligne et via les nouvelles technologies. Ces moyens de commission sont souvent facilement supervisés mais ils peuvent avoir un impact incroyablement négatif sur les victimes et leurs témoins, entravant parfois le processus de la justice. En outre, il convient de tenir compte du rôle que jouent les victimes dans la violence en ligne et facilitée par la technologie s'agissant de la production de preuves, compte tenu de la spécificité des preuves électroniques (captures d'écran de messages ou de photos, enregistrements vidéo depuis effacés par le ou les auteurs, par exemple).

Coopération internationale

S'agissant de la coopération entre les Parties à la Convention d'Istanbul, l'article 62 dispose que les Parties coopèrent, « dans la mesure la plus large possible », aux fins de prévenir la violence, de protéger et assister les victimes ou de mener des enquêtes ou des procédures concernant les infractions établies dans la Convention d'Istanbul, mais aussi d'appliquer des jugements pénaux, y compris les ordonnances de protection. Le rapport explicatif de la Convention précise que les Parties devraient « réduire, autant que faire se peut, les obstacles à la circulation rapide de l'information et des preuves » (Conseil de l'Europe 2011b).

La coopération entre les Parties s'applique également lorsqu'une victime qui réside dans la juridiction d'une Partie dépose une plainte pour une infraction commise dans une autre Partie. Il est précisé dans le rapport explicatif que « Ces autorités peuvent alors, soit engager une procédure si leur droit le permet, soit transmettre la plainte aux autorités de l'État dans lequel les faits ont été commis. Cette transmission s'effectue conformément aux dispositions pertinentes des instruments de coopération applicables entre les États considérés » (ibid.).

Enfin, la convention dispose que les efforts d'entraide judiciaire peuvent aussi trouver une base légale dans la Convention d'Istanbul, même si les États n'ont pas signé d'autre traité axé spécifiquement sur l'entraide judiciaire, incitant ainsi les Parties à la convention à engager une coopération en matière judiciaire.

S'agissant de la coopération internationale, de l'entraide judiciaire et de l'accès à des éléments de preuve électroniques dans des contextes transfrontaliers, les articles 25 et 29 à 34 de la Convention de Budapest peuvent apporter des éléments complémentaires aux dispositions de la Convention d'Istanbul.

Article 25 de la Convention de Budapest (Principes généraux relatifs à l'entraide)

> 1) Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale (…).
>
> 3) Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

Le rapport explicatif précise que « l'obligation de coopérer s'applique en principe à la fois aux infractions pénales liées à des systèmes et des données informatiques (...), et à la collecte de preuves sous forme électronique se rapportant à une infraction pénale ».

En effet, les données électroniques étant volatiles (rapidement dupliquées ou effacées) :

> L'objectif du paragraphe 3 consiste donc à faciliter l'accélération du processus visant à garantir l'entraide pour éviter que des informations ou des preuves essentielles ne soient perdues parce qu'elles auraient été effacées avant qu'une demande d'entraide n'ait pu être préparée et transmise et qu'une réponse n'ait pu être reçue.

Les articles 29 et 30 de la Convention de Budapest relèvent de l'entraide judiciaire en matière de mesures provisoires.

Article 29 de la Convention de Budapest (Conservation rapide de données informatiques stockées)

L'article 29 définit les conditions dans lesquelles une Partie peut demander que des données informatiques stockées soient conservées par une autre Partie dans le cadre d'une enquête pénale[32]. Cet article fait écho à l'article 16 (niveau national) dans le cadre de la coopération internationale (Conseil de l'Europe 2001b).

Les formes de violence à l'égard des femmes en ligne et facilitées par la technologie sont, comme nous l'avons vu, partiellement couvertes par les articles de fond 2 à 11 de la Convention de Budapest. Pour que la conservation puisse fonctionner dans ces cas, a) les parties devraient appliquer la double incrimination avec souplesse ; ou b) les parties à l'origine de la requête doivent demander la conservation sur la base d'une infraction facilitatrice visée aux articles 2 à 7 et 11. À titre d'exemple, une partie peut demander la conservation dans une affaire de cybermenaces en invoquant l'article 2, accès illégal à l'ordinateur d'une victime (Conseil de l'Europe 2018c).

Article 30 de la Convention de Budapest (Divulgation rapide de données conservées)

L'article 30 équivaut à l'article 17 (niveau national) dans le contexte de la coopération internationale.

Les articles 31 à 34 couvrent la coopération internationale concernant les pouvoirs d'enquête.

Article 31 de la Convention de Budapest (Entraide concernant l'accès aux données stockées)

L'article 31 fait écho à l'article 19 (niveau national) et explique que les Parties doivent avoir la capacité, à la demande d'une autre partie, de perquisitionner ou d'accéder de façon similaire, d'obtenir et de divulguer des données stockées au moyen d'un système informatique se trouvant sur leur territoire. La demande doit être satisfaite aussi rapidement que possible lorsqu'il existe un risque que les données soient modifiées ou perdues, ou lorsque les traités, arrangements ou législations applicables prévoient une coopération rapide.

---

32. Les données informatiques sont définies dans le préambule de la Convention de Budapest comme étant « toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ».

Article 32 de la Convention de Budapest (Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public)

L'article 32 mentionne des situations dans lesquelles les services répressifs d'une Partie peuvent agir unilatéralement, dans certaines circonstances seulement, pour accéder à des données informatiques avec le consentement de « la personne légalement autorisée à lui divulguer ces données » (pouvant s'agir du suspect présumé) ou lorsqu'elles sont accessibles au public**.** Aux termes de la note d'orientation sur l'article 32, « on considère généralement que les membres des services répressifs peuvent consulter toutes les données accessibles publiquement, et qu'à cette fin ils peuvent s'inscrire ou s'abonner aux services ouverts au public ». « Selon la note d'orientation, il est admis que les dispositions de l'article 32 constituent des exceptions au principe de territorialité en autorisant, sans passer par l'entraide judiciaire, l'accès à des données stockées à l'étranger » (Verdelho 2019).

Article 33 de la Convention de Budapest (Entraide dans la collecte en temps réel de données relatives au trafic)

En vertu de l'article 33, les Parties sont tenues, dans le cadre de l'entraide judiciaire et d'une enquête pénale, de collecter des données relatives au trafic pour d'autres parties « au moins à l'égard des infractions pénales pour lesquelles [cette collecte] serait disponible dans une affaire analogue au niveau interne », pour éviter que des données importantes relatives au trafic ne soient effacées ou supprimées par les fournisseurs de services.

Article 34 de la Convention de Budapest (Entraide en matière d'interception de données relatives au contenu)

L'article 34 définit les conditions dans lesquelles des données relatives au contenu peuvent être demandées. Les données relatives au contenu étant les données les plus sensibles (faisant l'objet de dispositions de protection de la vie privée), ces demandes dépendent de « régimes et législations internes en vigueur en matière d'entraide pour ce qui est de la portée de l'obligation d'assistance et des restrictions dont cette obligation doit faire l'objet » (Conseil de l'Europe 2001b). Le droit interne en vigueur dans un pays peut ne pas, en soi, s'appliquer aux infractions en ligne et facilitées par la technologie. Dans ce cas, le pays qui reçoit la demande peut être en mesure d'extraire des éléments de la demande du pays demandeur pour pouvoir coopérer. Un pays peut par exemple se fonder sur le fait que des menaces ont été envoyées, sans tenir compte de ce qu'elles ont été envoyées électroniquement. Mais si le droit interne ne couvre pas lui-même une infraction, et s'il n'est pas possible d'extraire des éléments exploitables d'une demande d'entraide judiciaire, la coopération internationale pour l'obtention de données relatives au trafic ou au contenu peut être bloquée (Conseil de l'Europe 2018c). Or il est important de noter que les données relatives au contenu peuvent être des éléments clés dans de nombreuses enquêtes pénales, y compris dans des affaires de violence à l'égard des femmes.

Nous avons vu que de nombreuses dispositions des deux traités peuvent se compléter lorsqu'il s'agit de poursuivre les auteurs de violence à l'égard des femmes en ligne et facilitée par la technologie. Les articles 16 à 21 de la Convention de Budapest complètent l'article 50 de la Convention d'Istanbul sur l'accès et l'obtention de preuves au niveau national. Les articles 25 et 29 à 34 de la Convention de Budapest étendent les capacités des Parties à la Convention de Budapest d'accéder à des preuves électroniques et de les obtenir, et étendent également les pouvoirs d'enquête dans le cadre de l'entraide judiciaire et de la coopération internationale.

CHAPITRE VII

OBSERVATIONS FINALES ET RECOMMANDATIONS

Observations finales

La présente étude porte sur la définition du phénomène de la violence à l'égard des femmes en ligne et facilitée par la technologie, ses causes, ses répercussions, et les supports où ce type de violence se produit, à savoir l'ensemble des plateformes en ligne et des outils technologiques connectés à internet auxquels les utilisateurs peuvent accéder. La violence à l'égard des femmes en ligne et facilitée par la technologie est la perpétuation des différentes formes de violence à l'égard des femmes que l'on observe dans le monde réel, dans la rue, au bureau, à l'école, à l'université, à la maison, et tout au long de la vie. La plupart des formes de violence à l'égard des femmes en ligne et facilitées par la technologie existent déjà hors ligne ; elles se répandent, s'amplifient ou se généralisent du fait de l'utilisation d'internet, par exemple dans le cas des violences domestiques telles que les violences et le harcèlement exercés après une séparation.

La violence en ligne et facilitée par la technologie présente aussi un éventail de spécificités : la victimisation est aggravée par le nombre d'auteurs, la multiplicité des intermédiaires utilisés, l'impossibilité de s'échapper et la difficulté de supprimer du contenu d'internet. Ces caractéristiques amplifient les répercussions négatives de cette forme de violence sur les victimes.

En outre, les victimes se heurtent à de nombreuses difficultés pour obtenir réparation, notamment la volatilité des preuves ou les obstacles rencontrés pour trouver de l'aide et de l'assistance. Il reste difficile d'engager des poursuites dès lors que les lois ne suivent pas nécessairement les évolutions de la technologie et que les représentants des services répressifs ne sont pas nécessairement suffisamment formés et ne disposent pas toujours de ressources et de moyens suffisants pour assister les victimes.

La Convention d'Istanbul, qui est l'instrument de protection des droits humains le plus ambitieux en matière de lutte contre la violence à l'égard des femmes et la violence domestique, a un large champ d'application et couvre toutes les formes de violence à l'égard des femmes et de violence domestique dans tous les domaines de la vie ; elle s'applique donc aussi à la violence à l'égard des femmes et des filles en ligne et facilitée par la technologie.

La Convention de Budapest sur la cybercriminalité et ses protocoles additionnels (le premier protocole additionnel porte sur le racisme et la xénophobie en ligne et le deuxième protocole additionnel, qui sera adopté prochainement, est axé sur le renforcement de la coopération et la divulgation de preuves électroniques dans le cadre d'enquêtes pénales) couvrent de nombreuses infractions commises à l'aide de systèmes informatiques

ou contre ces systèmes. Les Parties à la convention sont tenues de consolider leur droit procédural pénal et de renforcer leurs capacités de justice pénale pour obtenir des preuves électroniques et pour faciliter concrètement la coopération internationale et l'entraide judiciaire dans le cadre d'enquêtes et de poursuites contre la cybercriminalité et d'autres infractions impliquant des preuves électroniques.

Par ailleurs, un vaste paysage normatif d'instruments internationaux et régionaux s'attaque également à certains aspects du phénomène, notamment la Recommandation générale nº 35 du Comité CEDAW, la Recommandation du Conseil de l'Europe sur la prévention et la lutte contre le sexisme et sa Stratégie pour l'égalité entre les femmes et les hommes, plusieurs politiques de l'UE, y compris la Stratégie de l'UE en faveur de l'égalité entre les hommes et les femmes et la Stratégie de l'UE relative aux droits des victimes, le RGPD, la législation sur les services numériques, et la proposition d'accords concernant les preuves électroniques et la coopération comme le Code de conduite de l'UE visant à combattre les discours de haine illégaux en ligne. La coordination entre ces instruments devrait être renforcée pour apporter une réponse globale aux différentes formes de violence à l'égard des femmes en ligne et facilitées par la technologie.

L'étude établit une classification et propose des définitions des différentes formes de violence à l'égard des femmes en ligne et facilitées par la technologie, qui sont analysées dans le cadre des articles 33, 34 et 40 de la Convention d'Istanbul, complétés par des dispositions de la Convention de Budapest. Nous avons étudié les formes de harcèlement sexuel commises en ligne et par le biais des nouvelles technologies comme le partage non consenti d'images ou de vidéos, tel que les abus sexuels basés sur des images, les creepshots, les deepfakes et le cyber flashing, ou comme le harcèlement sexuel associé à des contraintes ou des menaces, tel que le sexting forcé, la sextortion, les menaces de viol, le doxing à caractère sexuel et l'intimidation à caractère sexuel. Des dispositions de la Convention de Budapest, notamment l'article 3, l'article 8 et l'article 10, ont été analysées sur leur complémentarité. Des formes de harcèlement en ligne et facilité par la technologie, comme l'installation de logiciels de harcèlement et les abus facilités par l'internet des objets, ont ensuite été analysées parallèlement aux articles 2, 3, 5 et 6 de la Convention de Budapest. Enfin, les formes de violence psychologique exercées en ligne, y compris le discours de haine sexiste, ont également été mentionnées. Le discours de haine sexiste sera étudié avec en toile de fond la Recommandation du Conseil de l'Europe sur la prévention et la lutte contre le sexisme et le premier protocole additionnel à la Convention de Budapest. L'analyse sur les dispositions de la Convention de Budapest montre que le cadre applicable à la cybercriminalité peut s'appliquer à la violence à l'égard des femmes en ligne et facilitée par la technologie et que les définitions contenues dans la Convention sur la cybercriminalité viennent compléter les définitions de la violence de la Convention d'Istanbul.

Dans la dernière partie, l'étude examine comment les dispositions de la Convention d'Istanbul relatives aux politiques intégrées, à la prévention, à la protection et aux poursuites peuvent s'appliquer à ces formes de violence. L'article 50 de la Convention d'Istanbul est traité parallèlement aux articles 16 à 21 de la Convention de Budapest, et l'article 62 de la Convention d'Istanbul (sur la coopération internationale) parallèlement aux articles 25, 29, 30, et 31 à 34 de la Convention de Budapest.

Pour conclure, la présente étude montre que les deux traités peuvent se compléter mutuellement de manière dynamique. La puissance de la Convention d'Istanbul réside dans la reconnaissance de la violence à l'égard des femmes en tant que violence qui touche les femmes parce qu'elles sont des femmes et dans le fait qu'elle établit clairement l'obligation pour les États d'y apporter une réponse, y compris dans leurs systèmes de justice pénale. La Convention de Budapest prévoit d'importants outils en ce qui concerne les enquêtes, l'obtention de preuves et la coopération internationale, s'agissant non seulement des infractions commises en ligne et par le biais des nouvelles technologies, mais également de toute infraction impliquant des preuves électroniques.

En ce qui concerne les politiques coordonnées et les efforts de prévention et de protection, la Convention d'Istanbul joue un rôle déterminant dans l'établissement d'une réponse forte à toutes les formes de violence à l'égard des femmes. Pour ce qui est de poursuivre les auteurs de violence à l'égard des femmes en ligne et facilitée par la technologie, y compris dans un contexte transfrontalier, les Parties peuvent s'inspirer des modèles d'outils et de méthodologies présentés dans la Convention de Budapest. Mais le domaine de la cybercriminalité, à ce jour, reste neutre du point de vue du genre, de sorte que les infractions commises en ligne contre des femmes ne sont pas conceptualisées dans le cadre de la cybercriminalité ; ce regard neutre du point de vue du genre sur les infractions relevant de la cybercriminalité se propage aux politiques publiques. Le large champ d'application de la Convention d'Istanbul et son approche globale pourraient donc servir de base pour élaborer des politiques sensibles au genre destinées à combattre la cybercriminalité touchant les femmes.

Au-delà d'une interaction *stricto sensu* entre les instruments, une série de recommandations est présentée ci-dessous.

Recommandations

Au niveau du Conseil de l'Europe

- Il serait utile de renforcer la coopération entre le mécanisme de suivi de la Convention d'Istanbul et le T-CY ainsi que la coopération avec l'ECRI et d'autres organes de lutte contre la discrimination du Conseil de l'Europe tel que le Comité directeur sur l'anti-discrimination, la diversité et l'inclusion (CDADI)[33]. Cette coopération pourrait prendre la forme d'échanges de vues et d'une interaction fructueuse, par exemple en examinant la question de la violence à l'égard des femmes en ligne et facilitée par la technologie d'une manière mutuellement enrichissante et complémentaire dans l'objectif de conceptualiser une réponse standardisée[34].
- Dans un deuxième temps, des activités de renforcement des capacités pour les Parties, axées sur les deux conventions, pourraient être envisagées pour accroître le niveau d'expertise et apporter une réponse ciblée à la violence en ligne et facilitée par la technologie dans les Parties à la Convention d'Istanbul ainsi que dans les Parties à la Convention de Budapest.

Au niveau du mécanisme de suivi de la Convention d'Istanbul

- La Recommandation générale N° 1 du GREVIO, axée sur la dimension numérique de la violence à l'égard des femmes, propose une liste complète de mesures destinée à guider les parties dans leurs réponses aux formes de violence à l'égard des femmes en ligne et facilitées par la technologie. Le GREVIO devrait se concentrer sur ces questions dans ses procédures d'évaluation.

Au niveau de la Convention de Budapest

- Le T-CY devrait continuer de reconnaître la dimension de genre de la violence à l'égard des femmes commise en ligne, y compris la cybercriminalité fondée sur le genre, dans leurs travaux faisant suite à l'étude de mapping élaborée en 2018.
- Le point focal de l'intégration de la dimension de genre nommé par le Bureau du Programme sur la cybercriminalité (C-PROC) devrait veiller à l'intégration d'une perspective de genre dans la conceptualisation et la mise en œuvre de toutes les activités de coopération.
- Le T-CY devrait envisager de rédiger une Recommandation générale relative à la Convention de Budapest, portant sur la violence à l'égard des femmes en ligne et facilitée par la technologie, en vue de compléter la recommandation générale du GREVIO sur cette question.

Au niveau du secteur privé

- Les plateformes devraient être encouragées à adopter des cadres internationaux sur les droits humains, y compris des cadres et des normes sur les droits des femmes, et à faire preuve d'un sens accru de leurs responsabilités concernant les mesures de prévention et de remédiation destinées aux victimes.
- Les États devraient notamment insister sur la transparence et la disponibilité de données détaillées concernant toutes les formes de violence à l'égard des femmes commises sur les plateformes.
- Les utilisateurs de plateformes internet devraient pouvoir accéder à des mécanismes de signalement immédiat, tant sur les plateformes des fournisseurs de services que sur les plateformes des services répressifs ; ces mécanismes de signalement devraient adopter une perspective intersectionnelle.
- Des informations juridiques devraient être mises à disposition sur chaque plateforme, selon le pays de résidence de l'utilisateur.
- Les pratiques de modération devraient tenir compte de toutes les formes de violence à l'égard des femmes commises en ligne.
- En ce qui concerne la violence contre les femmes facilitée par l'IdO, les concepteurs de ces dispositifs devraient s'appuyer à la fois sur l'expertise des spécialistes de la violence domestique et sur celle des experts féministes en cybersécurité pour intégrer la dimension de sécurité dans la phase de fabrication.

---

33. La Commission européenne contre le racisme et l'intolérance (ECRI) est une instance unique de monitoring dans le domaine des droits humains, spécialisée dans les questions de lutte contre le racisme, la discrimination (en raison de la « race », l'origine ethnique/nationale, la couleur, la nationalité, la religion, la langue, l'orientation sexuelle, l'identité de genre et les caractéristiques sexuelles), la xénophobie, l'antisémitisme et l'intolérance en Europe, disponible sur : www.coe.int/fr/web/european-commission-against-racism-and-intolerance
34. Interview avec Dr Gizem Guney, septembre 2020

ANNEXE 1

DISCUSSION SUR LES ABUS SEXUELS BASÉS SUR DES IMAGES, UNE FORME DE CYBERCRIME À CARACTÈRE SEXUEL FONDÉ SUR LE GENRE ET UNE FORME DE HARCÈLEMENT SEXUEL EN LIGNE AVEC CIRCONSTANCES AGGRAVANTES

On entend par abus sexuel basé sur des images le comportement consistant à partager et à diffuser en ligne, sans le consentement de la victime, des images ou des vidéos privées, obtenues avec le consentement de la victime au cours d'une relation intime ou volées ou piratées depuis les appareils de la victime, en utilisant parfois une tactique de doxing.

L'abus sexuel basé sur des images est également appelé exploitation sexuelle basée sur des images (Powell et Henry 2016), partage non consenti d'images ou de vidéos ou partage d'images intimes sans consentement (voir Facebook (n.d.), par exemple), pornographie non consentie (voir Citron et Franks 2014) ou « revenge porn ». De nombreux universitaires soulignent la nécessité de redéfinir la terminologie « revenge porn » utilisée par les médias pour proposer une perspective centrée sur la victime.

Plusieurs auteurs considèrent désormais cette infraction comme une forme de cybercriminalité touchant les femmes.

Mary Rogers, par exemple, préconise d'inclure l'abus sexuel basé sur des images dans la Convention de Budapest et présente l'infraction comme un cybercrime basé sur le genre. Elle analyse les cadres juridiques américains concernant ce qu'elle appelle la Pornographie non consentie (NCP – « Non-Consensual Pornography ») :

> Les États commencent à intégrer des lois sur la NCP dans leurs codes pénaux, mais le processus est lent et n'est pas uniforme. Le seul recours dont disposent de nombreuses victimes est la législation sur le droit d'auteur, qui est un recours civil et, dans la majorité des cas, ne peut pas empêcher qu'une image déjà en ligne continue d'être diffusée. C'est pourquoi l'intégration de la NCP dans la convention fournirait les orientations nécessaires au niveau mondial et encouragerait des normes d'incrimination uniformes (Rogers 2018).

Miha Šepec, de la faculté de droit de l'Université de Maribor en Slovénie, montre qu'il existe une dialectique entre les présentations juridiques de la question. Certains pays présentent l'abus sexuel basé sur des images comme une infraction à caractère sexuel tandis que d'autres pays le présentent comme une infraction qui affecte la vie privée de la victime. Šepec comprend l'abus sexuel basé sur des images comme « un cybercrime lié au contenu », semblable au matériel d'abus sexuel sur enfants. Il cite par exemple le Code pénal slovène (2017) qui érige en infraction pénale l'abus sexuel basé sur des images si la diffusion d'images porte gravement atteinte à la vie privée d'une personne. Šepec explique que cette présentation de la question doit alors 1) contenir l'intention de provoquer un sentiment de détresse 2) porter gravement atteinte à la vie privée de la victime. Pour l'auteur, il s'agit d'une approche juridique limitée qui ne tient pas compte des possibilités infinies qui existent pour infliger à une victime un abus sexuel basé sur des images (pour s'amuser, se vanter, pour en retirer un profit, etc.) :

> De nombreux auteurs ont proposé de considérer la vengeance pornographique soit comme de la violence sexuelle facilitée par la technologie (Henry & Powell, 2016), de la violence cyber sexuelle (Cripps & Stermac, 2018), de l'abus sexuel (Citron & Franks, 2014), une infraction à caractère sexuel (McGlynn, Rackley & Houghton, 2017) voire comme un « cyberviol », considérant ainsi que la vertu attaquée est l'identité sexuelle et l'intégrité sexuelle d'une personne. Nous pourrions la qualifier d'approche moderne, qui considère la vengeance pornographique comme une infraction à caractère sexuel grave. En revanche, le concept traditionnel du droit pénal continental est fermement ancré dans la conviction que l'intérêt attaqué par la vengeance pornographique est le droit à la vie privée d'une personne, et son droit à la dignité et à une bonne réputation. Par conséquent, les codes pénaux de l'Europe continentale définissent souvent la vengeance pornographique comme une atteinte à la vie privée, à la dignité et à l'intégrité

personnelle d'une personne – c'est-à-dire uniquement comme une infraction d'atteinte à la vie privée. Par conséquent, dans ces pays, l'infraction n'est pas prise aussi au sérieux que dans les pays où il s'agit d'une infraction à caractère sexuel (Šepec, 2019).

L'auteur soutient enfin qu'il convient de traiter l'abus sexuel basé sur des images comme « une infraction à caractère sexuel, étant donné que les conséquences sur l'intégrité sexuelle d'une victime sont bien plus similaires à celles d'autres infractions à caractère sexuel (en particulier la pornographie enfantine ou la violence et les abus sexuels) que des atteintes à la vie privée » (Šepec, 2019).

En effet, de nombreuses Parties à la Convention d'Istanbul ont adopté des lois qui peuvent s'appliquer à l'abus sexuel basé sur des images ; certaines le considèrent comme une question relative à la vie privée, d'autres tiennent compte de la dimension sexuelle de l'infraction.

- Dans le Code pénal d'Andorre, l'abus est considéré comme un crime contre l'honneur (Chapitre IX) ou une atteinte à la vie privée (Chapitre X).
- En Autriche, il figure dans le code pénal sous l'intitulé « Harcèlement prolongé impliquant un système informatique ou de télécommunications » (article 107c) et «Enregistrements d'images non autorisés» (article 120a).
- La Croatie incrimine le fait de créer, d'utiliser ou de diffuser des images privées à l'article 144 (enregistrement non autorisé d'images) du chapitre XIV du Code pénal intitulé « Atteintes à la vie privée ».
- L'Estonie érige en infraction pénale la divulgation illégale de données à caractère personnel et la divulgation illégale de données à caractère personnel sensibles à l'article 157 et 157.1 du Code pénal. Aucune mention spécifique n'est faite concernant d'éventuelles circonstances aggravantes compte tenu du caractère sexuel et genré de l'infraction lorsque des personnes de plus de 18 ans sont concernées.
- En France, elle est présentée dans l'article 266-2-1 du Code pénal comme une violation de la vie privée avec une dimension sexuelle aggravante et punit l'auteur de deux ans de prison et d'une amende de 60 000 euros.
- En Allemagne, l'article 201a du code pénal tient compte de la « Violation de la vie privée intime en prenant des photographies ou d'autres images ».
- En Pologne, l'infraction de harcèlement persistant d'une autre personne ou d'une personne étroitement liée à la victime, qui est définie à l'article 190a du code pénal, comprend également certaines manifestations en ligne importantes de ce comportement. À cet égard, la loi criminalise spécifiquement l'usurpation d'identité en ligne dans le but de causer à une autre personne un préjudice financier ou personnel.
- En Slovénie, une infraction spécifique de harcèlement a été introduite dans le code pénal pour inclure le traquage physique des personnes ainsi que le harcèlement effectué par des moyens de communication électroniques (article 134a).
- En Suisse, la loi ne reconnaît pas l'infraction spécifique de l'abus sexuel basé sur des images. Le code pénal comprend une infraction pornographique (article 197) ou une violation de la vie privée (article 179) qui tient compte de la dimension non consentie de l'infraction.
- En Espagne, l'article 197 actualisé du Code pénal couvre les infractions de découverte et de divulgation des secrets. La sanction tient compte du fait que l'infraction s'est déroulée dans le cadre d'une (ancienne) relation intime.

Le cadre de la Convention d'Istanbul, enrichi d'une perspective féministe sur la Convention de Budapest, permet d'examiner la question de l'abus sexuel basé sur des images comme une forme de harcèlement sexuel qui se déroule en ligne et par le biais des nouvelles technologies. Il présente l'avantage de tenir compte de la dimension sexuelle de l'infraction, de la dimension répétitive du harcèlement et des répercussions sur la victime, étant donné que le harcèlement sexuel est défini comme « toute forme de comportement non désiré, verbal, non-verbal ou physique, à caractère sexuel, ayant pour objet ou pour effet de violer la dignité d'une personne, en particulier lorsque ce comportement crée un environnement intimidant, hostile, dégradant, humiliant ou offensant ». Au même titre que d'autres types de violence observés dans le contexte de la violence domestique, la Convention d'Istanbul permet de le considérer comme une infraction plus grave en incluant, dans l'ensemble de circonstances aggravantes (article 46) le fait que « l'infraction a été commise à l'encontre d'un ancien ou actuel conjoint ou partenaire, conformément au droit interne, par un membre de la famille, une personne cohabitant avec la victime, ou une personne ayant abusé de son autorité ».

ANNEXE 2

DISCUSSION SUR LES CADRES D'ACTION, MESURES LÉGISLATIVES ET PRATIQUES DES PLATEFORMES INTERNET FACE AU DISCOURS DE HAINE SEXISTE EN LIGNE

La récente Recommandation du Conseil de l'Europe sur la prévention et la lutte contre le sexisme le définit comme étant :

> « Tout acte, geste, représentation visuelle, propos oral ou écrit, pratique ou comportement fondés sur l'idée qu'une personne ou un groupe de personnes est inférieur du fait de leur sexe, commis dans la sphère publique ou privée, en ligne ou hors ligne, avec pour objet ou effet : de porter atteinte à la dignité ou aux droits inhérents d'une personne ou d'un groupe de personnes ; ou d'entraîner pour une personne ou un groupe de personnes des dommages ou des souffrances de nature physique, sexuelle, psychologique ou socio-économique ; ou de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant ; ou de faire obstacle à l'émancipation et à la réalisation pleine et entière des droits humains d'une personne ou d'un groupe de personnes ; ou de maintenir et de renforcer les stéréotypes de genre » (Conseil de l'Europe 2019).

Le discours de haine sexiste en ligne s'accompagne de propos, d'insultes, d'un langage ordurier et, souvent, d'images pour exprimer de l'hostilité envers les femmes et les filles parce qu'elles sont des femmes. Les harceleurs profèrent généralement des insultes et font des commentaires sur l'apparence physique des femmes, comme leurs formes ou leur silhouette, le fait qu'elles se conforment ou non à des stéréotypes de genre et leur sexualité.

La Recommandation du Conseil de l'Europe sur le sexisme souligne que « (i)nternet a donné une nouvelle dimension à l'expression et à la diffusion du sexisme, en particulier du discours de haine sexiste, auprès d'un large public, même si les origines du sexisme ne sont pas à chercher du côté des technologies mais dans la persistance des inégalités entre les femmes et les hommes ».

Le discours de haine sexiste en ligne poursuit le même objectif que d'autres formes de discours de haine, hors ligne et en ligne : diminuer la présence d'une personne dans un espace public, humilier ou différencier, asseoir une dominance et un pouvoir, effrayer et terroriser une personne pour la réduire au silence et la rendre invisible.

Un aspect de la conversation sur le discours de haine sexiste en ligne est la dialectique entre le discours de haine et la liberté d'expression.

> (L)es efforts destinés à lutter contre le phénomène de (la violence à l'égard des femmes en ligne et facilitée par la technologie) ont été stoppés par la juxtaposition d'arguments sur l'égalité entre les femmes et les hommes et de considérations sur la liberté d'expression, ce qui a abouti à un statu quo, les femmes étant soumises à la violence et à la haine en ligne, et leurs voix réduites au silence – ce qui a été souligné par les rapporteurs spéciaux des Nations Unies (Barker et Jurasz 2019).

Il convient de noter que le discours de haine a été initialement présenté et défini dans le contexte du racisme et de l'antisémitisme ; ainsi le discours de haine sexiste fait également intervenir une importante composante raciale. En effet, la Recommandation n° R (97) 20 du Comité des Ministres du Conseil de l'Europe sur le « discours de haine » le définie comme :

> toutes formes d'expression qui propagent, incitent à, promeuvent ou justifient la haine raciale, la xénophobie, l'antisémitisme ou d'autres formes de haine fondées sur l'intolérance, y compris l'intolérance qui s'exprime sous forme de nationalisme agressif et d'ethnocentrisme, de discrimination et d'hostilité à l'encontre des minorités, des immigrés et des personnes issues de l'immigration.

La Recommandation de politique générale No. 15 de la Commission européenne contre le racisme et l'intolérance (ECRI) de décembre 2015 définit le discours de haine comme :

> le fait de prôner, de promouvoir ou d'encourager sous quelque forme que ce soit, le dénigrement, la haine ou la diffamation d'une personne ou d'un groupe de personnes ainsi que le harcèlement, l'injure, les stéréotypes négatifs, la stigmatisation ou la menace envers une personne ou un groupe de personnes et la justification de tous les types précédents d'expression au motif de la « race », de la couleur, de l'origine familiale, nationale ou ethnique, de l'âge, du handicap, de la langue, de la religion ou des convictions, du sexe, du genre, de l'identité de genre, de l'orientation sexuelle, d'autres caractéristiques personnelles ou de statut[35].

En outre, le Protocole additionnel à la Convention sur la cybercriminalité du Conseil de l'Europe, « relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, exige des États parties qu'ils adoptent une législation appropriée et veillent à ce qu'elle soit effectivement mise en œuvre. En outre, les États devraient adopter des mesures législatives et autres pour ériger en infractions pénales 'la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe' » (Conseil de l'Europe 2020b).

Dans leur article intitulé « #MasculinitySoFragile : culture, structure, and networked misogyny », Sarah Banet-Weiser et Kate Miltner (2016) tentent de répondre à « pourquoi, en ce moment précis de l'histoire, voit-on déferler une vague particulièrement virulente de violence et d'hostilité à l'égard des femmes ? ». Selon les auteurs, ces formes de violence « ne concernent pas seulement le genre mais sont également souvent racistes, les femmes de couleur étant particulièrement ciblées ». Les auteurs inventent le concept de la misogynie en réseau, soulignant les dimensions culturelles et structurelles croisées créant ce niveau de haine envers les femmes, et plus particulièrement les femmes de couleur, en ligne. En effet, certains groupes diffusent ce mélange particulier de sexisme, de racisme et de violence, certains utilisant une rhétorique traditionnelle d'extrême droite pour rationaliser la violence et d'autres inventant de nouvelles formes de discours d'extrême droite adapté aux espaces en ligne (Hampton/Slate 2019 ; Lavin 2020).

C'est l'une des raisons pour lesquelles l'auteure Margarita Salas décrit la dialectique entre le discours de haine sexiste en ligne et la liberté d'expression comme le « faux paradoxe » et demande que le discours de haine sexiste soit reconnu comme une forme de violence similaire au racisme et à la xénophobie.

> Lorsque nous parlons de liberté d'expression, nous nous plaçons sous l'angle des droits humains. Ces droits sont indivisibles, intimement liés et interdépendants, ce qui signifie que l'amélioration d'un droit facilite l'avancement des autres et que la privation d'un droit a une incidence négative sur les autres. Cela signifie aussi qu'ils ne doivent pas être hiérarchisés, que la liberté d'expression ne prévaut pas sur le droit de vivre une vie sans violence. Cela signifie aussi qu'il y a des limites à la liberté d'expression qui sont légitimes afin de trouver un équilibre avec d'autres droits humains » (Salas/GenderIT 2013).

Le Conseil de l'Europe travaille sur la question du discours de haine depuis de nombreuses années et de nombreux domaines ont été explorés, y compris, récemment, le discours de haine en ligne. « En raison de la prolifération du discours de haine en ligne, des efforts spécifiques ont été déployés pour comprendre sa nature singulière et pour relever les nombreux défis qu'il pose. Si le discours de haine en ligne n'est pas intrinsèquement différent, la nature des environnements en ligne fait qu'il est difficile d'imputer une responsabilité et d'élaborer des mesures juridiques adéquates » (Conseil de l'Europe 2020b).

Une étude de 2020 sur la question du discours de haine en ligne dans le cadre du Conseil de l'Europe propose un modèle de 30 indicateurs pour la mise en œuvre et l'évaluation des bonnes politiques visant à prévenir et corriger le discours de haine en ligne au moyen de la protection et de la réparation, par exemple. Cette étude montre que de multiples parties prenantes développent de facto des réponses au discours de haine en ligne, à différents niveaux comme dans les organisations internationales ou régionales, les États et les entreprises de haute technologie, les organisations de défense des droits des femmes et les organisations de la société civile. Selon l'auteur de l'étude, « Les agences gouvernementales, les plateformes internet et les organisations de la société civile préconisent et acceptent à juste titre de partager équitablement les travaux pratiques et la responsabilité juridique de la lutte contre le discours de haine en ligne » (Conseil de l'Europe 2020a).

---

35. ECRI (2015), Recommandation de politique générale n°15 de l'ECRI sur la lutte contre le discours de haine, disponible sur : http://rm.coe.int/recommandation-de-politique-generale-n-15-de-l-ecri-sur-la-lutte-contr/16808b5b03.

Au niveau des plateformes internet, deux types d'outils sont utilisés pour identifier et supprimer le discours de haine illégal et le discours de haine qui enfreint les politiques de la société en matière de contenu. Les systèmes de modération du contenu contrôlent et appliquent (soit par l'extraction de texte et l'apprentissage automatique ou les algorithmes soit par l'intermédiaire de modérateurs humains) une liste déterminée de règles et d'orientations sur le contenu posté par les utilisateurs (texte en particulier) pour déterminer s'il est acceptable ou s'il enfreint les conditions d'utilisation de la plateforme (y compris s'il enfreint la législation locale). De nombreuses voix s'élèvent à la fois contre les solutions algorithmiques (qui ne sont pas assez détaillées, ne tiennent pas compte du contexte, sont trop dépendantes de l'échantillon de données d'entraînement – potentiellement biaisées – utilisées par les outils d'apprentissage automatique ou les algorithmes, qui se traduisent par une responsabilité réduite en cas de zones grises dans la modération) et les solutions humaines de modération (mauvaises conditions de travail, ces emplois étant généralement externalisés vers des pays qui ont une législation du travail assez faible, formation insuffisante, risques de troubles de stress posttraumatique) (Cambridge Consultants/OfCom 2019 ; Sinders 2017 ; Breslow 2018). Le contenu est ensuite envoyé à des équipes de la conformité juridique qui analysent et suppriment le contenu illégal conformément à la législation locale.

Les flux de signalement constituent le deuxième mécanisme mis en œuvre par les plateformes internet pour corriger la présence de discours de haine en ligne. Chaque plateforme de réseaux sociaux dispose d'un ensemble d'outils de signalement qui tentent de tenir compte des manifestations de violence en ligne. Les utilisateurs sont invités à signaler tout contenu qui enfreint les politiques de la société ou parfois la législation locale. Les organisations qui travaillent en tant que signaleurs de confiance ou organes de surveillance signalent aussi tout contenu illégal. Certaines plateformes ont fait des progrès considérables pour développer des pages de signalement complètes, qui proposent des définitions des types de violence et sensibilisent les utilisateurs, d'autres ne se trouvent encore qu'à un stade embryonnaire et les utilisateurs disposent de peu de moyens pour signaler la violence. Il convient de noter que la plupart des définitions de la violence trouvées sur les plateformes sont neutres du point de vue du genre et sont loin de comprendre un cadre intersectionnel[36].

Des structures de surveillance sont également mises en place par les plateformes ; il peut s'agir de consultations publiques sur les politiques de contenu des plateformes et les orientations et processus de modération du contenu, une forme de surveillance caractérisée par Alexander Brown comme étant « l'échelon le plus bas de ce que pourrait être la surveillance » (Conseil de l'Europe 2020a), des processus de recours interne mis en place au niveau de la plateforme internet, utilisés soit pour faire appel contre des décisions de supprimer du contenu ou des décisions de ne pas supprimer du contenu, et des conseils de supervision, des comités directeurs ou des conseils de surveillance dont l'objectif est idéalement de rendre des décisions dans les affaires relevant des « zones grises ».

S'agissant de la réponse commune et coordonnée basée sur l'autorégulation entre le secteur privé et les États, on peut mentionner le Code de conduite visant à combattre les discours de haine illégaux en ligne, signé par la Commission européenne et la plupart des plateformes de réseaux sociaux (examiné ci-dessus).

Enfin, une législation a vu le jour en Europe pour combattre ces formes de discours de haine en ligne. Ces cadres législatifs énoncent l'obligation pour les plateformes de supprimer les discours de haine illégaux dans un délai précis (soit 24 heures soit sept jours en fonction du type de contenu) mais contiennent une série de vulnérabilités inhérentes. La législation sur le discours de haine comprend généralement des amendes en cas d'inobservations répétées de l'obligation de supprimer du contenu dans ledit délai, ce qui permet ainsi aux plateformes de décider de payer des amendes plutôt que d'adapter leurs pratiques. Les spécialistes de la liberté d'expression soulignent les risques que comporte le fait de placer des pouvoirs judiciaires entre les mains des acteurs privés et de laisser les plateformes décider de la suppression de discours de haine sans surveillance extérieure, voire de supprimer trop de contenu pour éviter toute responsabilité, surtout du contenu spécifique comme du journalisme (ibid.).

En effet, la loi relative à l'application du droit sur les réseaux, NetzDG) en vigueur en Allemagne, qui combat le discours de haine illégal et qui doit faire l'objet d'une révision, a été critiquée par les spécialistes de la liberté d'expression et de la protection des données sur le fait que la responsabilité juridique exigée des plateformes « est problématique car elle externalise effectivement des pouvoirs quasi judiciaires ou de justice pénale aux plateformes internet même si ces dernières n'ont généralement pas la capacité et l'expertise pour

36. Voir, par exemple, les centres d'assistance de Facebook (disponible sur : https://www.facebook.com/help/1126628984024935?helpref=hc_global_nav), Twitter (disponible sur : https://help.twitter.com/en/rules-and-policies/twitter-report-violation), Snapchat (disponible sur https://support.snapchat.com/fr-FR) et Tiktok (disponible sur : https://support.tiktok.com/).

atteindre les mêmes niveaux élevés de régularité de la procédure que ceux que l'on trouve dans des procédures judiciaires »(ibid.).

En France, la « proposition de loi Avia », qui prévoyait d'obliger les plateformes à supprimer les discours de haine signalés comme « manifestement illicites » dans les 24 heures et le matériel d'abus sexuel sur des enfants et la propagande terroriste dans un délai d'une heure, sous peine d'amendes, a été retoquée par le Conseil constitutionnel en juin 2020 pour les mêmes raisons :

> Compte tenu de la difficulté d'apprécier dans le délai imparti si le contenu signalé est manifestement illicite, de la sanction encourue dès la première violation et de l'absence de cause spécifique exonérant de toute responsabilité, [la législation] ne peut qu'inciter les opérateurs de plateformes en ligne à supprimer le contenu signalé, qu'il soit manifestement illicite ou non (Politico 2020).

Ainsi que le conclut Alexander Brown, il est « recommandé que le point de vue des victimes soit pris en considération par les agences gouvernementales, les plateformes internet et les organisations de la société civile, y compris les organes de monitoring, en tant qu'indicateur ou mesure du succès ou du progrès des outils de gouvernance » (Conseil de l'Europe 2020a). En outre, le fait de classer le discours de haine sexiste dans le cadre de la Convention d'Istanbul, en tant que forme de violence psychologique avec des circonstances aggravantes (comme le nombre d'auteurs impliqués par exemple), peut contribuer à intégrer cette approche centrée sur la victime dans la gouvernance du discours de haine, surtout pour les victimes du discours de haine sexiste et intersectionnel.

ANNEXE 3
GLOSSAIRE

Abus sexuel basé sur des images

On parle d'« abus sexuel basé sur des images » lorsque l'auteur de l'abus partage en ligne des images ou des vidéos sexuellement explicites de la victime qu'il a obtenues au cours de sa relation avec cette personne ou en piratant son ordinateur, ses comptes de réseaux sociaux ou son téléphone.

Adresse IP (adresse de protocole Internet)

Une « adresse IP » est un numéro attribué à chaque appareil connecté à internet et qui permet de l'identifier et de le localiser.

Airdrop

Airdrop est une fonctionnalité développée par Apple qui permet à un utilisateur d'échanger des contenus avec un autre utilisateur d'un produit Apple situé à proximité.

Algorithme

Un algorithme est une suite ou séquence d'instructions servant à réaliser une tâche automatisée dans un système informatique ou à résoudre un problème.

Appareils portables

Les appareils portables sont des dispositifs intelligents portés sur le corps, qui collectent, analysent et partagent des informations physiques dans l'objectif de suivre les habitudes ou la santé d'une personne.

Attaque DDoS (Distributed Denial of Service)

Une attaque DDoS, ou attaque par déni de service, vise à perturber le fonctionnement normal d'un service ou d'un serveur en lui envoyant de multiples requêtes, jusqu'à le saturer.

Body shaming

Le « body shaming » consiste à commenter, en s'en moquant, l'apparence physique d'une personne (jugée trop grosse ou trop maigre, par exemple).

Cloud

Le cloud (ou nuage) est un autre moyen de stocker des données numériques : il permet de stocker les données, non pas sur le disque dur d'un ordinateur, mais sur des serveurs externes, parfois situés en plusieurs endroits, qui sont la propriété d'une entreprise (un hébergeur) et qui sont gérés par cette entreprise.

Creepshots

Les « creepshots » sont des images suggestives de femmes photographiées à leur insu.

Cyberharcèlement

Le cyberharcèlement est un harcèlement pratiqué à l'aide d'outils et de services numériques, qui affecte plus particulièrement les personnes mineures.

Cyber flashing

Le « cyber flashing » consiste à envoyer des photos à caractère sexuel non sollicitées, en utilisant des applications de rencontre ou de messagerie ou via Airdrop ou Bluetooth.

Deadnaming

Le « deadnaming » ou « morinommage » consiste à utiliser sciemment le prénom de naissance d'une personne transgenre (prénom qui ne correspond pas au genre de cette personne) pour l'humilier, la menacer, lui faire peur ou lui faire du mal.

Deepfakes

Les « deepfakes » sont des vidéos falsifiées mais semblant authentiques, dans lesquelles un visage a été remplacé par un autre (grâce à des algorithmes et aux techniques de l'apprentissage profond) et les sons ont été modifiés.

Doxing

Le « doxing » (ou « doxxing ») consiste à diffuser en ligne des informations personnelles (numéro de téléphone, adresse électronique, adresse postale, coordonnées professionnelles, etc.) relatives à un individu, sans son consentement, dans le but d'inciter d'autres internautes à lui nuire.

Flaming

Le « flaming » est le fait de publier des messages offensants ou hostiles, tels que des insultes, sur des réseaux sociaux ou des forums.

Géolocalisation

La « géolocalisation » est la fonctionnalité d'un appareil lui permettant de connaître sa position géographique grâce aux signaux GPS ou à d'autres signaux.

Hacking

Le « hacking » consiste à détecter une porte d'entrée dans un système informatique ou un réseau, illégalement ou sans l'accord de son propriétaire.

Happy slapping (vidéolynchage)

Le « happy slapping », ou « vidéolynchage », consiste à agresser (physiquement ou sexuellement) une victime dans le but d'enregistrer l'agression et de la partager en ligne.

Internet des objets

L'« internet des objets » est le réseau des objets physiques qui sont connectés entre eux et avec internet, et qui enregistrent et transmettent des données sur leur utilisation.

Logiciel espion / logiciel de harcèlement

Un « logiciel espion » est un logiciel, généralement une application, téléchargé sur le téléphone ou l'appareil d'une personne et servant à suivre l'utilisation de cet appareil. Dans le contexte de la violence domestique, les logiciels espions sont considérés comme des « logiciels de harcèlement ».

Orbiting

L'« orbiting » consiste à s'abstenir de répondre aux messages d'une personne et de communiquer directement avec elle tout en continuant à suivre ses contenus en ligne de façon visible (liker, regarder les stories, etc.).

Outing

L'« outing » consiste à révéler l'orientation sexuelle ou l'identité de genre d'une personne sans son accord, souvent publiquement.

Preuves électroniques

Une preuve électronique est constituée de données contenues dans un dispositif numérique ou technologique ou produites par ce dispositif.

Sexting (textopornographie)

Le « sexting », ou « textopornographie », consiste à échanger, envoyer ou recevoir des messages sexuellement explicites, souvent accompagnés de photos ou de vidéos, par des textos ou dans un dialogue en ligne.

Sextortion

La « sextortion » ou « extorsion sexuelle » consiste à menacer une personne de publier des contenus sexuels (images, vidéos, deepfakes, rumeurs sexuelles) à des fins d'intimidation, de contrainte ou de chantage pour obtenir de nouveaux contenus sexuels ou de l'argent, parfois les deux.

Trolling

Le « trolling » désigne l'acte qui consiste à se rendre en ligne pour créer une discorde.

Upskirting

L'« upskirting » désigne l'acte qui consiste à prendre des photos à caractère sexuel ou intimes sous la jupe ou la robe d'une victime, sans son consentement, et à partager ce contenu en ligne.

ANNEXE 4
RÉFÉRENCES

Abdul Aziz, Z., (2017), *Due Diligence and Accountability for Online Violence against Women* : www.duediligence-project.org

Active Bystander UK (n.d.), consulté le 25 septembre 2020 : http://www.activebystander.co.uk/

Ajder, H., Patrini, G., Cavalli, F., et Cullen, L., (2019), *The State of Deepfakes : Landscape, Threats, and Impact* : https://sensity.ai/mapping-the-deepfake-landscape/

Algorithm Watch, (2020), *Our response to the European Commission's planned Digital Services Act* : https://algorithmwatch.org/en/submission-digital-services-act-dsa/

Amnesty International (2018), *Toxic Twitter, a toxic place for women* : www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1

Amnesty International, (2020), *Twitter Scorecard* : www.amnesty.be/IMG/pdf/20200922_rapport_twitter_scorecard.pdf

Association for Progressive Communications, OHCHR (n.d.), *Input on Protection Orders*, consulté le 14 octobre 2020 : www.ohchr.org/Documents/Issues/Women/SR/Shelters/APC_UNSRVAW_input%20on%20protection%20orders.pdf

Banet-Weiser, S., Miltner, K.M., (2016), *#MasculinitySoFragile : culture, structure, and networked misogyny*, Feminist Media Studies : www.tandfonline.com/doi/full/10.1080/14680777.2016.1120490

Barker, K., Jurasz, O., (2019), *Online Violence Against Women : addressing the responsibility gap?* : http://eprints.lse.ac.uk/103941/1/WPS_2019_08_23_online_violence_against_women_addressing_the_responsibility_gap.pdf

BBC (2019a), *Cyber-flashing : 'I froze when penis picture dropped on to my phone'* : www.bbc.com/news/uk-48054893

BBC (2019b), "Instagram : Girl tells how she was 'hooked' on self-harm images", available at : www.bbc.com/news/uk-47069865.

BBC (2020), *How your smart home devices can be turned against you* : www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse

Boukemidja, N.B., (2018), *Cyber Crimes against Women : Qualification and Means*, European Journal of Social Sciences : https://journals.euser.org/files/articles/ejss_v1_i3_18/Boukemidja.pdf

Breslow, J., *Moderating the 'worst of humanity' : sexuality, witnessing, and the digital life of coloniality* : www.tandfonline.com/doi/full/10.1080/23268743.2018.1472034

Cambridge Consultants, OfCom, (2019), *Use of AI in Online Content Moderation* : www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf

CBC, (2017), *Aydin Coban sentenced in Dutch court to 10 years for online fraud, blackmail* : www.cbc.ca/news/canada/british-columbia/aydin-coban-sentenced-netherlands-online-fraud-blackmail-1.4027359

Centre Hubertine Auclert, (2018), *Cyber-violences conjugales* : www.centre-hubertine-auclert.fr/sites/default/files/documents/rapport_cyberviolences_conjugales_web.pdf

Childnet, Save the Children, UCLan (2019), Project DeShame : www.childnet.com/our-projects/project-deshame

Citizen Lab, (2020), *Installing Fear* : https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/

Citron, D., Franks, M.A., (2014), *Criminalizing Revenge Porn* : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946

Comité pour l'élimination de la discrimination à l'égard des femmes (2007), *Recommandation générale nº 35 sur la violence à l'égard des femmes fondée sur le genre, portant actualisation de la recommandation générale nº 19* : https://undocs.org/pdf?symbol=fr/CEDAW/C/GC/35

Conseil de l'Europe, (2001a), *Convention sur la cybercriminalité :* https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680081561

Conseil de l'Europe, (2001b), *Rapport explicatif de la Convention sur la cybercriminalité*: https://rm.coe.int/16800ccea4

Conseil de l'Europe (2003), *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques :* https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/189

Conseil de l'Europe (2007), *Traite des êtres humains : recrutement par internet :* https://rm.coe.int/090000168064eeec1

Conseil de l'Europe (2011a), *Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique :* https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/090000168008482e

Conseil de l'Europe, (2011b), *Rapport explicatif de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique*, Série des Traités du Conseil de l'Europe nº 210 : https://rm.coe.int/16800d383a

Conseil de l'Europe (2015a), *Comité des Parties, Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, règlement intérieur du Comité des Parties :* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046325c

Conseil de l'Europe, (2015b), *Encourager la participation du secteur privé et des médias à la prévention de la violence à l'égard des femmes et de la violence domestique :* https://rm.coe.int/16805970be

Conseil de l'Europe (2017a), *Journalists under pressure – Unwarranted interference, fear and self-censorship in Europe :* https://book.coe.int/en/human-rights-and-democracy/7295-pdf-journalists-under-pressure-unwarranted-interference-fear-and-self-censorship-in-europe.html

Conseil de l'Europe (2017b), Partenariat avec les entreprises numériques : https://rm.coe.int/090000168079ced3

Council of Europe (2018a), Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data, available at : https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

Conseil de l'Europe (2018b), *Stratégie du Conseil de l'Europe pour l'égalité entre les femmes et les hommes 2018-2023 :* https://rm.coe.int/prems-093718-fra-gender-equality-strategy-2023-web-a5-corrige/16808e0809

Conseil de l'Europe, (2018c), *Étude cartographique sur la cyberviolence*, Comité de la Convention sur la cybercriminalité, Groupe de travail sur la cyberintimidation et les autres formes de violence en ligne, en particulier contre les femmes et les enfants (CBG) : https://rm.coe.int/t-cy-2017-10-cbg-study-fr-v2/1680993e65

Conseil de l'Europe, (2019), *Recommandation CM/Rec(2019)1 du Comité des Ministres aux États membres sur la prévention et la lutte contre le sexisme,* Comité des Ministres : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168093b269

Conseil de l'Europe, Brown, A., (2020a), *Models of Governance of Online Hate Speech. On the emergence of collaborative governance and the challenges of giving redress to targets of online hate speech within a human rights framework in Europe :* https://rm.coe.int/models-of-governance-of-online-hate-speech/16809e671d

Conseil de l'Europe, (2020b), Comité d'experts sur la lutte contre le discours de haine, *Background document :* https://rm.coe.int/background-for-adi-msi-dis-june-2020/16809f6b6d

Conseil de l'Europe (2020c), *Brochure sur les quatre piliers de la Convention d'Istanbul*: https://rm.coe.int/coe-istanbulconvention-brochure-fr-r03-v01/1680a06d50

Conseil de l'Europe (2020d), *Déclaration du président et de la vice-présidente du Comité de Lanzarote sur le renforcement de la protection des enfants contre l'exploitation et les abus sexuels en temps de pandémie de COVID-19 :* https://rm.coe.int/covid-19-lc-statement-fr-final/16809e17af

Conseil de l'Europe (2021), Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique, "Recommandation générale n° 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes", disponible sur : A METTRE A JOUR APRES LE 24 NOV

Daskal, J., and Kennedy-Mayo, D., (2020), *Budapest Convention : What is it and How is it Being Updated?*, Cross Border Data Forum : www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/

Dodaj, A., Sesar, K. (2020), *Sexting categories*, Mediterranean Journal of Clinical Psychology : https://cab.unime.it/journals/index.php/MJCP/article/view/2432/0

Dreßing H., Bailer J., Anders A., Wagner H. and Gallas C. (2014), "Cyberstalking in a large sample of social network users : Prevalence, characteristics, and impact upon victims", in Cyberpsychology, Behavior, and Social Networking, 17(2), 61-67, available at : www.few.vu.nl/~eliens/sg/local/cyber/social-stalking.pdf.

European Agency for Fundamental Rights (2014), *Violence à l'égard des femmes : une enquête à l'échelle de l'UE. Les résultats en bref :* https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance-oct14_fr.pdf

Commission européenne, (2019), *E-evidence – cross-border access to electronic evidence :* https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

Commission européenne, (2020a), *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Une Union de l'égalité : stratégie en faveur de l'égalité entre les hommes et les femmes 2020-2025 :* https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX :52020DC0152&from=FR

Commission européenne, (2020b), *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Stratégie de l'UE relative au droit des victimes (2020-2025) :* https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX :52020DC0258&from=FR#footnoteref32

European Commission (2020c), Countering illegal hate speech online, 5th evaluation, of the Code of Conduct, available at : https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf.

Commission européenne (2020d), *Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE :* https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX :52020PC0825&from=fr

Parlement européen, (2020), *Réponse à une question parlementaire :* https://www.europarl.europa.eu/doceo/document/E-9-2020-002184-ASW_FR.html#def1

Service de recherche du Parlement européen (2021), *Combating gender-based violence : Cyber violence, European added value assessment :* www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf

Union européenne, (2008), *décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal :* https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33178

European Women's Lobby (2017), *#HerNetHerRights ressource pack :* www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf

Europol (n.d.), *High-Tech crime, Crime areas*, consulté le 1er octobre 2020 : www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/high-tech-crime

Facebook (n.d.), *Not without my Consent*, www.facebook.com/safety/notwithoutmyconsent/pilot, consulté le 14 octobre 2020.

Fetters, A., The Atlantic, (2018), *Why It's Hard to Protect Domestic-Violence Survivors Online :* www.theatlantic.com/family/archive/2018/07/restraining-orders-social-media/564614/

Fondation des Femmes (n.d.), Une Force Juridique, consulté le 20 septembre : https://fondationdesfemmes.org/une-force-juridique/

FRA (Fundamental Rights Agency) (2014), "Violence against women : an EU-wide survey. Main results report", available at : https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report.

Code pénal allemand, (Strafgesetzbuch – StGB), *Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by article 2 of the Act of 19 June 2019 (Federal Law Gazette I, p. 844)*" : www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

Ging, D., et Siapera, E., (2018), *Special issue on online misogyny*, Feminist Media Studies : https://doi.org/10.1080/14680777.2018.1447345

Glitch UK (n.d.), *A little means a lot*, consulté le 1er octobre 2020 : https://fixtheglitch.org/almal/

Glitch & End Violence against Women (2020), *The Ripple Effect, Covid 19 and the epidemic of online abuse :* https://glitchcharity.co.uk/wp-content/uploads/2021/04/Glitch-The-Ripple-Effect-Report-COVID-19-online-abuse.pdf

Guney, G., (2020), *The Group of Experts under the Istanbul Convention on Preventing and Combating Violence against Women and Domestic Violence and the ECtHR : Complementary or Contradictory Tools?*, EJIL :Talk, Blog of the European Journal of International Law : www.ejiltalk.org/the-group-of-experts-under-the-istanbul-convention-on-preventing-and-combating-violence-against-women-and-domestic-violence-and-the-ecthr-complementary-or-contradictory-tools/

Hampton, R., Slate, (2019), T*he Black Feminists Who Saw the Alt-Right Threat Coming :* https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html

Megarry J. (2014), "Online incivility or sexual harassment ? Conceptualising women's experiences in the digital age", in *Women's Studies International Forum*, 47, pp. 46-55, available at : www.sciencedirect.com/science/article/abs/pii/S0277539514001332.

Harris, B., (2020a), *Technology, domestic and family violence : perpetration, experiences and responses*, QUT Centre for Justice : https://eprints.qut.edu.au/199781/1/V1_Briefing_Paper_template.pdf

Harris, B., (2020b), *Technology and Violence Against Women*, Walklate, S., Fitz-Gibbon, K., Maher, J. et McCulloch, J. (dir.) The Emerald Handbook of Feminism, Criminology and Social Change (Emerald Studies in Criminology, Feminism and Social Change), Emerald Publishing Limited, pp. 317-336 : https://eprints.qut.edu.au/199781/1/V1_Briefing_Paper_template.pdf

Hinson, L., Mueller, J., O'Brien-Milne. L., Wandera, N., (2018), *Technology-facilitated gender-based violence : What is it, and how do we measure it?*, International Center for Research on Women : www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/

IPU (2018), *Sexism, harassment and Violence Against Women in parliaments in Europe :* www.ipu.org/resources/publications/issue-briefs/2018-10/sexism-harassment-and-violence-against-women-in-parliaments-in-europe

Kelly L. (1988), Surviving Sexual Violence (Feminist Perspectives Series), University of Minnesota Press.

Khouiel, L., Vice (2020), *Quand le revenge porn s'adapte au confinement :* www.vice.com/fr/article/bvg4pz/quand-le-revenge-porn-sadapte-au-confinement

Klein, J., The Atlantic, (2020), V*irtual parental visitation could have unintended consequences for abuse survivors :* www.theatlantic.com/family/archive/2020/06/dangers-virtual-visitation-abuse-victims/613243/

Langlais-Fontaine, C., (2020), *Démêler le vrai du faux : étude de la capacité du droit actuel à lutter contre les deepfakes*, La Revue des droits de l'homme : http://journals.openedition.org/revdh/9747

Lavin, T., (2020), Culture Warlords : My Journey into the Dark Web of White Supremacy, Hachette

Laxton, C., Women's Aid, (2014), *Virtual World, Real Fear, Women's Aid report into online abuse, harassment and stalking :* http://bit.ly/2h0W4OX

Legifrance (2018), Loi no. 2018-703 du 3 aout 2018 renforçant la lutte contre les violences sexuelles et sexistes, disponible sur : www.legifrance.gouv.fr/jorf/id/JORFTEXT000037284450/.

Legifrance (2020), Loi no. 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales, disponible sur : www.legifrance.gouv.fr/jorf/id/JORFTEXT000042176652.

Liggett O'Malley, R., (2020), *Cyber Sextortion : An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime :* www.researchgate.net/publication/339798771_Cyber_Sextortion_An_Exploratory_Analysis_of_Different_Perpetrators_Engaging_in_a_Similar_Crime

Maple, C., Shart, E., Brown, A. (2011), *Cyber stalking in the United Kingdom : An Analysis of the ECHO Pilot Survey*. Université du Bedfordshire : www.beds.ac.uk/media/244385/echo_pilot_final.pdf

Markit, IHS., (2017), *The Internet of Things : A movement, not a market*, cité dans Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., et Tanczer, L. (2019). '*Internet of Things' : How abuse is getting smarter*. Safe –The Domestic AbuseQuarterly : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350615

McGlynn, C., Rackley, E. & Houghton, R. (2017), *Beyond 'Revenge Porn' : The Continuum of Image-Based Sexual Abuse :* https://link.springer.com/article/10.1007/s10691-017-9343-2#citeas

Morgan C., Webb R. T., Carr M. J., Kontopantelis E., Green J., Chew-Graham C. A., Kapur N. and Ashcroft D. M. (2017), "Incidence, clinical management, and mortality risk following self-harm among children and adolescents : cohort study in primary care", in *BMJ 359*, j4351, available at : www.bmj.com/content/359/bmj.j4351.

Morrow, S., (2019), *Should We Worry About IoT Being Used as a Weapon of Mass Control?*, IoTforall : www.iotforall.com/iot-domestic-abuse

NPR (2014), *Smartphones Are Used To Stalk, Control Domestic Abuse Victims :* www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

O'Connell, A., Bakina, K., (2020), *Using IP rights to protect human rights : copyright for 'revenge porn' removal*, Legal Studies, Cambridge University Press : www.cambridge.org/core/journals/legal-studies/article/using-ip-rights-to-protect-human-rights-copyright-for-revenge-porn-removal/2C1840AC0EB870FB2134CEE9586E76D6

Pariser, E., (2011), *The Filter Bubble : What the Internet Is Hiding from You*, Penguin.

Peppet, S. R., (2014), *Regulating the Internet of Things : First Steps Toward Managing Discrimination, Privacy, Security, and Consent :* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074

Plan International (2020), *Free To Be Online?*, the States of the World's Girls : https://plan-international.org/publications/freetobeonline

Politico (2020), *French constitutional court strikes down most of hate speech law* : www.politico.eu/article/french-constitutional-court-strikes-down-most-of-hate-speech-law/

Powell, A., Henry, N., (2016), *Policing technology-facilitated sexual violence against adult victims : police and service sector perspectives :* www.researchgate.net/publication/297673926_Policing_technology-facilitated_sexual_violence_against_adult_victims_police_and_service_sector_perspectives

Powell, A., Scott, A.J., Flynn, A., Henry, N., (2020), *Image-based sexual abuse : An international study of victims and perpetrators :* www.researchgate.net/publication/339488012_Image-based_sexual_abuse_An_international_study_of_victims_and_perpetrators

Rogers, M., (2018), *No More Revenge : Criminalizing Non-Consensual Pornography Through the Convention on Cybercrime*, Michigan Journal of International Law, University of Michigan Law School Ann Arbor, Michigan : www.mjilonline.org/no-more-revenge-criminalizing-non-consensual-pornography-through-the-convention-on-cybercrime/

Salas, M., Gender IT, (2013), *The false paradox : freedom of expression and sexist hate speech* : https://www.genderit.org/es/node/3820

Salter, M., Dragiewicz, M., Burgess, J., Fernández, A., Suzor, N., Woodlock, D., Harris, B., (2018), *Technology facilitated coercive control : Domestic violence and the competing roles of digital media platforms*, Feminist Media Studies : www.researchgate.net/publication/323847103_Technology_facilitated_coercive_control_Domestic_violence_and_the_competing_roles_of_digital_media_platforms

Šepec, M., (2019), "Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence", International Journal of Cyber Criminology, available at : https://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf

Setterfield, R., (2019), *The Regulation Of 'Revenge Porn' in England And Wales : Are Existing Legal Solutions Effective?*, University of Surrey : http://epubs.surrey.ac.uk/851986/1/Rosalind%20Setterfield%20Thesis%20%28Revisions%29.pdf

Simonovic, D., (2020), Nations Unies. Conseil des droits de l'homme. Rapporteuse spéciale sur la violence contre les femmes, Nations unies. Conseil des droits de l'homme. Secrétariat, *Rapport de la Rapporteuse spéciale sur la violence contre les femmes, ses causes et ses conséquences concernant la violence en ligne à l'égard des femmes et des filles du point de vue des droits de l'homme :* https://digitallibrary.un.org/record/1641160

Sinders, C., (2017), *Current Reading List (of papers) on Online Harassment and Machine Learning* : https://medium.com/@carolinesinders/current-reading-list-of-papers-on-online-harassment-and-machine-learning-c70fe674f9d1

Tegan S. Starr, T.S., Lavis. T., (2018), *Perceptions of Revenge Pornography and Victim Blame*, International Journal of Cyber Criminology Vol 12 Issue 2 juillet – décembre 2018 : www.cybercrimejournal.com/Starr&Lewisvol12issue2IJCC2018.pdf

Van der Wilk, A., (2018), département thématique « Droits des citoyens et affaires constitutionnelles », *Cyber violence and hate speech online against women :* www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

Verdelho, P., (2019), *Obtaining digital evidence in the global world*, UNIO – EU Law Journal : https://revistas.uminho.pt/index.php/unio/article/view/2298

Woodlock, D., (2017), *The Abuse of Technology in Domestic Violence and Stalking*, Violence Against Women : http://marvin.cs.uidaho.edu/Teaching/CS112/domesticAbuseStalking.pdf

La Convention d'Istanbul est le traité international le plus ambitieux en matière de lutte contre la violence à l'égard des femmes et la violence domestique. Son vaste ensemble de dispositions couvre des mesures de prévention et de protection de grande envergure ainsi qu'un certain nombre d'obligations visant à garantir une réponse adéquate de la justice pénale à ces graves violations des droits humains. La Convention de Budapest sur la cybercriminalité est l'accord international le plus pertinent en matière de cybercriminalité et de preuve électronique. Elle prévoit la criminalisation des infractions commises à partir et au moyen d'ordinateurs, des outils de droit procédural pour obtenir des preuves électroniques, ainsi que la coopération internationale entre les Parties.

Cette étude examine l'application complémentaire de ces deux conventions pour lutter contre la violence en ligne à l'égard des femmes et celle facilitée par la technologie, au moyen de politiques coordonnées, la prévention, la protection, les poursuites et la coopération internationale.

PREMS 155621

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE